INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

ProQuest Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

UMI®

Red, Gray, and Blue: A Security Environment Approach to National Security Policy Countering Emerging Threats Targeting Critical Infrastructure

By

William Charles Flynt III
Lieutenant Colonel, U.S. Army

B.A., The Ohio State University, 1983
M.P.A., Cornell University, 1991
M.M.A.S., School of Advanced Military Studies of the U.S. Army Command & General Staff College, 1995

Submitted to the Department of Political Science
and the Faculty of the Graduate School of the
University of Kansas
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy

Professor Philip A. Schrodt, Ph.D.
Chair

Professor Burdett A. Loomis, Ph.D.

Professor Donald P. Haider-Markel, Ph.D.

Date Submitted: 11 June 2001

Disclaimer: The views expressed in this study do not necessarily reflect the official positions of the United States Department of Defense or any government agency.

Abstract

William Charles Flynt III, M.P.A., M.M.A.S., Ph.D.
Department of Political Science, May 2001
University of Kansas

Novel aspects of the security environment make necessary a radical change in the paradigm employed by the US national security elite in formulating national security policies. All policy is grounded on theory, and theory is predicated by its paradigm. Failure by policymakers to grasp that a Kuhnian *gestalt* switch is required to correctly perceive the new security environment has allowed the continued influence of an obsolete paradigm that sees the world political system as an international system of states *qua* major actors, with interests defined in terms of geographical regions. This paradigm does not adequately explain unique components of the altered world political system. Consequently, national security policies founded on this paradigm do not adequately address the most dangerous threats to the United States emerging in the current security environment – non-state actors employing Weapons of Mass Effects (WME). Several factors enable non-state actors to challenge sovereign states, and especially the United States, with unprecedented levels of violence. These factors include rampant proliferation of WME and related materials and equipment in the aftermath of the Soviet Union's demise, the diffusion of knowledge and technologies that arm non-state actors with a level of sophistication and expertise in research and development formerly the exclusive province of great power states, the freeing of non-state actors' political agendas from the Cold War's bipolar constraints, the expansion of an open Internet and broader communications architecture that provides instant access to information and secure, global communications, and the emergence of a US strategic vulnerability in its absolute reliance on a highly-automated, tightly-interdependent and fragile system of infrastructures. This study argues that a radical transformation in national security policy is needed to counter emerging threats targeting US critical infrastructures and population. This transformation cannot effectively proceed until the old paradigm is rejected. To that end, this dissertation presents a paradigmatic framework that describes a security environment approach and details seven models of possible state versus non-state conflict. The study also defines a comprehensive typology of threats by identities, means, *modus operandi*, targeting preferences, and ends, and develops decision trees that typify the order of action, time sequencing, and interactions during a non-state actor's WME attack of a state's critical infrastructures or population.

To Dea, Bill, Kelsey, and Connor

In dim eclipse, disastrous twilight sheds
On half the nations, and with fear of change
Perplexes monarchs.
~ Milton, *Paradise Lost*

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

Tables

Figures

Chapter One: Introduction

Effective research scarcely begins before a scientific community thinks it has acquired firm answers to questions like the following: What are the fundamental entities of which the universe is composed? How do these interact with each other and with the senses? What questions may legitimately be asked about such entities and what techniques employed in seeking solutions? At least in the mature sciences, answers (or full substitutes for answers) to questions like these are firmly embedded in the educational initiation that prepares and licenses the student for professional practice. Because that education is both rigorous and rigid, these answers come to exert a deep hold on the scientific mind. That they can do so does much to account both for the peculiar efficiency of the normal research activity and for the direction in which it proceeds at any given time. When examining normal science...we shall want finally to describe that research as a strenuous and devoted attempt to force nature into the conceptual boxes...[1]

This study finds that US national security policies designed to counter emerging threats are flawed, because they ultimately rest on an inappropriate theoretical framework. The national security policy elite has approached the challenge posed by emerging threats from perspectives founded upon a state-centric worldview. This worldview is not obsolete – states matter – but it is inadequate for formulating national security policies countering emerging threats. Attempting to craft policy countering emerging threats from a perspective that sees a security environment comprised of states is an inappropriate application of paradigm, theory, and model. It is akin to approaching guerrilla warfare wearing the lenses of strategic nuclear deterrence. The lenses are not flawed, just mistakenly employed as an approach to a problem they were never designed to solve. "The proper tool for the job" is a familiar aphorism. Paradigms, theories, and models are intellectual tools and not articles of faith. Failure to employ the correct tool for the task – or to design new tools for new tasks – leads to the also familiar aphorism of Jervis' Law of the Instrument – when all you have is a hammer, everything looks like a nail.[2] However "strenuous and devoted" the "attempt to force nature into the conceptual boxes" of an inappropriate intellectual tool, it is ultimately futile. In the case of national security policy, it is dangerously irresponsible. This study explicates a new framework relevant to the fundamentally changed security environment, specifically addressing emerging threats targeting US critical infrastructure and population with Weapons of Mass Effect (WME).[3] The implications for national security policy are highlighted and examined from the perspective of this framework.

---

[1] Thomas S. Kuhn, *The Structure of Scientific Revolutions*, 2nd ed. (Chicago: The University of Chicago Press, 1970), pp. 4-5.

[2] Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976), p. 108.

[3] Weapons of Mass Effect (WME) include chemical, biological, radiological, nuclear and cyber weapons, as well as the employment of conventional weapons in ways that inflict massive *effects*. Although the use of such weapons can easily be operationalized as a quantitative variable based on projected casualties or other arbitrary measures, this would limit the study of emerging threats in ways that would foreclose the analysis of means, targeting, and ends unrelated to inflicting casualties, but still highly-relevant to national security concerns. The standard of emerging threat success is not always inflicting casualties, and not all WME are capable of causing injury to humans. This is

Following Van Evera's categories of research, this dissertation proposes theory and is policy-evaluative and prescriptive. Theory and policy are inextricably bound. "It is often said that policy-prescriptive work is not theoretical. The opposite is true. All policy proposals rest on forecasts about the effects of policies. These forecasts rest in turn on implicit or explicit theoretical assumptions about the laws of social and political motion. Hence all evaluation of public policy requires the framing and evaluation of theory, hence it is fundamentally theoretical."[4] The new security environment requires new policies, in turn requiring the framing of theory within a new paradigm.

Recent efforts at designing policy to counter emerging threats have recognized the challenge, but failed to adequately meet it. The US Department of Justice's (DoJ) futile efforts to limit the proliferation of encryption software beyond US borders, and its later equally quixotic overtures to the European Community (EC) to establish by fiat an international public key escrow system, demonstrate that the most fundamental essence of the challenge was not understood. Operating from a Cold War paradigm of state control of telecommunications systems, DoJ sought to control the "great game" of strategic intelligence by imposing new rules to offset their lack of agility, only to discover that transnational actors were not playing by DoJ's rules, or even the same game.

Over a decade ago the Cold War ended and the established paradigm was made inadequate. Lieutenant General Michael Hayden, the Director of the National Security Agency (NSA), believes changing technology and the changed security environment is affecting US intelligence capabilities, stating "We are behind the curve in keeping up with the global telecommunications revolution."[5] Addressing the need to change, General Hayden added "This is about an agency that's grown up in one world, learned a way to succeed within that world and now finds itself in another world, and it's got to change if it hopes to succeed in that world."[6] General Hayden's focusing event convincing him of the need for change occurred on January 24th, 2000, when the NSA's systems, strained and running at near maximum capacity went offline for 72 hours.[7] In the current security environment, past approaches are inadequate to deal with new challenges, like strong encryption, fiber optic cables, and laptops.

---

especially true of cyberstrikes. Instead, a qualitative approach is taken regarding WME, hence the relative refinement of the more primitive term Weapons of Mass Destruction (WMD).

[4] Stephen Van Evera, *Guide to Methods for Students of Political Science* (Ithaca: Cornell University Press, 1997), pp. 89-93.

[5] Interview with Lieutenant General Michael V. Hayden, "NSA Head: Tech Weakness Makes US Vulnerable," CBS's 60 Minutes II, as cited by Reuters, February 12, 2001. Document available at http://www.cnn.com/2001/TECH/internet/02/12/usa.security.reut/index.html.

[6] Ibid.

[7] Lieutenant General Michael V. Hayden, Director National Security Agency, remarks to the Kennedy Political Union of the American University, 17 February 2000, p. 3 of 7; document available at

For a decade after the Cold War the NSA remained ossified within a paradigmatic framework that saw the challenge as identifying military forces in Eastern Europe and eavesdropping on first the Soviet Union, then the Commonwealth of Independent States, and finally a rump Russian republic. Former Cold Warriors observe the Soviet Union collapsed of its own weight, a Darwinian failure to adapt to a changing environment. General Hayden remarks "[NSA] benefited in the past from the high walls of security we placed around our activities during the cold war. However, we've paid a price...[w]e can no longer afford to operate that way."[8] This study argues that concerning emerging threats targeting critical infrastructure with WME, the United States may also demonstrate a Darwinian failure to adapt to a changed environment. If so, it will be because we failed to recognize that our past paradigm had become our intellectual prison. This study follows Imre Lakatos' insight that "conceptual frameworks can be developed and also replaced by new, *better* ones; it is we who create our 'prisons' and we can also, critically, demolish them."[9]

The study's main line of argument is that in the current security environment policymakers require a different theoretical framework upon which to base national security policies intended to protect critical infrastructures from non-state actors employing asymmetric, anonymous, and asynchronous attacks. In developing a security environment approach to national security policy, this study addresses two closely related questions: 1. How can we understand the changed security environment theoretically?, and, 2. What are the implications of the changed security environment for national security policies countering emerging threats? From examination of these questions will flow a framework to understand the changed security environment and emerging threats, and discussion of the implications for national security policy countering emerging threats from the perspective of this framework. As it addresses theory, the study deals to great extent deductively with these questions; as a component of the dissertation includes national security policy evaluation and prescription, it is necessarily normative and empirical.

These questions arise due to a confluence of factors. The end of the Cold War and the subsequent demise of the Soviet Union freed two potent forces: the liberated minds of millions of individuals globally who were anxious for political power, as well as the stockpiled inventories, technologies, and knowledge to develop WME. Concurrent with this freeing of the international

---

http://www.nsa.gov. See also Gregory Vistica, "Inside the Secret Cyberwar," *Newsweek* (February 21, 2000).

[8] Hayden, Remarks to Kennedy Political Union, p. 6 of 7.

[9] Imre Lakatos, "Falsification and the Methodology of Scientific Research Programmes," in Imre Lakatos and Alan Musgrave, eds., *Criticism and the Growth of Knowledge* (Cambridge: Cambridge University Press, 1970), p. 104. Original italics.

system from a bipolar structure came an unleashing of human energy, political ideals, potential capabilities for violence, and the proliferation of knowledge.[10] Further accelerating change, the breadth and depth of technology continues to expand at an exponential rate. Our innovation exceeds our understanding, and the advantages of expert knowledge and superiority in research and development has been wrested from states; once, but no longer, the exclusive possessors of those advantages. One result has been the ascension of some "peripheral" states, for example India, to great power status not only in the realm of nuclear weapons, but also in the arena of information technology. The proliferation of WME and related materials and equipment, the diffusion of knowledge and technologies that establish non-state actors' functional parity in research and development of weapons, the unleashing of non-state actors to pursue political agendas free of superpower domination, the expansion of the Internet that provides instant information and global communications, and the emergence of US strategic vulnerability through reliance on highly-automated, tightly-interdependent and fragile infrastructures all conspire to make it a far different world. This confluence of factors has spawned a convergence of novel threats. This study, however, focuses on another challenger – non-state actors. Formerly armed only with intent to strike at the United States, but lacking capability, several now command both.

The dissertation argues that the world political system changed following the end of the Cold War, but that policymakers have not abandoned the past paradigm that guided Cold War strategy, hence US security policy's failure to effectively address emerging threats. The study offers two answers to the questions concerning understanding and implications of the changed security environment. First, the changed security environment can be understood for the purpose of national security policy formulation from the Red, Gray, and Blue paradigm detailed below. From this paradigm theories and models flow to describe and explain the socio-political characteristics and actions of non-state threat actors in the changed security environment. Second, national security policy must be tailored to the specific threats it is designed to counter. Tailoring policy to threat, as will become clear in the analysis below, is immensely challenging in the new security environment. Ironically, national security elites appear, as Mearsheimer presciently foresaw, almost nostalgic for the

[10] Following Kaplan, in a loose bipolar system "alliances tend to be long-term, to be based on permanent...interests, and to have ideological components." The result of nuclear proliferation in a loose bipolar system is that "wars tend to be quite limited; and even limited wars are rare." The dissolution of the Cold War eliminated these effects of system structure, and has made possible a variety of the Unit Veto System sketched by Kaplan, where WME possessed by non-state actors can deter Great Powers. See Morton A. Kaplan, "Variants on Six Models of the International System," in James N. Rosenau, ed., *International Politics and Foreign Policy* (New York: The Free Press, 1969), pp. 297-298 [quotes], pp. 298-300 [Unit Veto System].

predictability of the Soviet Union.[11] A fundamental element throughout the study is the examination of the use of power, in its most elemental form of violence, by non-state actors at the systemic level. The violence employed by these actors is not limited to physical attack, but encompasses a range of capabilities examined in depth in Chapter Four.

The centrality of non-state actor violence to this study, however, requires a brief treatment here. The issue is not that non-state actors can use violence; non-state actors have commonly used violence, sometimes wide-spread violence, throughout history. The issue is also not about carnage. In fact, some examples of the violence of concern in this study may not directly produce casualties as their primary effect. Nor is scale of violence a quantifiable indicator of efficacy of threat attack, as a small application of force against a critical node may yield disproportionate effects. The violence of concern in this study is based on effects, regardless of means of inflicting damage, methods of employment, or even results in the physical dimensions. This violence can be described as "system relevant" violence.

As a definitional issue in the dissertation, system relevant violence is used throughout to describe a level of violence, which varies in characteristics by case, that penetrates a threshold resulting in a change in another systemic actor's ability to exercise power. A strike that lessens the ability of an actor to exercise power is relevant to that actor's capabilities in the world political system, and thus the strike is a system relevant level of violence.

The study takes conditional exception to Wendt's assertion that "Since the state is a structure of political authority with a monopoly on the legitimate use of organized violence, when it comes to the regulation of violence internationally it is states one ultimately has to control."[12] The exception taken is conditional, because control of states could limit international (i.e., inter-state, if Wendt's assertion is interpreted to conflate the term nation with state) violence. From this interpretation, however, the first clause specifying political authority, monopoly, and legitimate use of organized violence is superfluous. The argument could be reduced to "control of states regulates international [sic] violence." States may, or may not, possess a monopoly on legitimate, organized violence. However, the "control" of states (itself a problematic proposition under anarchy) would only constitute a necessary (not sufficient) condition towards regulation of the employment of only "legitimate,"(but not "illegitimate") violence between states (but not between asymmetric, i.e., state versus non-state,

---

[11] John J. Mearsheimer, "Why We Will Soon Miss the Cold War," *The Atlantic Monthly*, August 1990, pp. 35-50.
[12] Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999), p. 8.

actors at the systemic-level). Thus Wendt's premise that the control of states as structures of political authority with "a monopoly on the legitimate use of organized violence" is sufficient to regulate violence internationally is either partially weakened or so narrowly correct that an important aspect is missing. In fairness to him, Wendt understands the above discussion, recognizes that other actors employ violence, and states that the choices of unit of analysis and level of analysis dictate what a theory can explain. The point is not that Wendt's chosen point of departure is incorrect, rather there is a need for theory explaining other types of system relevant violence. This requires a different paradigm. In Wendt's *Social Theory of International Politics*, he self-consciously constrains his argument to state actors. That is an appropriate and necessary approach to describing and explaining systemic politics of state actors. This study concerns system relevant violence by non-state actors, or states masquerading as non-state actors through imitation of various *modus operandi* and signature traits for deceptive purposes. Taking conditional exception to Wendt's approach using the state as major system actor, however, does not mean taking exception to Wendt's insights. Chapters three and four draw heavily on his ideas, especially concerning identities and their deterministic shaping of interests.

This criticism of inadequacy could be applied to Neorealism as well. Waltz, like Wendt, does not claim to explain everything, in spite of the arguments of some critics' protestations.[13] In fairness to Waltz, until recently states were, in fact, the only actors capable of system relevant levels of violence, for example by employing WME, and this made a hard-core tenet of Neorealism that states were the principal actors that counted on the systemic level tenable. The emergence of non-state actors capable of system relevant violence, however, is a new aspect of the changed security environment; a change of the underlying reality that theory is required to explain. We need new theories, because we have a greatly altered reality to explain. That is not to argue that state-centric theory is obsolete; it is required to explain systems of state actors, or purely interstate systems. But as Wendt points out "that simply means that state-centered IR theory can only be one element of a larger progressive agenda in world politics, not that it cannot be an element at all."[14] The degree of change is so great, we first need a relevant paradigm. However, that is not to argue that no elements survive a paradigm shift. There is continuity across shifts, otherwise there would exist no potential for progress. Below this point is revisited in discussion regarding continuity of classical Realist tenets applicable even in the new security environment.

---

[13] See, for example, John A. Vasquez, "The Realist Paradigm and Degenerative versus Progressive Research Programs: An Appraisal of Neotraditional Research on Waltz's Balancing Proposition," *American Political Science Review*, Vol. 91, No. 4 (December 1997), pp. 899-912.
[14] Wendt, *Social Theory of International Politics*, p. 10.

This study asserts that non-state actors capable of WME employment can potentially affect the world political system in both scope and degree that rivals all but the most powerful, advanced states. Systemic anarchy makes conceptions of "legitimate" violence problematic. Under anarchy, those actors capable of employing violence have the self-ordained right to do so; those opposing such violence have the self-ordained right to attempt to stop them. From this conflict is spawned. Non-state actors, from some normative perspectives, may not be empowered with "legitimate" political authority to employ system relevant violence (as opposed to states employing interstate violence), but they can employ violence at and beyond the system relevant threshold. This fact has implications for interstate (vice system relevant) violence as a consequence of Third Actor Escalation during an interstate dispute.

Third Actor Escalation of a crisis by a non-state actor could act as the catalyst for open hostilities between states. A simple scenario illustrates the point. Two state actors are involved in brinkmanship during a crisis that approximates the game of Chicken. As a result of deliberate moves designed to enhance bargaining position, intimidate, and convince the opponent of one's resolve, as well as serve as preparations for the possibility of open warfare should neither participant "swerve," both state actors have reduced their opponent's margins for timely response to indications and warnings by prepositioning forces and heightening defense conditions. At this critical point, a non-state actor masking its attack as one of the state-actor protagonists launches a strike, and the attacked state immediately retaliates against the other state, in retribution for what it has perceived as a preemptive strike launched against itself by the other state. The non-state actor, playing Blainey's fisherman, furthers its interest while the states in their roles as fighting waterbirds are distracted.[15]

In this new world order deterrence is more difficult. Discerning indications and warnings encompasses novel challenges, demands new disciplines and technologies, and is a different art of war than that exercised in the Cold War. The nature of covert operations escapes the bounds of the physical world. Conventional and nuclear forces are diminished in importance, incapable of engaging the new, emerging threats, yet still indispensable because, while their potent viability paradoxically negates any probability of their use, their absence leaves a state actor in a condition of relative unarmed vulnerability before other state actors possessing the capability. States have not transcended or escaped interstate relations explained by state-centric IR theories. Rather, they now have the additional burden of operating in a world political system (vice purely interstate system) where non-state actors are relevant as "major actors." This necessitates a new paradigm, theories, and models to inform national security policy.

---

[15] Geoffrey Blainey, *The Causes of War*, 3rd ed., (New York: The Free Press, 1988).

State-centric paradigms for understanding international relations are of questionable utility for formulating security policy countering emerging threats. Neorealism, Neoliberal Institutionalism, and other mainstream, international relations theories and their variants that have state-centric, Lakatosian hard cores must be rejected for the purpose of understanding the emerging threats detailed in this study. It is not necessary to argue that these theories are flawed in explaining various aspects of the international system. There is a large literature that debates, without closure, the merits and demerits of the competing theories, and it is not the purpose of this study to become involved in that debate. Instead, it suffices for the purpose of this study to simply point out that theories explaining the interactions of states within the international system are, by definition, not designed to explain state versus non-state conflict. A theory detailing the politics of state actors with both anonymous and overt, non-state threat actors is not engaged in the realm of interstate relations, but is engaged in the realm of world politics between asymmetric actor types. Consequently, a theory of international relations that views states as the "major actors" is largely inapplicable to the research focus of this study. This study examines a different problem within the arena of world politics, not international *qua* interstate relations, *per se*.

Similar to how a state-centric paradigm is unable to serve as a foundation for national security policy countering emerging, non-state threats, a theory of policy change and formulation that is incapable of explaining radical change in the policy environment is unable to detail how such a process of formulating policy to counter emerging threats in the current fundamentally altered security environment *should* occur. Baumgartner and Jones' theory of Punctuated Equilibrium (PE) parallels a Kuhnian pattern of scientific revolutions, and is capable of *prescribing* as a theoretical guide to policymakers *how* the policy formulation process should proceed in crafting new policies to deal with emerging, non-state threats. A concrete policy document example advocating just such a "revolutionary" destruction of the old paradigm-based policies and institutions, and its replacement by new paradigm-based policies and radical institutional redesign is examined; the January 2001 Phase III report of the United States Commission on National Security/21st Century, *Road Map for National Security: Imperative for Change*. This final report of the Commission states that "after more than two years of serious effort, this Commission has concluded that without significant reforms, American power and influence cannot be sustained" in the new security environment.[16] The Commission recommends several major policy departures from the past way of doing business, including the creation of a National Homeland Security Agency (NHSA) based on the Federal Emergency

[16] *Road Map for National Security: Imperative for Change*, Phase III Report of the United States Commission on National Security/21st Century (Washington, DC, 31 January 2001), p. iv.

Management Agency (FEMA), and reassigning the United States Customs Service, the United States Border Patrol, and the United States Coast Guard to the NHSA.[17]

In formulating national security policies to counter emerging threats, paradigms founded on a state-centric perspective of international relations are inadequate. The term *international* relations itself points to the need. Paradigms of international relations, by definition, address the relations between nations, or, as typically used, nations are conflated with states. A *world politics* paradigm, here specifically a security environment approach – Red, Gray, and Blue – is required when dealing with emerging threats that are non-state actors capable of system relevant violence.

A fundamental text of the discipline of political science and the field of international relations is Waltz's *Theory of International Politics*. It addresses the state as the fundamental unit within the international system. Keohane's Neoliberal Institutionalism and Wendt's *Social Theory of International Politics* also takes the state as the major unit of interest within the system. These scholars are cognizant of the implications of their choice, and to great extent states are, in fact, important within the system. But they are not the only units, and these theories do not address the gap left in systemic theorizing by leaving unexamined other actor types. Theories addressing states as the unit of analysis are inadequate for formulating national security policy in the altered security environment. This study proposes the security environment be perceived in terms of a Red, Gray, and Blue framework, or paradigm.

The study begins this task below with a clarification of conceptual terms, because progress is best made by using precise concepts and terminology. It is a conceptual analysis of what is demanded from a security environment approach to national security policy countering emerging threats targeting critical infrastructure. This articulation of a paradigm creates a framework adequate to encompass the changed nature of the security environment. This paradigm – Red, Gray, and Blue – has three principle components: Self (Blue), Threat (Red), and Environment (Gray). From the perspective of the Red, Gray, and Blue framework, the study explicates a typology of emerging threats that enables creating theories and pure-type models of non-state actors or states emulating non-state actors for deceptive purposes.

The hierarchy of intellectual tools, from highest order of abstraction to the lowest runs: paradigm, theory, and then model. There is significant debate on what these terms mean, and some scholars use them differently and inconsistently even within a single work. If this study is to avoid similar confusion, it is necessary to first briefly make clear what is meant by the terms paradigm,

[17] Ibid, p. 118.

theory, and model, and detail the relations between the different elements in order to cogently present its argument.

Paradigm:

In his classic work *The Structure of Scientific Revolutions* Thomas Kuhn outlines how science proceeds in a cyclical fashion, with periods of continuity – stasis – within a research community being punctuated by the subversion, and eventual replacement, of the community's paradigm. Kuhn argues this change constitutes a scientific revolution, which redefines the community's standards, valid research problems, and permissible solutions. These and other commitments of the research community to some extent self-define that community and specify the topics comprising the research field, and, by implication, those that do not.[18] The US national security policy elite constitute such a community.

Research findings that do not conform to a community's paradigm – anomalies – are important because they are not just factual findings in their implications. Anomalies potentially signal research findings that may challenge the community's existing paradigm, and lead to a scientific revolution. During such a scientific revolution, our understanding of the world is fundamentally altered, as the old paradigm is replaced with a new paradigm that results in a quite different understanding of the world.

One example of the overthrow of an established paradigm cited by Kuhn is the work of Copernicus. The Ptolemaic system was a geocentric paradigm, or framework, of the heavens with Earth occupying the central position. Until its downfall as the dominant paradigm in the field of astronomy, the geocentric system was taught as an article of faith on the level of religious dogma, with the acknowledged order of the planets arranged as the Earth, Moon, Mercury, Venus, Sun, Mars, Jupiter, and Saturn. Beginning in 1497, however, Copernicus began astronomical observations that led him to become dissatisfied with the Ptolemaic system of the heavens. In 1543, Copernicus published his *De revolutionibus orbium coelestium libri VI* in which he set forth a paradigm of a heliocentric system in which the planets revolved around the sun. His paradigm of the heavens eventually proved simpler and more accurate in both describing and predicting the locations of celestial bodies than the Ptolemaic paradigm. It, however, contradicted Aristotle, who had asserted the static nature of Earth, broke with Ptolemy's accepted framework, and additionally inherently contained two radical premises. First, observations of the stars showed that they remained in fixed positions, yet if the Earth revolved

[18] Kuhn, *The Structure of Scientific Revolutions*, p. 7.

around the sun, the stars should shift in their positions according to the movement of the Earth. If Copernicus' model was correct, then the stars must then necessarily be far more distant than previously imagined, with the concomitant imperative that the universe was immensely larger than thought by scholars perceiving the heavens through Ptolemaic lenses. Second, Aristotle had taught that the phenomenon of falling was due to objects seeking their natural place at the center of the universe. As Copernicus was arguing that the Earth was not the center of the universe, what force could explain falling objects? This puzzle, of course, eventually led to the Newtonian conception of gravity.[19]

The Copernican revolution is an example of altering perception of the world through shifting paradigms. The physical universe and its arrangement remained the same both before and after publication of Copernicus' *magnum opus*. The objects perceived did not alter, but rather *how* they were perceived changed. Kuhn employs the metaphor of a *gestalt* to illustrate this altered perception:

> One perceptive historian, viewing a classic case of a science's reorientation by paradigm change, recently described it as "picking up the other end of the stick," a process that involves "handling the same bundle of data as before, but placing them in a new system of relations with one another by giving them a different framework." Others who have noted this aspect of scientific advance have emphasized its similarity to a change in visual gestalt: the marks on paper that were first seen as a bird are now seen as an antelope, or vice versa. That parallel can be misleading. Scientists do not see something *as* something else; instead, they simply see it. ...In addition, the scientist does not preserve the gestalt subject's freedom to switch back and forth between ways of seeing. Nevertheless, the switch of gestalt, particularly because it is today so familiar, is a useful elementary prototype for what occurs in full-scale paradigm shift.[20]

Copernicus placed the heavens in "a new system of relations with one another by giving them a different framework." Anomalies – facts – documented from his observations did not correspond to the Ptolemaic paradigm, and only when the paradigmatic lens was altered did the heavens fall into their orbits first for Copernicus, and then for 16th century astronomers and, ultimately, the world. Suppe called what Kuhn would understand as a paradigm a *Weltanschauung*, or "an exceedingly complex entity, being approximately the whole of one's background, training, experience, knowledge, beliefs, and intellectual profile which is of possible relevance to working with a theory."[21] *Weltanschauung* is in its philosophical and political context translated, literally, as "world view."[22]

---

[19] Thomas S. Kuhn, *The Copernican Revolution: Planetary Astronomy in the Development of Western Thought* (Cambridge, MA: Harvard University Press, 1957).
[20] Kuhn, *The Structure of Scientific Revolutions*, p. 85.
[21] F. Suppe, "The Search for Philosophic Understanding of Scientific Theories," in F. Suppe, ed., *The Structure of Scientific Theories* (Urbana: University of Illinois Press, 1974), p. 218.
[22] *Pons Collins Großwörterbuch für Experten und Universität Deutsch-Englisch Englisch-Deutsch (Stuttgart: Ernst Klett Verlag, 1997), p. 766.*

The importance placed by Suppe on training, knowledge and other aspects of intellectual profile in the composition of a worldview parallels a major point of emphasis by Kuhn. As cited in this chapter's epigraph "education is both rigorous and rigid," and this rite of passage into the community of an academic discipline serves to influence the world view – paradigm – of scholars within that school of thought.

Kuhn defines a paradigm as "what the members of a scientific community share."[23] In his 1969 postscript to *The Structure of Scientific Revolutions* he states that the term theory "connotes a structure far more limited in nature and scope" than that of paradigm. The term paradigm is used in two ways by Kuhn: "On the one hand, it stands for the entire constellation of beliefs, values, techniques, and so on shared by the members of a given community. On the other, it denotes one sort of element in that constellation, the concrete puzzle-solutions which, employed as models or examples, can replace explicit rules as a basis for the solution of the remaining puzzles of normal science."[24] Kuhn's dual usage corresponds to two lay definitions of paradigm, as "a philosophical and theoretical framework of a scientific school or discipline within which theories, laws, and generalizations and the experiments performed in support of them are formulated," and "an outstandingly clear or typical example or archetype," respectively.[25] Kuhn's first meaning he titles a "disciplinary matrix," which encompasses a community's common theoretical, methodological, evaluative, assumptive, and other commitments framing a world view. His second meaning is that of an "exemplar" that defines by example the elements in the framework, or disciplinary matrix.

Kuhn employed the term paradigm as the core concept in arguing that science changes through fundamental shifts in the paradigm supporting scientific study during particular ages. This makes for a periodization of science that accords to shifts in the paradigm; "a succession of tradition-bound periods punctuated by non-cumulative breaks."[26] Kuhn's concept of "scientific revolution" has had wide influence.[27] However, his use of the term paradigm excited considerable controversy and confusion over what exactly he and the term meant. Masterson, in her "The Nature of a Paradigm," cites Kuhn himself as a contributing source of the confusion. She observes Kuhn uses the term "paradigm" in at least twenty-one different senses, and she details the meaning for each of the senses.

---

[23] Kuhn, *The Structure of Scientific Revolutions*, p. 176.
[24] Ibid, p. 175.
[25] *Merriam-Webster's Collegiate Dictionary*, 10th ed. (Springfield, MA: Merriam-Webster, 1998), p. 842.
[26] Kuhn, *The Structure of Scientific Revolutions*, p. 208.
[27] See Janet Buttolph Johnson and Richard A. Joslyn, *Political Science Research Methods*, 3rd ed. (Washington, DC: CQ Press, 1995), pp. 29, 38, for an example where the concept of "scientific revolution" is treated as a fundamental concept for political scientists.

Of these, the first and third senses are the most relevant for the purpose of this study: "(1) as a universally recognized scientific achievement (p. x): '[Paradigms] I take to be universally recognized scientific achievements that for a time provide model problems and solutions to a community of practitioners'. ...(3) As a 'philosophy', or constellation of questions (pp. 4-5): '[No] scientific group could practise [sic] its trade without some set of received beliefs. Nor does it make less consequential the particular constellation to which the group, at a given time, is in fact committed. Effective research scarcely begins before a scientific community thinks it has acquired firm answers to questions like the following: What are the fundamental entities of which the universe is composed? How do these interact with each other and with the senses? What questions may legitimately be asked about such entities and what techniques employed in seeking solutions?'"[28]

In his "Postscript – 1969," Kuhn acknowledges that he was loose in employing the term paradigm.[29] To clarify his meaning for his critics, he delineated two main senses in which one can view a paradigm. Kuhn states "in much of the book the term 'paradigm' is used in two different senses. On the one hand, it stands for the entire constellation of beliefs, values, techniques, and so on shared by the members of a given community. On the other, it denotes one sort of element in that constellation, the concrete puzzle-solutions which, employed as models or examples, can replace explicit rules as a basis for the solution of the remaining puzzles of normal science."[30] The first sense Kuhn names a *disciplinary matrix*, and the second sense he titles an *exemplar*.

Suppe more simply notes "Kuhn admits that his use of 'paradigm' confuses and identifies two quite distinct notions: *exemplars*, which are concrete problem solutions accepted by the scientific community as, in a quite usual sense, paradigmatic; and *disciplinary matrixes*, which are the shared elements which account for the relatively unproblematic character of professional communication and the relative unanimity of professional judgment in a scientific community, and have as components symbolic generalizations, shared commitments to beliefs in particular models, shared values, and shared exemplars."[31]

---

[28] Margaret Masterman, "The Nature of a Paradigm," in Imre Lakatos and Alan Musgrave, eds., *Criticism and the Growth of Knowledge* (Cambridge: Cambridge University Press, 1970), pp. 61-62; the page numbers in parentheses within Masterman's quote cite the location of Kuhn's quotes in Kuhn, *The Structure of Scientific Revolutions*.
[29] Thomas S. Kuhn, "Postscript – 1969," in *The Structure of Scientific Revolutions*, 2nd ed. (Chicago: The University of Chicago Press, 1970), pp. 174-176.
[30] Kuhn, "Postscript – 1969," p. 175.
[31] Suppe, p. 138.

In his essay "Second Thoughts on Paradigms," Kuhn answers criticism of his treatment of paradigms in *The Structure of Scientific Revolutions*.[32] Kuhn does not depart from his original core usages of the term, but rather further refines them conceptually, albeit still not tightly organized or delineated. His discussion clarifies that he meant the term paradigm in his previous work in two general senses: as a *disciplinary matrix* and as an *exemplar*. The first sense is "global, embracing all the shared commitments of a scientific group; the other isolates a particularly important sort of commitment and is thus a subset of the first."[33] Yet, later in naming the three "constituents" of the disciplinary matrix, he names symbolic generalizations, models, and exemplars. Thus we find that Kuhn's third constitutive element of a disciplinary matrix, the exemplar, is simultaneously the second major sense in which he employs the term paradigm; in other words, the third element within the first sense of Kuhn's use of the term paradigm is also the second sense of how he employs the term.

Viewing this organization in outline form points out the inherent circularity of using a sub-element from the first sense to constitute the second sense of the major usage of the term paradigm.

1) The First Kuhnian Sense of Paradigm: "global, embracing all the shared commitments of a scientific group." Entitled the *disciplinary matrix*, it is composed of three elements:

a) Symbolic Generalizations.

b) Models.

c) Exemplars (see Second Kuhnian Sense of Paradigm).

2) The Second Kuhnian Sense of Paradigm: "isolates a particularly important sort of commitment and is thus a subset of the first." Entitled the *exemplar*, it is a "concrete problem solution." (see First Kuhnian Sense of Paradigm, sub-element c).

If one is using a term in a "second sense" that is encompassed within the "first sense," by one's own explicit definition of the "first sense," isn't one just using the term in its first sense? This circularity is not necessarily fatal to making his point; it is just poor organization of presentation, and doesn't need to be belabored. It does, however, mean that Kuhn is focusing on a concept of paradigm which possesses multiple, constitutive elements, and that he has focused on one sub-element in substantive detail, the exemplar, while consigning the remaining elements to a separate, more abstract usage of the term paradigm. Unfortunately, Kuhn does not specify in his "Second Thoughts on Paradigms" or his other essays where theories fit into this picture. Below Lakatos will amend this oversight.

---

[32] Thomas S. Kuhn, "Second Thoughts on Paradigms," in Frederick Suppe, ed., *The Structure of Scientific Theories* (Chicago: University of Illinois Press, 1974), p. 459-482.
[33] Kuhn, "Second Thoughts on Paradigms," p. 460.

The concept of paradigm is a macro-level, meta-theoretical concept. As noted, scholars often cite as an example of two different paradigms the Copernican heliocentric system vis-à-vis the Ptolemaic geocentric system. The two paradigms constitute antithetical views of how the universe is ordered. From these diametrically opposed views, different theories describing, explaining, and predicting the movement of the planets are created. Lakatos' "hard core," from this perspective approximates a paradigm, as in Kuhn's disciplinary matrix, the first sense of his use of paradigm.[34] Lakatos notes: "Indeed...*my concept of a 'research programme' may be construed as an objective, 'third world' reconstruction of Kuhn's socio-psychological concept of paradigm.*"[35] Similarly, Lakatos' concept of a "problemshift" when he uses it in a meta-theoretic sense corresponds to Kuhn's "paradigm shift," or "gestalt switch." The principle difference between Kuhn's "paradigm shift" and Lakatos' progressive "problemshift" is that Lakatos sees "scientific revolutions [note that Lakatos here is, quite consciously and explicitly, using Kuhn's term of "scientific revolution"] as constituting rational progress rather than as religious conversions."[36] Kuhn, of course, sees them as rapid changes, but he does not take issue with them being rational, as Lakatos notes.

One can better understand Lakatos' argument concerning the structure of research programs by considering the image of four nested, concentric spheres. Working from the center out, 1) the innermost sphere is the "hard core," or tenets, of the "paradigm," which Lakatos names a research program. He states a research program is constituted of a "series of scientific theories. The most important such series in the growth of science are characterized by a certain continuity which connects their members. This continuity evolves from a genuine research programme adumbrated at the start." The "hard core" is the foundational tenets, the framework, within which adumbration proceeds. Whether one believes the sun or the earth is the center of the solar system is a tenet of a research program within its hard core. 2) The next outer sphere is a shield around the hard core beliefs of the community, called by Lakatos the "negative heuristic" that protects the hard core from challenge by its own hypotheses. This negative heuristic prevents the development of hypotheses and theories that are not true to the core tenets, and thus not representative of the paradigm. Thus, a theory that purports to

---

[34] "Recall that Lakatos argues that research programs have four elements: a hard core consisting of unchanging, privileged knowledge; a negative heuristic which forbids that knowledge from being directly challenged; a protective belt of auxiliary hypotheses, which 'bear the brunt of tests and get adjusted and re-adjusted, or even completely replaced, to defend...the core'...and a positive heuristic that 'guides the production of specific theories within the programme'" in Colin Elman and Miriam Fendius Elman, "Lakatos and Neorealism: A Reply to Vasquez," *The American Political Science Review*, Vol. 91, No. 4 (December 1997), p. 924.

[35] Imre Lakatos and Alan Musgrave, eds., *Criticism and the Growth of Knowledge* (Cambridge: Cambridge University Press, 1970), p. 179. Original italics.

[36] Imre Lakatos, "Falsification and the Methodology of Scientific Research Programmes," in Lakatos and Musgrave, *Criticism and the Growth of Knowledge*, p. 91.

be within the Realist paradigm will evidence traits characteristic of other Realist theories and models, because they were all created on the foundation of the Realist hard core. Should it contradict the paradigm's hard core tenets, for example by espousing classically Utopian arguments, one would hardly call it a "Realist theory." Lakatos states the "negative heuristic of the programme forbids us to direct the *modus tollens* at this 'hard core.'"[37] *Modus tollens*, as a fundamental rule of formal logic refers to inferences of the form A ⊃ B (in which ⊃ signifies the causal statement "If . . . then"); ~B, therefore, ~A (~ signifies "not"). Lakatos' explicit admonition that *modus tollens* could not be turned against the hard core is recognition that failure of a hypothesis does not falsify the paradigm, but only a hypothesis. This is further articulated by Lakatos in his description of the next outer sphere of a paradigm, but an example may illustrate the point. Adopting as one's perspective the heliocentric paradigm, one could mistakenly form a hypothesis that the earth rotates around the moon. When observation falsified this hypothesis, however, that would not call into question the higher level abstraction of the heliocentric paradigm, or hard core. The error of a hypothesis does not falsify the paradigm. 3) The next sphere is a belt of dynamic hypotheses and theories that describe, explain, and predict reality as viewed from the perspective of the hard core's tenets. These hypotheses and theories describe, explain, and predict the world from the perspective of and founded upon the paradigm's tenets. Should a hypothesis be proven false, Lakatos' observation of the inappropriateness of directing *modus tollens* against the hard core requires that *modus tollens* instead be directed against the theories and hypotheses in this protective belt. He notes "we must use our ingenuity to articulate or even invent 'auxiliary hypotheses', which form a *protective belt* around this core, and we must redirect the *modus tollens* to these. It is this protective belt of auxiliary hypotheses which has to bear the brunt of tests and get adjusted and re-adjusted, or even completely replaced, to defend the thus-hardened core."[38] Lastly, 4) The outer sphere represents the "positive heuristic" that allows development and testing of specific hypotheses, and, in turn, theories, in response to puzzles. In this fashion newly found data discovered during research, if found viable, can be subsumed through the mechanism of the positive heuristic into the protective belt of hypotheses as new hypotheses that further the progressive evolution of a research program. Unexplained anomalies, or puzzles, do not challenge the paradigm, or hard core, in the short- to mid-term. This is because the positive heuristic prescribes the order of research within the research program. It "consists of a partially articulated set of suggestions or hints on how to change, develop the 'refutable variants' of the research-programme...the positive heuristic of the programme saves the scientist from becoming confused by the ocean of anomalies."[39]

---

[37] Ibid, p. 133.
[38] Ibid. Original italics.
[39] Ibid, p. 135.

The Lakatosian negative heuristic, protective belt, and positive heuristic describes the work of Kuhnian "normal science." Furthermore, a degenerative Lakatosian problemshift is equivalent to a Kuhnian paradigmatic pre-crisis stage. Abandonment of a research program constitutes a change for both Lakatos and Kuhn. Although Lakatos and Kuhn do differ on several points, the principal differences between the two, for example the speed and nature of change (Lakatos sees it as a slow, deliberate process, Kuhn as a potentially rapid, akin to "gestalt switch" process), do not make their explanations of paradigms (research programs) incompatible, or even significantly different upon detailed study. Lakatos can be understood to have refined and added to Kuhn's earlier concept, or as he notes "Where Kuhn sees 'paradigms', I *also* see rational 'research programmes'."[40] The similarity between the two is acknowledged several times by Lakatos, for example "...theories are usually connected by a remarkable *continuity* which welds them into *research programmes*. This *continuity* - reminiscent of Kuhnian 'normal science'-plays a vital role..."[41]

Kuhnian normal science is the practice of the research community within a paradigm established and accepted by its members. It is this established paradigm, and the reticence of community members long familiar with it, that hampers the emergence of a new paradigm during a paradigmatic crisis. Kuhn states that "[n]ormal science...often suppresses fundamental novelties because they are necessarily subversive of its basic commitments."[42] Crafting security policies to deal with fundamentally novel threats within the old paradigm is an example of Kuhnian normal science's resistance to new paradigms.

Resuming the discussion of Realism, Stephen Van Evera and Robert Gilpin both make the point that Realism is not a theory, but an overarching paradigm within which multiple "realist" theories exist. This makes Realism, capital "R," a broad, flexible perspective that is not constrained to the necessarily more narrow perspective of a specific theory within the paradigm, such as Neorealism.[43] Hard core tenets of the Realist paradigm can endure, even when realist, lower-case "r," theories fade. This is because there exists both continuity and change in the world. Elements of continuity can survive even across paradigm shifts. But intellectual tools, like theories, also change to reflect change in reality.

---

[40] Ibid, p. 177. Original italics.
[41] Ibid, pp. 131-132. Original italics.
[42] Kuhn, *The Structure of Scientific Revolutions*, p. 5.
[43] See Stephen Van Evera, "Elements of the Realist Paradigm: What Are They?" typescript, 27 January 1992, p. 4. as cited in Benjamin Frankel, *Realism: Restatements and Renewal* (London: Frank Cass, 1996), p. xiii, and Robert G. Gilpin, "No One Loves a Political Realist," *Security Studies*, Vol. 5, No. 3 (Spring 1996), pp. 3-26.

An example of an element of the Realist paradigm's hard core, which Lakatos would consider "unchanging, privileged knowledge" would be the concept of anarchy as characteristic of the world political system. One must understand a paradigm's core tenets before one can evaluate the perspective, particularly in light of change in the reality it frames. Realism, of course, traces its research program back to ancient times. Commonly cited founders of the Realist perspective include Thucydides, Kautilya, Machiavelli, Hobbes, and others. The basis of Realism's claim to ancient lineage is founded on a common paradigm shared by these and other political philosophers.

Scholars such as Carr, Spykman, Niebuhr, Morgenthau, and Kissinger incorporated into their work the thoughts of the ancient world's realists. Contemporary scholars, like Mearsheimer, Waltz, Grieco, Gilpin, Lynn-Jones, and others believe elements of the Realist paradigm that would be familiar to Thucydides continue to have value for understanding the world.[44] The common, continuing elements of view shared by these scholars stem from the enduring, hard core of the Realist paradigm. This section reviews key perspectives of Realism's core tenets. It then adopts a concise listing of these enduring tenets, which undergird discussion in Chapter 3 and Chapter 4.

E.H. Carr sees as two fundamental components of the Realist perspective the concepts of power and state. He also makes one of the most lucid statements on the utility of using the political construct "*state*" to be found in Realist literature:

> On power, Carr believes:
>
> > Political power in the international sphere may be divided, for purposes of discussion, into three categories: (a) military power, (b) economic power, (c) power over opinion. We shall find, however, that these categories are closely interdependent; and though they are theoretically separable, it is difficult in practice to imagine a country for any length of time possessing one kind of power in isolation from the others. In its essence, power is an indivisible whole.[45]

Carr's insights into power are from a state-centric perspective. As this dissertation is concerned with non-state actors, we can see beyond the contextual allusions to states to understand that power, as seen by Carr, involves violent, financial, and socio-political or informational forms. The forms of power are interdependent, and in this aspect, the degradation of one form results in a corresponding degradation in the "indivisible whole" of an actor's power. Carr remarks specifically on the notion of military power and war, as the form of violent power:

> > The supreme importance of the military instrument lies in the fact that the *ultima ratio* of power in international relations is war. Every act of the state, in its power

---

[44] See especially Robert Gilpin, *War and Change in World Politics* (New York: Cambridge University Press, 1981), pp. 3, 10, 13.
[45] E.H. Carr, *The Twenty Years' Crisis, 1919-1939* (New York: Harper Torchbooks, 1964), p. 108.

> aspect, is directed to war, not as a desirable weapon, but as a weapon which it may require in the last resort to use.[46]

Carr's concept of power is not a primitive understanding limited to naked violence, although he accepts violence as the ultimate base of power. Instead, he argues that the employment of violence is a means of last recourse, hence its "supreme importance." This necessarily means that other instruments of power are available for employment prior to the resort to force, as well as presumes that the other means are suitable for obtaining the ends desired. The first presumption deals with feasibility, the second with suitability. The third presumption any actor must critically examine prior to the deliberate employment of violence is its acceptability. Due to its inherent costs and risks for all parties, violence will typically not be employed until an actor has exhausted less self-debilitating means to reach its ends. Where the three assumptions of feasibility, suitability, and acceptability are met, an actor will likely employ violence as a means to an end.

Carr explains the utility of using the state as a reified actor or anthropomorphism in a forceful statement. This study is concerned with non-state actors, however Carr's statement also serves to point out a common misunderstanding that the Realist research program is tied inextricably to the political construct of the state:

> ...controversy about the attribution of personality to the state is not only misleading, but meaningless. To deny personality to the state is just as absurd as to assert it. The personality of the state is not a fact whose truth or falsehood is a matter for argument. It is what international lawyers have called 'the postulated nature' of the state. It is a necessary fiction or hypothesis-an indispensable tool devised by the human mind for dealing with the structure of a developed society...The fiction of the group-person, having moral rights and obligations and consequently capable of moral behaviour, is an indispensable instrument of modern society; and the most indispensable of these fictitious group-persons is the state. In particular, it does not seem possible to discuss international politics in other terms." [Carr then footnotes: "This does not, of course, mean that the state is a necessary form of political organisation, but only that, so long as the state *is* the accepted form, its personification is a necessary fiction. The same would apply to any other form (e.g. the class). The personification of the proletariat has gone far in Soviet Russia, e.g. the fiction that it 'owns' the means of production.][47]

Carr's explicit recognition, as Morgenthau's below, that other forms of actor are acceptable within Realist theorizing is very important for this study. It means that identification of a particular actor type is absolutely not contained within the Realist paradigm's hard core. Instead, specification of actor type is contained within the Lakatosian research program's protective belt of hypotheses and theories, which bear the brunt of adjustment and even abandonment. One of this study's key

---

[46] Ibid, p. 109.
[47] Ibid, p. 149.

arguments is that non-state actors capable of system relevant violence are not only "major actors," but important to account for in a paradigm of world politics. This argument is not incompatible with classic, enduring elements of the Realist philosophy. Where hypothesis and theory does not conform to reality, they must be altered to fit reality. This does not mean the theories and hypotheses are without value; it only means they are without value to explain that particular reality. For example, a theory of the international political system that views states as the primary actors may apply to that reality, but it does not apply, by definition, to a world that includes non-state actors. The reality of world politics changes over historic periods, as Kuhn noted in his concept of paradigmatic periodization, and theory must change to explain the new realities of the world. Morgenthau and Carr, both classical realists, agree that the state is not an eternal component of the Realist perspective, and that inclusion of a different actor is possible within the paradigm. Morgenthau, an icon of classical Realism and an undeniable authority on the point, notes:

> Nothing in the realist position militates against the assumption that the present division of the political world into nation states will be replaced by larger units of a quite different character, more in keeping with the technical potentialities and the moral requirements of the contemporary world. The realist parts company with other schools of thought before the all-important question of how the contemporary world is to be transformed.[48]

The importance of both Carr's and Morgenthau's explicit positions that the state is not the only actor of potentially major theoretical interest within the Realist research program is that in accordance with the Lakatosian research design model, Realism's positive heuristic can adapt to a world where actors other than states are key without this constituting a modification of a core tenet. This has implications for whether Realism can be considered a "progressive" or "degenerative" research design in the Lakatosian sense, as well as how enduring is Realism's Kuhnian paradigm. Misunderstanding of this point has lead many to question the validity of the Realist research program in a contemporary environment where actors other than states are becoming relevant.

Morgenthau's position on power is a two-step rationale. Like Carr's concept of power, it is sophisticated. First:

> The main signpost that helps political realism to find its way through the landscape of international politics is the concept of interest defined in terms of power. This concept provides the link between reason trying to understand international politics and the facts to be understood. It sets politics as an autonomous sphere of action and understanding apart from other spheres, such as economics (understood in terms of interest defined as wealth), ethics, aesthetics, or religion.[49]

---

[48] Hans J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*, 4th ed. (New York: Alfred A. Knopf, 1967), p. 9.
[49] Ibid, p. 5.

And, second:

> Its [power's] content and the manner of its use are determined by the political and cultural environment. Power may comprise anything that establishes and maintains the control of man over man. Thus power covers all social relationships which serve that end, from physical violence to the most subtle psychological ties by which one mind controls another. Power covers the domination of man by man, both when it is disciplined by moral ends and controlled by constitutional safeguards, as in Western democracies, and when it is that untamed and barbaric force which finds its laws in nothing but its own strength and its sole justification in its aggrandizement.[50]

Both Carr's and Morgenthau's concepts of state and power are not uni-dimensional. This concept of power within the Realist paradigm, like that of state, is sometimes deeply misunderstood. The Realist school views coercive, physical violence as the *ultima ratio*, but this does not mean that it accepts that violence is the only element of power that can influence. A thorough reading of key Realists, as the quotes above make clear, exposes these misunderstandings. Especially important is Morgenthau's insight that power is involved with *"social relationships."* Support of Morgenthau's insight that power even extends to "the most subtle psychological ties by which one mind controls another" is found in a, to some, unexpected corner. Wendt agrees with Morgenthau's insight, stating that "Self-help and power politics are institutions, not essential features of anarchy. *Anarchy is what states make of it.*"[51] This is a critical insight for understanding the new security environment and the role of non-state actors within it.

Addressing the entire core of Realism's tenets, Sean M. Lynn-Jones and Steven E. Miller outline what they see as six key principles:

> First, realists believe that states are the most important actors in international politics. They therefore focus on explaining the behavior of states and tend to pay less attention to individuals and transnational actors like corporations and multinational organizations. Second, realists regard anarchy-the absence of any common sovereign-as the distinguishing feature of international life. Without a central authority to enforce agreements or to guarantee security, states must rely on their own means to protect their interests. Third, realists assume that states seek to maximize either their power or their security. Some realists focus on power as an end in itself, whereas others regard it as a means to security. Fourth, realists usually assume that states generally adopt rational policies that aim to achieve power and/or security. Fifth, realists normally agree that states will tend to rely on the threat or use of military force to secure their objectives in international politics. Sixth, most realists believe that aspects of the international system - especially the distribution of power among states - are the most important causes of the basic patterns of

---

[50] Ibid, p. 9.

[51] Alexander Wendt, "Anarchy is What States Make of It: The Social Construction of Power Politics," *International Organization*, Vol. 46, No. 2 (Spring 1992), p. 395. Original italics.

> international politics and foreign policy. Although realists may recognize that state-level factors matter, they emphasize the importance of international factors.[52]

From this list, especially the first, fifth, and sixth points concerning actor, use of force, and systemic influence, respectively, it is apparent that Lynn-Jones and Miller have erroneously modeled the core tenets of Realism from a contemporary theory's perspective. Their statements are strongly influenced by the realist theory, lower-case "r," of Neorealism, as opposed to the enduring thoughts of the classical research program, which more capably captured the paradigmatic framework. As such, they mistake theory for paradigm. Additionally, the definitive tone of their list is bought at the price of leaving behind sophisticated insights, like Carr's and Morgenthau's views of the state as just one possible actor-type and how different elements collectively constitute power, as well as Wendt's contribution to viewing power and interest as having components of social construction. Lynn-Jones and Miller aim, but fail, to hit the hard-core of Realism. They have instead described the larger research program, perhaps unwittingly, from the more narrow, specific, and subordinate perspective afforded by Neorealist lenses.

Randall Schweller cites seven propositions that in his view comprise the core of the Realist perspective:

> In my view, the 'hard core' of the realist school of thought consists...of seven propositions...about international politics. (1) Humans do not face one another primarily as individuals but as members of groups that command their loyalty. (2) International affairs take place in a state of anarchy. (3) Power is the fundamental feature of international politics; it is the currency of international politics required to secure any national goal, whether world mastery or simply to be left alone. (4) The nature of international interaction is essentially conflictual: 'A world without struggle would be a world in which life had ceased to exist'. (5) Humankind cannot transcend conflict through the progressive power of reason to discover a science of peace. (6) Politics are not a function of ethics; morality is the product of power. (7) Necessity and reason of state trump morality and ethics when these values conflict.[53]

Schweller's propositions return to the sophistication of Carr and Morgenthau regarding actor and power. He, however, adopts Spykman's view that a "world without struggle would be a world in which life had ceased to exist,"[54] or, in other words, embraces a thoroughly and exclusively Hobbesian world view of "warre of every man against every man."[55] This misses Wendt's insight that other

---

[52] Michael E. Brown, Sean M. Lynn-Jones, and Steven E. Miller, eds, *The Perils of Anarchy: Contemporary Realism and International Security* (Cambridge, Massachusetts: The MIT Press, 1995) pp. ix-x.

[53] Randall L. Schweller, "New Realist Research on Alliances: Refining, Not Refuting, Waltz's Balancing Proposition," *The American Political Science Review*, Vol. 91, No. 4 (December 1997), p. 927. Ancillary footnotes internal to the quote have been omitted.

[54] Nicholas John Spykman, *America's Strategy in World Politics: The United States and the Balance of Power* (New York: Harcourt Brace, 1942), p. 12, as cited in Schweller.

[55] Thomas Hobbes, *Leviathan* (London: Penguin, 1985), p. 188.

anarchies are possible. The fact of the matter is, although conflict is possible, so is peace. Asserting the nature of international interaction is essentially conflictual is not any more true or false than stating it is essentially peaceful. It can be both, and how two actors define their interests influences whether relations are peaceful or not. Morgenthau stated that interests defined in terms of power constituted the essential nature of politics, which suggests that only if one was to argue the extreme position that power, hence interests, is always served by conflict could the essential nature of interactions, international or otherwise, be conflictual, as Schweller believes.[56] The Realist research program does accept that force is the *ultima ratio*, but that is an entirely different statement than the assertion "[t]he nature of international interaction is essentially conflictual."

For a perspective that is quintessentially classical, one must look beyond Neorealism. Morgenthau proposes six principles of Realism:

> 1. Political realism believes that politics, like society in general, is governed by objective laws that have their roots in human nature.
> 2. The main signpost that helps political realism to find its way through the landscape of international politics is the concept of interest defined in terms of power.
> 3. Realism assumes that its key concept of interest defined as power is an objective category which is universally valid, but it does not endow its key concept of interest defined as power with a meaning that is fixed once and for all. The idea of interest is indeed of the essence of politics and is unaffected by the circumstances of time and place.
> 4. Political realism is aware of the moral significance of political action. It is also aware of the ineluctable tension between the moral command and the requirements of successful political action. And it is unwilling to gloss over and obliterate that tension and thus to obfuscate both the moral and the political issue by making it appear as though the stark facts of politics were morally more satisfying than they actually are, and the moral law less exacting than it actually is.
> 5. Political realism refuses to identify the moral aspirations of a particular nation with the moral laws that govern the universe.
> 6. The difference, then, between political realism and other schools of thought is real, and it is profound. However much the theory of political realism may have been misunderstood and misinterpreted, there is no gainsaying its distinctive intellectual and moral attitude to matters political.[57]

As evident above, Morgenthau is less absolute than contemporary theorists on questions of what constitutes power, the form that actors can take, and the nature of politics.

From the discussion above a list of this study's hard core tenets can be created. They share much with the Realist school, but part with elements limited to the Cold War era's context of states as

---

[56] Morgenthau, *Politics Among Nations*, p. 5.
[57] Ibid, pp. 4-11.

the principal "major actors," the supremacy of the military instrument of power, and the view that the system is necessarily founded on conflict, thus rejecting a possibility of an "anarchical society."[58]

1. The world political system is anarchic, "defined as the absence of centralized authority,"[59] with survival the ultimate end of most actors. Different anarchies are possible because agents, in part, constitute the nature of their anarchy.[60]
2. Systemic actors are those that can employ power at a system relevant level.
3. The Third Image, the system, influences the First and Second Image systemic actors within it. Systemic actors, in turn, influence the Third Image.[61] Actors (agents) and Environment (structure) are interdependent and mutually constitutive.[62]
4. Systemic actors seek power and security.
5. First Image actors are, by definition, unitary. Second Image actors intend to be unitary, rational actors.[63] Rationality may be culturally based.
6. Violence is the *ultima ratio*, but other instruments of power (diplomatic, economic, informational, psychological, and social) are also effective means. Power extends to diverse instruments, from "physical violence to the most subtle psychological ties."[64] The specific end desired by an actor seeking power and security partially dictates the means required; other influences predicating means required are the actor's identity, other actors' capabilities and intents, and the security environment.
7. Distribution of power, relative gains, and ranking or position are important among Second Image actors. First Image systemic actors will tend to focus on absolute gains.
8. Necessity and reason for existence trump morality and ethics when these values conflict.

This study follows Kuhn's sense of paradigm as a disciplinary matrix. It accepts that the paradigm comprises a *Weltanschauung*, as noted by Suppe, which is shared by a particular professional community. The community of interest in this study is the US national security elite concerned with policy formulation to counter emerging threats to critical infrastructure and population. The common beliefs shared by a community of scholars in their collective *Weltanschauung* are encompassed within

---

[58] The term anarchical society is, of course, Hedley Bull's. Bull distinguished between system (interdependent elements within a whole), and a society (shared norms and interests). Bull believed that some cooperation based on shared ideas was possible. See Hedley Bull, *The Anarchical Society* (New York: Columbia University Press, 1977).
[59] Wendt, *Social Theory of International Politics*, pp. 246-247.
[60] Ibid, p. 247.
[61] Kenneth N. Waltz, *Man, the State, and War* (New York: Columbia University Press, 1954).
[62] Wendt, "The agent-structure problem in international relations theory," pp. 335-370.
[63] Wendt, *Social Theory of International Politics, p. 246.*
[64] Morgenthau, *Politics Among Nations*, p. 9.

the Lakatosian hard-core of that specific research program. The concept of power articulated by Morgenthau is followed. Both First Image and Second Image actors can exercise system relevant power, hence be systemic actors.

Theory:

Waltz states that "The longest process of painful trial and error will not lead to the construction of a theory unless at some point a brilliant intuition flashes, a creative idea emerges."[65] Kuhn agrees that theory is arrived at deductively and spontaneously, only sometimes hinted at by a deliberate, inductive methodology. He states:

> Sometimes the shape of the new paradigm is foreshadowed in the structure that extraordinary research has given to the anomaly...More often no such structure is consciously seen in advance. Instead, the new paradigm, or a sufficient hint to permit later articulation, emerges all at once, sometimes in the middle of the night, in the mind of a man deeply immersed in crisis. What the nature of that final stage is-how an individual invents (or finds he has invented) a new way of giving order to data now all assembled-must here remain inscrutable and may be permanently so. Let us here note only one thing about it. Almost always the men who achieve these fundamental inventions of a new paradigm have been either very young or very new to the field whose paradigm they change. And perhaps that point need not have been made explicit, for obviously these are the men who, being little committed by prior practice to the traditional rules of normal science, are particularly likely to see that those rules no longer define a playable game and to conceive another set that can replace them.[66]

Facts and theory are "not categorically separable."[67] Waltz maintains that "[r]ather than being mere collections of laws, theories are statements that explain them...Theories are qualitatively different from laws. Laws identify invariant or probable associations. Theories show why those associations obtain...Theories cannot be constructed through induction alone, for theoretical notions can only be invented, not discovered."[68] Had Copernicus proceeded inductively, he would have continued to amass observations – facts or data points – in the hope of discerning a pattern. In fact, Copernicus made a relatively small number of observations. They were enough, however, to prompt him to explore the possibility that the Ptolemaic paradigm was wrong, and to deduce a different paradigm. Policymakers have received sufficient data to determine the inadequacy of the underlying theories they consciously or unconsciously employ to craft security policy. Like Copernicus, they have no need for exhaustive, interminable studies. However, their inability to change their paradigm

---

[65] Waltz, *Theory of International Politics*, p. 9.
[66] Kuhn, *The Structure of Scientific Revolutions*, pp. 89-90.
[67] Ibid, p. 7.
[68] Kenneth N. Waltz, *Theory of International Politics*, p. 5.

forces them to adopt elaborate internalized, but irrelevant, emendations to their theories to justify the policy positions they adopt.

Waltz explains that theories can be framed in multiple ways. His *Man, the State, and War* sorted according to "images," where the causes of war were located in man (First Image), the state (Second Image), and the state system (Third Image).[69] His *Theory of International Politics*, however, is a "systemic" theory. Waltz argues that "[t]heories of international politics that concentrate causes at the individual or national level are reductionist; theories that conceive of causes operating at the international level *as well* are systemic."[70]

Wendt argues that Waltz is wrong, stating that he "has misconstrued what divides the two kinds of theory."[71] Wendt asserts structures cannot have effects apart from the traits and interactions of the actors within a system. He distinguishes two senses when a theory might be considered systemic: when the international system is either the dependent or independent variable. The dependent variable sense is when a theory seeks to explain state behavior in aggregate patterns, instead of the actions of an individual state. The independent variable sense entails a theory's emphasis of the causal "powers" of the international system's structure.[72] Wendt believes that what Waltz calls "systemic" theory concerns the "macro-structure" of international politics, while Waltz's view of reductionist theory is concerned with "micro-structure.[73]

Crafting a theory at different levels of analysis, as J. David Singer noted in his classic article "The Level of Analysis Problem in International Relations," has implications for what the theory is able to describe, explain, and predict.[74] Choosing a lower level of analysis increases descriptive richness and explanation of specific cases, while choosing a higher level of analysis increases understanding of the comprehensive dynamics and nature of the system. Moul agrees, and notes that "[t]he level-of-analysis problem is concerned with the choice and limitations of particular units of analysis."[75] Waltz's inclusion of the qualifier *"as well"* in discussing that systemic causes also be included with consideration of First or Second Image causes is the proper approach. However, Wendt

---

[69] Waltz, *Man, the State, and War*; see also Waltz, *Theory of International Politics*, p. 18.
[70] Waltz, *Theory of International Politics*, p. 18. Italics added.
[71] Wendt, *Social Theory of International Politics*, p. 12.
[72] Ibid, p. 11.
[73] Ibid, p. 12.
[74] J. David Singer, "The Level-of-Analysis Problem in International Relations," in Phil Williams, Donald M. Goldstein, and Jay M. Shafritz, eds., *Classic Readings of International Relations*, 2nd Edition (New York: Harcourt Brace College Publishers, 1999), pp. 105-119.
[75] William B. Moul, "The Level of Analysis Problem Revisited," *Canadian Journal of Political Science*, Vol. VI, No. 3 (September 1973), p. 494.

argues, Waltz does not deliver on this point, and instead focuses attention on structure at the expense of agent.[76] Waltz goes so far as to assert that for the purpose of systemic theorizing states can be considered functionally undifferentiated, or "like units."[77] This may not have been an unreasonable point of departure during the Cold War, when states were the "major actors" capable of exercising system relevant power. But it is no longer true. Policymakers, because they have not yet "demolished" their paradigmatic "prisons" have not escaped their "conceptual boxes." Because of this their subordinate theories hold that states are the major actors and that for purposes of serving as a foundation for policy, states can be considered like units. Wendt's insight that agents and structure are interdependent and mutually constitutive has yet to be fully understood by a community rigorously educated, as Kuhn observed, with Neorealism as the theory upon which national security policy *de facto* rests.

Van Evera defines theory as "general statements that describe and explain the causes of effects of classes of phenomena. They are composed of causal laws or hypotheses, explanations, and antecedent conditions. Explanations are also composed of causal laws or hypotheses, which are in turn composed of dependent and independent variables."[78] This concise definition is in line with Waltz's definition of theory as showing why associations obtain; "theories explain laws."[79] Theory can range from simple to complex constructions. When extremely vast in scope, theories approach the level of paradigms as ways of looking at the world, or sub-components of it. At the other end of the continuum, a very simple theory may resemble a law under the static conditions of *ceteris parabis*. This points out that distinctions in the hierarchy of intellectual tools are not sharply delineated, but at their boundaries begin to overlap.

To craft a theory one must be clear on what one wishes to explain, which level of analysis is appropriate, and the units of analysis one wishes to employ. Explanation is the primary purpose of theory, and confusion on any of the above points hampers explanation.[80] But theories inescapably are constructed from pre-existing paradigms. Critique and prescription of policy without the paradigmatic and theoretical foundations either implicitly or explicitly known to the reader is at best confusing and at worse counterproductive. An initial articulation of this study's hard core as a point of departure has

---

[76] Wendt, *Social Theory of International Politics*, p. 256.
[77] Waltz, *Theory of International Politics*, pp. 104-105.
[78] Van Evera, *Guide to Methods for Students of Political Science*, p. 7.
[79] Waltz, *Theory of International Politics*, pp. 5-6.
[80] J. David Singer, "The Level-of-Analysis Problem in International Relations," in Phil Williams, Donald M. Goldstein, and Jay M. Shafritz, eds., *Classic Readings of International Relations*, 2nd Edition (New York: Harcourt Brace College Publishers, 1999), p. 107; Stephen Van Evera, *Guide to Methods for Students of Political Science*, pp. 17-21; Waltz, *Theory of International Politics*, p. 6.

been stated above to make explicit the point of departure for addressing two closely related questions: 1. How can we understand the changed security environment theoretically?, and, 2. What are the implications of the changed security environment for national security policies countering emerging threats? Specifying one's paradigm is a necessary, but not sufficient, component of answers to the study's two questions. One must additionally specify one's theories. This is accomplished below.

Van Evera observes a theory is nothing more than a set of connected causal laws or hypotheses: "A 'theory' that cannot be arrow-diagrammed *is not a theory* and needs reframing to become a theory. (According to this criteria much political science 'theory' and 'theoretical' writing is not theory.)"[81]

One component of this study's second question concerning implications of the changed security environment for national security policy concerns vulnerability of Self.[82] This, in turn, leads to several questions the main one of which is "How has Self become more vulnerable to attacks by emerging threats?"

There are several possible explanatory hypotheses that collectively contribute to addressing this question. Some of them are:

1. The collapse of the Soviet Union, and the resulting change in the structure of the international system from the Cold War's bipolarity, destroyed patron-client relationships and freed potential threat actors from superpower control. The result was new states and non-state actors freed to pursue their own political agendas.
2. The loss of the Soviet Union's control of critical research and development, knowledge, its cadre of WME experts and technicians, facilities and equipment, oversight of client states' WME programs, and vast stocks of chemical, nuclear, biological, and radiological agents (CNBR) has led to global proliferation of and ready access to WME in global markets.
3. WME proliferation has provided hostile actors with weapons of potentially strategic effect. These actors may previously have possessed intent to attack the United States, but were constrained by their limited capabilities. Possession of WME means they now possess both intent and capability.
4. Knowledge and technological advances have enabled potential threats to conduct strikes directly against the United States. Advances in communications, encryption, steganography, and digital

[81] Stephen Van Evera, *Guide to Methods for Students of Political Science*, pp. 14-15.
[82] Throughout the study the terms Self and Other are used in Hegelian fashion, stemming from the celebrated "master-slave" dialectic in Chapter IV of his *Phenomenology of the Spirit*. See Leo Rauch and David Sherman, *Hegel's Phenomenology of Self-Consciousness* (New York: SUNY Press, 1999).

watermarking all allow command and control (C2) of distributed, covert operations on the Internet.

5. A single Superpower system presents a single, best target for those dissatisfied with the status quo of the world political system. By definition, a Superpower is active globally, a fact that inevitably increases exposure to and interaction with potentially hostile Others.
6. The increased interdependence and automation of the US critical infrastructure has increased its fragility and vulnerability, hence its value as a target.
7. Threats lack the scale of power to directly challenge the United States in conventional warfare or open conflict, thus making asymmetric, unconventional attacks the best feasible, acceptable, and suitable option. Information gives them their power, not forces.
8. Targeting US critical infrastructure avoids known U.S. strengths and attacks known weakness.

In narrative format this theory of how Self has become more vulnerable to attacks by emerging threats states that the Cold War approximated Kaplan's loosely bipolar system, with a concomitant division into ideological camps that were subject to superpower influence and control, especially in the arena of WME research and development. The collapse of this order freed two potent forces: the liberated minds of millions of individuals around the world anxious for political power, and the inventories, technologies, and knowledge of the former Soviet Union's and client states' massive WME programs. The freed peoples of the world formed into "new" (some of which are actually quite "old") political groups, some defined along ethnic or religious lines. Many groups are currently pursuing WME as either an "absolute" guarantor of their future political survival, or a potent means for furthering strategic ends. Many of these groups have historic meaning for the people they represent, and possess ideological, religious, or other reasons for viewing the United States' sole superpower status with suspicion. Other groups possess hostile intent towards the US based on past conflict or other motivations. The proliferation of WME provides these groups, whether newly-formed nations or transnational actors, either First Image or Second Image, with a capability for system-relevant violence. Groups capable of WME employment may view the US as a *de facto* hegemon hampering the achievement of their ends, a threat to their existence, as well as oppose the current world political system's *status quo* as illegitimate, and view the anonymous, asymmetric use of WME against the United States as both an effective and efficient means to their ends. The simultaneous increasing reliance of the United States on its increasingly fragile critical infrastructures, and the potentially catastrophic consequences of a successful strike, makes it a high-visibility and low-risk, soft target.

The above argument suggests the following variables and arrow-diagramed theory:

See also Jerome Bruner, *Acts of Meaning* (Cambridge, MA: Harvard University Press, 1990), pp. 99-103, 108-117.

a = Collapse of the Soviet Union; the antecedent condition for change in the international system structure, and loss of control of Soviet WME stocks, research, facilities, and expert cadre.

b = Change in the international system structure from bipolar to multipolar.

c = Number of state and non-state actors free of strict Superpower control following change in international system (this includes actors from both the former Soviet and US camps).

d = Loss of control of Soviet WME stocks and research. Simultaneous relentless advance in technology, information, and knowledge that reduces difficulty in pursuing WME research and development. Condition variable.

e = Loss of Superpower oversight of client states WME programs (again, both former Soviet and US camps). Condition variable.

f = Attainment by emerging threats of WME strategic attack capability against the United States. Dependent variable.

$$\therefore, a \Rightarrow b \Rightarrow c \Rightarrow f$$
$$\mathbf{X}$$
$$\Rightarrow d$$
$$\mathbf{X}$$
$$\Rightarrow e$$

This is not a quantitative study, yet variables in a qualitative study still must be defined, or operationalized. Operationalizing the above variables poses no significant challenge. The variables can be operationalized as follows:

b = Change in the international system structure from bipolar to multipolar. This is perhaps most easily demonstrated by the exercising of independent political activity by Eastern European countries, the rise of the EU, and the number of states in the UN pursuing different political agendas than they did during the Cold War.

One way to operationalize this variable is to count the number of independent nation-states within the Soviet Union's former sphere of influence now able to exercise independent balancing, bandwagoning, or other maneuvers. This, contrasted with a demonstrated lack of ability to conduct such maneuvers while within the Soviet empire will yield a before and after picture of how the number of actors has increased in the wake of the Soviet Union's collapse. Similarly, the U.S. sphere, while not as black and white, can also be analyzed. Did western European states change from a perfect, public track record of support for American security policy when confronting the Soviet Union, only to begin exercising more independence following the fall of the empire?

c = Number of state and non-state actors free to maneuver from strict Superpower control following the change in the international system (both Soviet and U.S. camps).

To operationalize this one must examine Soviet and American security or economic arrangements. Did the fall of the Soviet Union result in a movement away from Communist vs. Free World economic lines (bipolar) to a more regionalized trade grouping (multipolar)? Did the collapse of the Warsaw Pact result in an increased number of bilateral and regional security arrangements? That would also signal a bipolar to multipolar shift, which increases the number of state and non-state actors acting independently. The number of non-state actors maneuvering beyond Superpower control is apparent in the growing number of legitimate NGOs and also, based on belief, "illegitimate" non-state actors like Osama bin Laden's Al Qaida.

d = Loss of control of Soviet WME stocks and research. Condition variable.

This variable can be operationalized through numerous open sources. There exist extensive documented cases of proliferation. Additionally, there exists an extensive literature consisting of numerous proliferation journals, US House and Senate testimonies of subject matter experts, and other credible, openly published sources.[83]

e = Loss of Superpower oversight of client states WME programs (both U.S. and Soviet camps). Condition variable.

This variable is operationalized through post-Cold War open sources for evidence of former client state WME programs that were in existence during the Soviet Union's hegemony of the client state, but subsequently disbanded following the breakup of the Soviet Union. The resulting employment status

[83] For a representative publication see Sam Nunn, *Managing the Global Nuclear Materials Threat: Policy Recommendations* (Washington, DC: Center for Strategic and International Studies Press, 2000).

of the WME research cadre and the status of inventories, equipment, and facilities provides insight into whether the specific program potentially contributed to proliferation.

f = Attainment by state or non-state actor of WMD strategic attack capability. Dependent variable.

One way to operationalize this variable is to review various open sources including professional security and proliferation journals for documented evidence of WME capability by these actors. A case by case study of each actor is required. Another way is to review the continual, on-going testimony of security policy elites throughout the world for admission in open sources of these states or non-state actors possessing WMD and other details. Lastly, obviously, some actors have publicly demonstrated WME capability through test shots of nuclear weapons (India and Pakistan) or deployment of WME during conflict (Iraq during the Gulf War deployed at least chemical munitions forward). An extensively documented example of a non-state actor is Aum Shinrikyo.

This study accepts Van Evera's definition of theory. The purpose of this dissertation, however, is to answer two questions: how we can understand the changed security environment theoretically, and what are the implications of the changed security environment for national security policies countering emerging threats targeting critical infrastructure. This study presents a paradigm, theory, and model as a contribution to understanding the above questions. It is a qualitative study, and quantitative possibilities and potential explorations and directions for research inherent in the above arrow-diagramed theory, while interesting, are not addressed. Rather, as the title states, this study outlines a security environment approach to national security policy formulation. Each critical infrastructure requires different analyses, and each threat actor in the typology presented in chapter four also requires different analyses. What this study contributes, however, is an approach for conducting these disparate analyses; as such, it is theoretically-driven and abstract. The development of specific theories of specific threat actors targeting specific infrastructures is impossible to accomplish in a single work; this new field of policy is not only too deep and broad for a single work to be all encompassing, the field is too nascent to begin quantitative analysis of incident databases that have not yet been built. But an approach to these challenges and the field in general can be articulated, and that is the purpose of this study.

This chapter has so far made explicit a paradigmatic hard core, and presented a theory that establishes the relevance and importance of the policy field. Below, models are presented that describe and explain the nature of the challenges that national security policy must address in this fundamentally altered security environment.

Models:

Models, according to Kuhn in the "Second Thoughts on Paradigms," "provide the group with preferred analogies or, when deeply held, with an ontology. At one extreme they are heuristic...[a]t the other, they are the objects of metaphysical commitment."[84] This is the extent of Kuhn's treatment of model as a concept, which is inadequate. It conforms with his "Postscript – 1969" in which he states:

> Consider next a second type of component of the disciplinary matrix, one about which a good deal has been said in my original text under such rubrics as 'metaphysical paradigms' or 'the metaphysical parts of paradigms.'...Rewriting the book now I would describe such commitments as beliefs in particular models, and I would expand the category models to include also the relatively heuristic variety: the electric circuit may be regarded as a steady-state hydrodynamic system; the molecules of a gas behave like tiny elastic billiard balls in random motion. Though the strength of group commitment varies, with non-trivial consequences, along the spectrum from heuristic to ontological models, all models have similar functions. Among other things they supply the group with preferred or permissible analogies and metaphors. By doing so they help to determine what will be accepted as an explanation and as a puzzle-solution; conversely, they assist in the determination of the roster of unsolved puzzles and in the evaluation of the importance of each. Note, however, that the members of scientific communities may not have to share even heuristic models, though they usually do so.[85]

Models can be, of course, both heuristic and metaphysical, in the sense they serve both as aids to learning and illustrations of underlying principles of a field, including providing an ontology of entities studied by scholars within a community. Waltz more concisely provides a definition of a model: "*Model* is used in two principal ways. In one sense a model represents a theory. In another sense a model pictures reality while simplifying it, say, through omission or through reduction of scale."[86] In his book *Guide to Methods for Students of Political Science*, Van Evera does not explicitly define model as a distinct concept.

In explicating in the interest of precision and clarity the hierarchy of intellectual tools as used in this study, especially in light of the policy evaluative and prescriptive aspects inherent in the approach, the term model requires further treatment. RAND analysts Hodges and Dewar detail a conceptual framework for validation and uses of models designed to describe, explain, and potentially

---

[84] Kuhn, "Second Thoughts on Paradigms," pp. 462-463.
[85] Kuhn, "Postscript – 1969," p. 184.
[86] Waltz, *Theory of International Politics*, p. 7. Suppe views models in the same two senses as Waltz. See Frederick Suppe, ed., *The Structure of Scientific Theories* (Chicago: University of Illinois Press, 1974), pp. 96-97.

predict outcomes of conflict ranging from tactical engagements to strategic nuclear exchanges.[87] They present a framework for Department of Defense (DoD) and Intelligence Community (IC) modelers responsible for formulating high-powered, frequently large-scale computer simulations of hypothetical conflict scenarios.

Hodges and Dewar argue that prediction using a computer simulation of a conflict scenario requires that the model meet four prerequisites. Prerequisite 1 (P1) is it must be possible to observe and measure the situation being modeled. P2 requires that the scenario being modeled exhibit a constancy of structure in time. P3 stipulates that the conflict being modeled exhibit a constancy across variations in conditions not specified in the model. P4 states it must be possible to collect ample data with which to make predictive tests of the conflict model.[88] P1 and P4 are straightforward. However, I find Hodges' and Dewar's treatment of P2 and P3 vague and insufficient, so I amplify the explanations of them below beyond Hodges' and Dewar's treatment of them.

Here prediction requires a brief treatment before continuing with the discussion. Prediction is *ex ante* inference. In his "The End of the Cold War: Predicting an Emergent Property," Bueno de Mesquita actually engages in *ex post facto* statistical analysis using an expected utility model based exclusively on data available in 1948.[89] He argues that had an analysis using his model and methods been conducted in 1948, a quantifiably justifiable "prediction" could have been made concerning the end of the Cold War and the fall of the Soviet Union. Logically, this is a problematic assertion as his model did not exist in 1948, nor was the significant computational power required to calculate the model available to political scientists in 1948. Leaving this aside, Bueno de Mesquita actually engages in, in this case, postdiction.

Following Hodges and Dewar, predictions can be either specific or weak.[90] For example, they note a specific prediction may forecast the location of a specific planet at a specific time. Astronomers can accurately calculate such locations using mathematical models. These models are objective, highly quantifiable, and empirically verifiable. A weak prediction, on the other hand, is not capable of such precise quantification of outcome(s). It may be limited to simple comparisons of success; for example, a modeled computer defense of the national electric grid has a high probability of surviving a specific modeled cyberstrike against it. A fine-grained resolution of outcome is not to be expected

---

[87] James S. Hodges and James A. Dewar, *Is It You or Your Model Talking? A Framework for Model Validation* (Santa Monica: RAND, 1992).
[88] Hodges and Dewar, pp. 9-12.
[89] Bruce Bueno de Mesquita, "The End of the Cold War: Predicting an Emergent Property," *Journal of Conflict Resolution*, Vol. 42, No. 2 (April 1998), pp. 131-155.

from weak predictive models. Social sciences, as opposed to "hard" sciences, deal with weak predictions.[91]

Weak predictions may be predicated by the complexity of the system studied, in this case the critical infrastructure of electrical power generation, transmission, and distribution. As Perrow notes the complexity of systems have reached the point that the possible linkages between components are incomprehensible during failure.[92] A complex system in the process of being attacked will itself trigger secondary effects that were neither intended nor foreseen by system designers. Modeling the response and effects of a complex system under attack results in weak predictions.

Postdiction has forensic utility when applied against archived databases, and can itself inform efforts aimed at prediction with pattern analysis. However, postdiction is not prediction. Scholars engaged in statistical maschinations of historic data can discover many interesting things, but practitioners of national security require predictive ability. Postdiction is only policy relevant to the extent that patterns discovered are used to inform subsequent prediction. This can only be accomplished through models.

Taking the prerequisites in turn, P1 dictates that the model's variables, both dependent and independent, be quantifiable. As the level of precision in measuring the variables increases and the validity of the model improves, the precision of the prediction from the model potentially increases. A model capable of specific prediction potentially could include all relevant variables, be populated with extremely accurate data and founded on "hard science" laws operating under known, controlled conditions. Calculating the location of planets uses a model that closely approximates these traits. A case where the model cannot be validated, however, is notional weapons being employed against notional defenses and countered by notional countermeasures. As Hodges and Dewar point out, none of the systems exist, thus even if modelers believe they understand "the physics of the situation" the model cannot be validated, hence cannot be relied upon for specific prediction.[93] This is true even if modelers believe they comprehend the environment within which systems, or actors, operate when the system or actor is complex or unpredictable, or chaos is present.[94]

---

[90] Hodges and Dewar, pp. 6-7.
[91] Van Evera, *Guide to Methods for Students of Political Science*, pp. 30-32.
[92] Charles Perrow, *Normal Acccidents: Living with High-Risk Technologies* (New York: Basic Books, 1984) p. 9.
[93] Hodges and Dewar, p. 9.
[94] The study uses the term chaos to mean two specific, literal definitions, i.e., "a state of things in which chance is supreme," and "the inherent unpredictability in the behavior of a natural system (as the atmosphere, boiling water, or the beating heart)." This does not mean that situations must be

P2 requires the situation being modeled demonstrate constancy of structure and effects across trials, i.e., *reliability*. This is the assumption that the scenario being modeled is *stable* in causal structure and effects, and that the model is *reliable* in the formal sense.[95] The independent variables within the model must interact in a consistent manner resulting in consistent effects, holding all other variables *ceteris paribus*, regardless of when applied, or how often applied. This can be illustrated by an example. Consider a human subject whose performance on a test is being measured. A second trial holding all variables the same (same human, same test, same room, etc.) would likely find that the individual has learned from the first trial what to expect in the second trial, and consequently, has increased his performance over the first trial. This situation violates P2, and the results of iterative trials will not be consistent, or *reliable*. This implies that P2 requires a model that excludes the *agency* of thinking beings, or even unthinking, but animate objects or any dynamic characteristics, such as growth, learning, reproduction, or death. It also excludes cases where chaos exists.

This does not mean that living things possessing *agency*, or the capacity to act and exert power, must be excluded from models in order to meet P2. It simply requires that their agency be incapable of altering the causal structure of the situation modeled. For example, a model of strategic nuclear exchange involves, obviously, a world full of people possessing agency. But models of such conflict can be built and used to predict, with varying degrees of probability, the outcomes. An extreme model postulating a small village targeted by multiple, large-yield nuclear weapons would predict, with a probability approaching perfect certainty, the destruction of the village. In this extreme model, the agency of the victims cannot significantly affect the causal structure or effects of multiple nuclear explosions, and the model can be judged reliable in predicting an outcome of annihilation. Certainly, human agency was involved in the decision to launch the nuclear weapons, and not abort the flight of the missiles, etc., but these are factors preceding and exogenous to the modeled explosions.

P3 demands that the situation being modeled exhibit constancy across variations in exogenous conditions not specified in the model. P3 addresses the model across exogenous variable change given

---

orderly to meet the requirements of P2, as in a controlled laboratory experiment. A confused, unorganized (i.e., chaotic) situation can still meet P2. An example is throwing a locked cage of rats into a blast furnace. The situation in the furnace will be chaotic, but the ultimate outcome of multiple trials, *ceteris paribus*, will still be, predictably, dead rats. *Merriam-Webster's Collegiate Dictionary*, 10th ed. (Springfield, MA: Merriam-Webster, 1998), p. 191.

[95] "Reliability "concerns the extent to which an experiment, test, or any measuring procedure yields the same results on repeated trials....The more consistent the results given by repeated measurements, the higher the reliability of the measuring procedure..." Edward G. Carmines and Richard A. Zeller, *Reliability and Validity Assessment*, Series on Quantitative Applications in the Social Sciences, No. 07-001, Sage University Papers (Beverly Hills, CA: Sage, 1979) as cited in Johnson and Joslyn, *Political Science Research Methods*, p. 82.

endogenous variable *ceteris paribus*. What Hodges and Dewar are noting with this prerequisite is the concept of *robustness*.[96] The model of targeting a small village with a massive, nuclear strike can *prima facie* be judged as a *robust* model. The fact that in one computer simulation the climatic conditions were deep winter, but the next computer trial substituted a variable value of "rainy, summer day" is not a sufficient change in exogenous conditions to affect the causal structure and effects of the model. The model of a massive nuclear strike against a small village is *robust* across change in exogenous variables, specifically here climatic conditions. If the variable of climatic conditions affected the model's causal structure and effects significantly, then the model is less robust.

Continuing with examples of WME employment, the model of a non-persistent chemical weapon aerosol cloud is not robust across climatic conditions. Winds, rain, sunshine and other conditions significantly affect the causal structure and effects of a non-persistent chemical weapon aerosol cloud model. Here the model is not robust across exogenous change, again specifically in this case climatic conditions. The *robustness* of the model could be improved by adding the climatic conditions variable into the model, specifying that holding optimum weather conditions constant, the robustness is increased. But this has the effect of limiting the applicability of the model to specified cases. There is a tension between robustness, parsimony, applicability, and utility. A model can be made more robust at the cost of parsimony, by including all variables that if left exogenous to the model would affect its causal structure and effects if changed. But a model that includes many variables that must be held constant is of lesser applicability to diverse real-world scenarios, hence of narrower utility. A model that is made more "robust" at the cost of parsimony is of less applicability, hence utility except for those rare cases when the situation – reality – conforms to the model's multiple variable values.

Summarizing their thoughts on P2 and P3, Hodges and Dewar note that "P2 is necessary if you want to validate a model for the same conditions as those in your tests, and P3 is necessary if you want to validate a model for a wider range of conditions."[97] This points out the need for models to be "nested" within theoretical tools, specifically theory (ies) and paradigm, at a higher level of abstraction. Without embedding a model within theory and ultimately paradigm, one cannot specify the conditions exogenous to the model that affect its reliability (P2) and robustness (P3). Models constructed without the implicit or explicit exposition of the model's theory and paradigm are castles

---

[96] *Robustness* used in the sense that the model "remains a reasonable procedure [or approach] even if some of the assumptions underlying it are not met in the data (a property statisticians refer to as 'robustness')." John H. Aldrich and Forrest D. Nelson, *Linear Probability, Logit, and Probit Models*, Series on Quantitative Applications in the Social Sciences, No. 07-045, Sage University Papers (Beverly Hills, CA: Sage, 1984), p. 9.

in the air, unable to be anchored to reality's ground, and hence of no value to practitioners. Nesting models within theory and paradigm, however, is only a necessary condition, and not a sufficient one, for them to serve as intellectual tools in any practical fashion. The theory and the paradigm must also accurately reflect reality, albeit at an abstract level, for the model to have anchor points in reality. Even a neatly nested construction will be at best a beautiful fiction, and at worse a catastrophic failure, if not representative of reality.

P4 dictates that it must be possible to collect ample data with which to make predictive tests of the model. This prerequisite is not only about the possibility that valid measurements can, in fact, be conducted, but that there exists some minimum number of events to measure.[98] For example, prior to the Trinity Test on 16 July, 1945 there existed no nuclear explosion that could have been measured from which to make predictions. Even after the test, significant disagreement among experts persisted on the effects of nuclear weapons. It was not until the 6th and 9th of August, 1945 employment of nuclear weapons against Hiroshima and Nagasaki, respectively, that virtually all doubts about this "absolute weapon's" efficacy were erased.[99]

Kuhn also addresses the important concept of model. Exemplar is a "concrete problem solution, accepted by the group as...paradigmatic." While Kuhn points out that the three elements (symbolic generalization, model, and exemplar) of the disciplinary matrix are interdependent, and changes in any of them can affect the others, as well as that community's behavior, research locus, and standards, he focuses on exemplar as the second substantive sense of paradigm. [100]

Kuhn states that:

> More than other sorts of components of the disciplinary matrix, differences between sets of exemplars provide the community fine-structure of science. All physicists, for example, begin by learning the same exemplars: problems such as the inclined plane, the conical pendulum, and Keplerian orbits...As their training develops, however, the symbolic generalizations they share are increasingly illustrated by different exemplars.[101]

Thus, exemplars provide to the community concrete examples upon which they all agree, and can use to communicate. For example, two physicists discussing a particular real-world problem would both

---

[97] Hodges and Dewar, *Is It You or Your Model Talking? A Framework for Model Validation*, p. 12.
[98] The term "valid" is used here in the sense of "a valid measure is one that measures what it is supposed to measure....validity involves the correspondence between the measure and the concept it is thought to measure." Johnson and Joslyn, *Political Science Research Methods*, p. 83.
[99] The term, of course, is Brodie's. Bernard Brodie, ed., *The Absolute Weapon* (New York: Harcourt Brace, 1946).
[100] Kuhn, "Second Thoughts on Paradigms," p. 462-463.
[101] Kuhn, "Postscript – 1969," p. 187.

understand if one of them were to assert that the problem was, in essence, a real-world case of a classic inclined plane exemplar. Kuhn sees exemplars in the Waltzian first sense of a model, that is, representing a theory. Kuhn defines his notion of models (vice exemplars) in the Waltzian second sense of a model, or a specific picture or example of reality. But neither Waltz nor Kuhn would demand that a model be a perfect picture of reality. Waltz states "A full description [of reality] would be of least explanatory power [in a model]; an elegant theory, of most."[102] It is important to note here that Waltz uses the term *theory* as a synonym for model in the quote, although he explicitly states two purposes of model: theory representation *and* depiction of reality. Kuhn only sees a *model* as a depiction of reality, and his concept of *exemplar* is the representation of a *theory* containing *symbolic generalizations* (laws) as a model in the Waltzian sense of theory representation.

The Kuhnian *exemplar* and the Waltzian sense of model as theory representation both can be better understood as Platonic Forms, the abstract, idealized archetype which defines a concrete entity as a specific object or characteristic.[103] The Kuhnian exemplar of an inclined plane can be understood as the Platonic Form of the stylized inclined plane, not a specific case concerning an engineer on a specific construction site. Neither Kuhn nor Waltz cites Plato's Forms in stating their concepts of models. However, Kuhn in his "Second Thoughts on Paradigms" relates the tale of how a young boy learns to distinguish a swan from geese and ducks. In doing so, the boy learns from his father the characteristics of what constitutes ideal "swan-ness," like the length and curvature of the neck, and other characteristics. In this way the boy learns, in essence, the Platonic Form of an abstract, idealized swan, which he employs to correctly identify swans in reality.[104]

Hodges and Dewar argue that there are seven uses of a model beyond prediction. Having acknowledged the difficulty above of predicting the consequences of an attack on a complex system, like an infrastructure, that does not equate to saying that there is no need for modeling the system. The purposes of modeling a system, other than prediction, are:

1. As a bookkeeping device, to condense masses of data or to provide a means or incentive to improve data quality.
2. As an aid in selling an idea of which the model is but an illustration.
3. As a training aid, to induce a particular behavior.

---

[102] Waltz, *Theory of International Politics*, p. 7.
[103] Plato, *The Republic*, trans. G.M.A. Grube (Indianapolis: Hackett, 1974), pp. 135-140. See especially paragraph 476 a-d.
[104] Kuhn, "Second Thoughts on Paradigms," pp. 473-477.

4. As part of an automatic management system whose efficacy is not evaluated by using the model as if it were a true representation.
5. As an aid to communication, e.g., in purely intellectual explorations or in operating organizations.
6. As a vehicle for *a fortiori* arguments.
7. As an aid to thinking and hypothesizing, e.g., as a stimulus to intuition in applied research or in training or as a decision aid in operating organizations.[105]

These seven uses of a model beyond prediction will apply in Chapter 4 when a typology of emerging threat actors is detailed. A brief overview of the seven purposes will facilitate discussion.

Ordering reality is one purpose of a model. As a bookkeeping device, a model can contain data in discrete compartments, maintaining them in relevant relationships to other model components, and catalogued chronologically or in other ways. This ordering, or bookkeeping function, enables later functions of the model, such as hypothesizing. Without this use, data would become disassociated from relationships that correspond to reality, and potentially be lost or corrupted. In computer databases, automatically and continually fed with massive amounts of data from remote sensors, this is a significant purpose of a model. Without such anchoring in reality, models are of no practical utility.

Policy formulation requires advocates. The second use of a model is to serve as an aid in selling an idea. A model, whether physical or mathematical can illustrate the results of policy in a concrete fashion. The model provides the policymaker with an impression of what will be the results of a specific policy's adoption. Regardless of whether these results are portrayed in terms of financial savings, or of drug confiscations resulting from interdiction of illicit smuggling, models can aid in convincing policymakers to adopt a policy.

Models can also serve as training aids, or to induce a desired behavior. In the context of this study, watch officers charged with monitoring the shallow structure of cyberspace surrounding critical facilities embedded within a critical infrastructure, such as a major node in the national electric grid, will be trained to react to their sensors and other devices through the use of models.[106] Before they can

---

[105] Hodges and Dewars, p. 19.

[106] This study defines the shallow structure of cyberspace as the portion of cyberspace surrounding the actor and in which the actor interfaces with applications that control the infrastructure's processes. The deep structure of cyberspace is defined as the portion of cyberspace beyond the actor's control. In high-security networks, both the actor's shallow and deep structures may be isolated from the larger global cyberspace, or "islanding." This can be accomplished by building at the physical-level dedicated transmission channels, unconnected to the global, deep cyberspace structure. This is an

recognize a hostile intrusion into their networks, they must first be trained to recognize the traces of such an intrusion using a model.

Use of a model as a component of an automatic management system is also an example found in several infrastructures. Continuing with the electric system, models of usage patterns process data from multiple remote sensors in real-time to monitor the load, demand, and supply of electric current. When the model reports a portion of the grid approaching peak usage, the operator knows from the model that he needs to bring peak generating plants on-line within a specified time to meet imminent demand for electricity.

A fifth purpose of models is to aid communication. The value of a common vocabulary among a community of professionals is well known. A model can serve as a type of common vocabulary, a shared reference to reality, that can assist communications between those who know the model.

A model can be an *a fortiori* argument for policy. If a model of a cyberstrike biased to represent a low-level threat actor, holding exogenous variables constant, defeats a modeled computer defense of an electric infrastructure node, that demonstration can be used as an *a fortiori* argument for dedicating more resources towards that node's protection. This is because an actual threat actor would represent a more capable threat than that modeled in the simulated cyberstrike, which in itself was sufficient to defeat the computer defense of the electric infrastructure node.

Lastly, a model can be used to aid thinking. This is a powerful purpose, as it implicitly exercises both of the Waltzian senses of model: theory representation and depiction of reality. Policy is the result of thinking based on some theory of reality concerning what needs to be done, how it can be done, when it can be done, and a host of other factors. Consciously or not, policymakers use models, even if only poorly-articulated mental ones, to consider the ramifications of a considered

---

expensive solution, and most transmissions, including military, travel over the same deep structure of cyberspace as personal emails, albeit in encrypted format. The last point of shallow cyberspace is the actor's point of presence (POP) on the "edge" of the deep structure of cyberspace. An individual's POP can vary in both physical space and cyberspace, however where the communications depart the actor's control, for example, at the beginning of the Internet Service Provider's (ISP) network, the actor loses control of the transmission and the deep structure of cyberspace for that actor begins. The terms deep and shallow cyberspace are this study's interpretation; for information on the POP and "edge," and related concepts, see Ray Horak, *Communications: Systems and Networks*, 2nd ed. (Foster City, CA: M&T Books, 2000), pp. 2-6; *SAFE: A Security Blueprint for Enterprise Networks*, White Paper (San Jose, CA: Cisco Systems Inc., 2001), pp. 4, 19-21, 47.

policy. If they employ a good model in such thinking, that contributes to the formulation of good policy to some degree.

Hypotheses and Laws:

Kuhn explains a symbolic generalization as an expression employed by a community routinely. He cites as an example the formula $f = ma$ as a symbolic generalization used within the physical sciences upon which scientists agree and which they use to communicate. A symbolic generalization gives a community a base for logic. Here Kuhn's use of symbolic generalization equates to the concept of a law. Van Evera defines a law as a relationship between phenomena, which can be either deterministic or probabilistic.[107] Waltz, similar to Van Evera, states that "[l]aws establish relations between variables."[108] Laws, all agree, are subordinate to higher constructs, such as theories.

A detailed treatment of hypotheses and laws is not required, although they are intellectual tools that shape theoretical work. The intellectual tools that are sometimes contentious among scholars, i.e., paradigms, theories, and models, have been explicitly addressed above, and provide an adequate foundation for the study, as well as an explicit basis for critique. This study employs hypotheses and laws in convention with their standard, accepted use as defined by Kuhn, Waltz, and Van Evera.

Paradigmatic and Theoretic Shape of the Study:

The phenomenon of conflict is a central concern of world politics. This study examines actors capable of employing means of violence that yield system relevant, strategic effects. Such actors are systemic actors. Thus, the unit of analysis is the Waltzian "Second Image," specifically actors capable of employing WME. However, it is not limited to only state actors. Waltz argues in *Man, the State, and War* that, from a strictly second image perspective, "the internal structure of states determines not only the form and use of military force but external behavior generally."[109] In addressing the implications of the Second Image, Waltz points out "that internal political structure will determine the organization and use of military force."[110] Waltz, of course, focuses exclusively on the state as the arch-Second Image, however, he does not assert that they are the only actors that exist in a given system. In *Theory of International Politics*, he defines political structures using three criteria: 1.

[107] Van Evera, *Guide to Methods for Students of Political Science*, p. 7.
[108] Waltz, *Theory of International Politics*, p. 1.
[109] Waltz, *Man, the State, and War*, p. 125.
[110] Ibid, p. 124.

the principle according to which they are ordered; 2. the differentiation of units and the specification of their functions; and 3. the distribution of capabilities across units.[111] The second criterion, differentiation of unit and specification of function, drops out from Neorealism, because Waltz addresses only states, which he asserts are functionally undifferentiated.[112] In defining structure generically he states "International structures are defined in terms of the primary political units of an era, be they city states, empires, or nations, " and "States are not and never have been the only international actors. But then structures are defined not by all of the actors that flourish within them but by the major ones."[113] Waltz, although he focuses exclusively on states, clearly does not maintain that only states can be Second Image actors. This conforms to the thoughts of two other preeminent Realists: Carr and Morganthau, as already detailed above. This study addresses "systemic actors" other than states, i.e., non-state actors. This includes both First and Second Image actors, although the overwhelming majority of systemic actors are Second Image actors. A characteristic of the new security environment is that First Image actors can potentially be systemic-level actors, capable of affecting the world political system by employing WME or other instruments of power.

Wendt points out that "In much of IR scholarship units and levels of analysis are conflated."[114] However, the choice of, for example, multinational corporations as the unit of analysis (i.e., "that which is being studied")[115] does not constrain one to a sub-systemic level of analysis. How multinational corporations affect the international system is an analysis of how a Waltzian Second Image actor influences the Third Image. How multinational corporations affect individuals is an alternative where Second Image affects on the First Image is the focus. Adopting Wendt's terms, it is an analysis of how a specific agent influences a particular structure, and vice versa.[116] Waltz chooses the state as the unit of analysis ("interacting units"), and the international system as the level of analysis ("international structure"). He also argues that this is a two-way flow of influence: "Structural

---

[111] Waltz, *Theory of International Politics*, chapter 5.
[112] Ibid, p. 105. See also Wendt, "Anarchy Is What States Make of It," p. 396; and Wendt, *Social Theory of International Politics*, pp. 98-103.
[113] Waltz, *Theory of International Politics*, p. 91 and p. 93, respectively.
[114] Alexander Wendt, *Social Theory of International Politics* (Cambridge: Cambridge University Press, 1999), p. 7, fn 22.
[115] Paul R. Viotti and Mark V. Kauppi, *International Relations Theory*, 3rd ed. (Needham Heights, MA: Allyn & Bacon, 1999), p. 498.
[116] Alexander E. Wendt, "The Agent – Structure Problem in International Relations Theory," *International Organization*, Vol. 41, No. 3 (Summer 1987), pp. 335-370.

theory emphasizes that causation runs from structures to states *and* from states to structure."[117] This is reflected in one of his figures:[118]

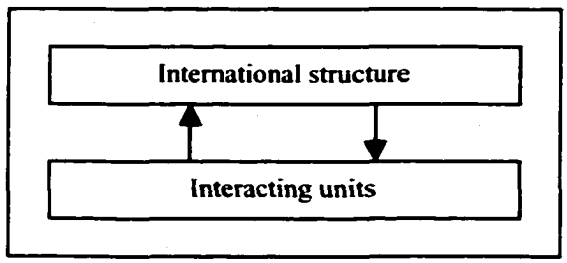


Figure 1 – 1: Waltz's Figure

This study takes as its unit of analysis, that which is being studied, non-state actors capable of employing WME, and the level of analysis as systemic. Its paradigm is constituted of "Red, Gray, and Blue" where Red is a Threat, Threat itself being a sub-set of Other; Gray is the Environment; and Blue is Self. These three elements of the Environment are dynamically interdependent and mutually constitutive. The study accepts Waltz's injunction that "[a]ny approach or theory, if it is rightly termed 'systemic,' must show how the systems level, or structure, is distinct from the level of interacting units."[119]

The dissertation contains five chapters. The first chapter is this introduction, which has accomplished the not-trivial task of explicitly defining the major conceptual terms and themes that serve as the study's foundation. It has also introduced the problem being studied; a significant challenge that is the focus of the US national security elite. This is a challenge that contains potential political and policy ramifications rivaling the National Security Act of 1947, and the Goldwater-Nichols Act of 1986.

The second chapter, the CIP Policy Field and Punctuated Equilibrium Theory, presents Baumgartner and Jones' theory of the policy process of change and formulation, and examines whether that theory is functionally adequate to describe and explain how national security policy formulation should proceed in the fundamentally altered security environment. Examples of current policies countering emerging threats serve to detail the theory for describing and explaining how future policies countering such threats to critical infrastructure can best address the challenge. The chapter argues

---

[117] Kenneth N. Waltz, "Evaluating Theories," *American Political Science Review*, Vol. 91, No. 4 (December 1997), p. 914.
[118] Waltz, *Theory of International Politics*, p. 40, figure 3.1; see also Waltz, "Evaluating Theories," p. 914, figure 1.
[119] Waltz, *Theory of International Politics*, p. 40.

three hypotheses, discussion of which demonstrates the need for a new approach guiding national security policy and its formulation.

The third chapter, Red, Gray, and Blue, presents the security environment approach to these threats. It serves as both a representation of the theory advanced in the chapter, as well as a depiction of the current security environment. Seven possible models within the framework are introduced.

The fourth chapter, A Typology of Emerging Threats and the Game of Stalker, presents a typology of pure-type, systemic actors other than states, including states emulating a non-state actor for operational purposes. It explicates the threat identities, their means and capabilities, critical infrastructure targeting preferences, and ends. Following presentation of the complete typology, analysis of seven threat attack models are discussed.

The fifth chapter is the conclusion. The study's findings are summarized, policy recommendations are stated, and directions for future research suggested.

The central national security policy challenge addressed by this study is a strike employing WME against a US critical infrastructure or population. Figuratively speaking, the study argues the United States is at ground zero on 17 July, 1945 with this challenge. Data exists, but it is limited by a so-far happy dearth of incidents. The US national security elite are aware that a new era has dawned in the arena of conflict, but they lack, as the Trinity test shot engineers lacked on the day after Trinity, a framework within which to comprehend the enormity of the moment. Activity and funding has not been lacking, and substantial programs have been set in motion in the six years since the President's Council on Critical Infrastructure Protection (PCCIP) submitted their report to the President that has generated legislation and, in turn, created a new national security policy field. These efforts have perhaps been inevitably like many other urgent responses; a flurry of activity mixed with some measure of breathlessness. The result has been, in the words of one scholar, ataxia: a lack of order and the inability to coordinate.[120]

The Bush Administration has inherited an important, but still very nascent, policy field concerning a major national security challenge. However, until a common coordinating paradigm is adopted that will serve to unite members of the US national security policy elite in defining "the legitimate problems and methods"[121] of this new field, ataxia will remain the result of good intentions and best efforts.

---

[120] Amy E. Smithson, *Ataxia: The Chemical and Biological Terrorism Threat and the US Response* (Washington, DC: Henry L. Stimson Center, 1999).
[121] Kuhn, *The Structure of Scientific Revolutions*, p. 10.

Lisa Roberts notes that a Kuhnian paradigm crisis ends in one of three ways. A community handles the crisis within the old paradigm, the community deems the crisis as insoluble and sets it aside, or a new paradigm emerges.[122] The national security policy community to date has favored the first two approaches. It is necessary, however, to move to the third. This study intends to contribute to establishing that framework.

[122] Lisa J. Roberts, "Thomas Kuhn's The Structure of Scientific Revolutions," *E-Prime, ΣEOS, and the General Semantics Paradigm: Revolutions, Devolution, or Evolution?* (Concord, CA: International Society for General Semantics, 1999), p. 67.

Chapter Two: The CIP Policy Field and Punctuated Equilibrium Theory

"[The] emergence of a new category is a signal public policy event. When people start thinking of [new policy fields] entirely new definitions of problems and conceptualizations of solutions come into play."[1]

Introduction:

This chapter addresses the effect of the changed security environment on formulation of national security policies designed to counter emerging threats. The development of ten core policy documents in the CIP field is examined to establish a benchmark for analysis. The chapter then presents Baumgartner and Jones' theory of change and formulation within the policy process, and examines whether that theory is functionally adequate to explain how national security policy change and formulation should ideally proceed in the fundamentally altered security environment.

This study, as noted in Chapter 1, maintains that theory and policy are inextricably bound. Van Evera's observation that all policy proposals are based on theoretical assumptions reinforces the expectation that a change in a policy community's framework should necessarily be reflected in an eventual corresponding change in policy generated by that community.[2] If reality has changed to the extent that a new theoretical framework is required to explain it, as this study maintained in Chapter 1, then national security policies designed to address this changed reality should reflect this paradigm shift.

The above leads to three hypotheses. First, if the policy community paradigm framing reality has become obsolete, then policy formulated under this obsolete paradigm will be inadequate to address the new reality, i.e., past policies will prove inadequate in countering emerging threats in the changed security environment. Second, if there has been a shift in that paradigm, then security policy formulation should be changing in an attempt to keep pace with the changed framework as members of the policy community recognize the inadequacy of the old paradigm. Third, if the paradigm is directly relevant to the security policy change and formulation process, then that process must be capable of paralleling the paradigm's pattern of change. Amplifying the third hypothesis, an incremental change in theoretical framework should be met with an incremental change in policy, but a radical Kuhnian "gestalt switch" in paradigm should precipitate a correspondingly radical change in security policy and its formulation; *a relevant theory of policy change and formulation must account for both cases.*

---

[1] Kingdon, p. 113.
[2] Stephen Van Evera, *Guide to Methods for Students of Political Science*, pp. 89-93.

The study's argument is that the altered security environment requires a new framework – paradigm – to understand it. The bipolar clarity of the Cold War has evaporated, and in its place is a system with diverse actors. Theories that deal with state-on-state conflict – the classic stereotype of war – still apply within their bounded contexts. Certainly, in the international system there still remain states and the potential for conflict between them. What is now additionally required, however, is a framework that aids in understanding the new security environment and its diverse actors, and theories that can aid understanding of the emerging threats as well as conflict between non-traditional actors and states. The role of emerging threat actors is not adequately treated by mainstream theories of international relations. Given a change in theoretical framework, one would anticipate a subsequent change in policy. Because of this, policies resting on these bounded theoretical foundations are inadequate in the altered security environment.

The chapter finds that the PE theory of policy change and formulation advanced by Baumgartner and Jones is suitable for both periods of paradigmatic stability (Kuhnian normal science), as well as radical change of paradigm (Kuhnian scientific revolution). Additionally, policy formulated under the previous paradigm is found inadequate, substantiating the first hypothesis. As an example of inadequate policy formulated under the old paradigm, the 1992 and 1999 Federal Response Plans (FRP) issued by the Federal Emergency Management Agency (FEMA) are examined, and found to not only inadequately address emerging threats, but in its 1999 version also to be counterproductive and uncoordinated with previously published higher security policy documents, specifically PDD 63 and other core policies. This example supports hypothesis one's assertion that policy formulated under the old paradigm will be inadequate to address emerging threats in the changed security environment. The discussion also illustrates how during a Kuhnian paradigmatic crisis old policies are challenged by new policies, reflecting the more elemental challenge of the old paradigm by the new paradigm.

Hypothesis two states that if there has been a shift in paradigm, then security policy formulation should be changing to keep pace with the changed framework. This chapter finds that, in fact, the past approximately five years has resulted in ten major security policy documents, and numerous Presidential commissions, Blue Ribbon panels, study groups, and other efforts to change US security policy in light of an altered framework. This has led to the creation of a new security policy field – Critical Infrastructure Protection – that involves every major US agency, and spans government from the local, state, regional, to Federal levels. The United States Commission on National Security / 21st Century (USCNS/21) phase III report makes fifty major policy recommendations, seven regarding securing the national homeland. These recommendations and others made by the Commission in other

areas evidence characteristics of radical change detailed by the PE theory. The findings of the chapter strongly support hypothesis two.

Hypothesis three maintains that if, as Van Evera asserts, the paradigm is directly relevant to the security policy change and formulation process, then the process should be capable of paralleling the paradigm's pattern of change. A theory of policy formulation that cannot account for radical change, for example, is of limited utility in a policy environment undergoing radical change. The findings concerning Baumgartner and Jones' Punctuated Equilibrium (PE) theory support hypothesis three. In fact, the PE theory strongly resembles both in form and substance Kuhn's theory of scientific revolutions, which also advances the argument that a "punctuated equilibrium" characterizes periods of equilibria, or Kuhnian normal science, with punctuations, or paradigm shifts.

This chapter examines national security policy formulation concerning critical infrastructure protection with these three hypotheses in mind. It first details a previous radical shift in the United States' security environment, and the corresponding shift in paradigm followed by policy, after World War II to establish a relatively recent type precedent. During that period of fundamental change in the international system an American diplomat provided an enduring strategic compass – a paradigm – for the national security elite to frame and understand their era, and from this epiphany flowed national security policies of the most profound and strategic import. This precedent, and others which could be cited from different eras, demonstrate that the chapter's argument that the structure of policy change parallels the structure of paradigm change has familiar historical roots.

Challenges within the current security environment are next presented, developing the required knowledge of background and problems leading to change of security policies and the recent creation of the CIP security policy field. Discussion of the challenges facing US national security policy provide the requisite context for understanding the nature of changes in the security environment, paradigm, and policies. A specific security policy, the Federal Response Plan (FRP), is examined for applicability in addressing emerging threats, and found inadequate. This examination supports hypothesis one.

The next section of the chapter reviews the PE theory of Baumgartner and Jones. This is followed by an examination of its applicability to the structure of policy change generated by this new security environment and its problems, or the shifting paradigm's structure. The chapter's analysis finds that the PE theory is suited to explain policy change and formulation during both incremental and radical shifts in security environment and paradigm. This examination supports hypothesis three.

Following the presentation of the PE theory, the specific case of a major national security policy change is process-traced. This case proceeds from its roots in challenges to the US, through the corresponding paradigm shift, and into the macropolitical limelight of a US House of Representatives Resolution for establishment of a new national security agency. This process tracing is examined for conformation to the PE theory. The analysis supports hypothesis two.

The chapter then concludes the discussion, finding the reality of the post Cold War security environment requires a new framework to understand it and to formulate effective security policy. Baumgartner and Jones' PE theory is a functionally adequate model of policy change and formulation capable of serving as a macro-level guide for the pattern of CIP policy development. It addresses how we can understand the changed environment, as well as the implications of the changed security environment for national security policies countering emerging threats.

Different threats require different policies. The means, methods, targeting preferences, and ends of non-state actors are different than state actors. Certainly, protecting vulnerable infrastructures demand new policies. Of course, there is substantial need in the current security environment for new policies to counter new threats. But this era's need for change is not unprecedented in degree, although it is obviously different in type. The two questions that now should be confronting US national security policymakers is what theoretical framework is appropriate, and what concrete policy actions they should be taking in light of this changed security environment and paradigm. The policymakers' two questions parallel at a lower level of analysis and abstraction the study's two closely related, strategic questions: 1. How can we understand the changed security environment theoretically?, and , 2. What are the implications of the changed security environment for national security policies countering emerging threats? These are questions with precedents. The current Kuhnian paradigmatic crisis is analogous to a previous change in the world political system that serves as a concrete historical illustration of how paradigm drives policy. The analogy also serves to remind us that although our context and characteristics are, in fact, novel, our circumstances possess, when considered from a broader perspective, a familiar sense of déjà vu.

Kennan's Gift of an Epiphany:

In retrospect, George Kennan had little difficulty in drafting his long telegram from Moscow and in having its views adopted wholesale by the American security elite. A then relatively junior and little-known Foreign Service officer, Kennan was asked by the State Department in February 1946 to reveal the animus driving Soviet post-war diplomacy and actions following an ominous foreign policy

speech by Stalin. Kennan was well positioned by virtue of his intellect, position as the Chargé d' Affaires in Moscow, and experience to lay bare for Washington the *realpolitik* essence of Soviet diplomacy. In some 8,000 words he sketched a perspective of the Soviet Union, its ends and *modus operandi*, and the implications for a pragmatic U.S. security policy response that expressed "within the compass of a single document, ideas of such force and persuasion that they immediately change[d] the direction of a nation's foreign policy."[3] Dean Acheson judged it a "truly remarkable dispatch," and credited it with having "a deep effect on thinking within the Government."[4] Kennan's telegram disabused those within the US security elite who viewed Soviet conduct as an understandable result of recent war, fear, and suspicion that would inevitably be dispelled by a *quid pro quo* strategy of engagement by the United States. A brilliant, clear statement fueled by "a mixture of exhilaration at having been asked and exasperation at having until then been ignored," Kennan was surprised how readily Washington accepted his telegram.[5] The characteristics of Kuhn's paradigmatic crisis stage suggest why Washington was ready for a framework that would describe, explain, and predict what they were observing, but failing to comprehend: "Because it demands large-scale paradigm destruction and major shifts in the problems and techniques of normal science, the emergence of new theories is generally preceded by a period of pronounced professional insecurity. As one might expect, that insecurity is generated by the persistent failure of the puzzles of normal science to come out as they should. Failure of existing rules is the prelude to a search for new ones."[6] The national security elite were baffled by the Soviet's behavior, and when this collective failure of the Defense Department, State Department, and other US organizations to frame reality in a coherent and pragmatic fashion reached a sufficiently high level of official frustration, the US State Department sought elsewhere for answers and cabled a junior foreign service officer in Moscow for insight.[7] Kennan provided the epiphany.

Gaddis states the reason for the rapid ascension of Kennan's view to national security policy was due to the security elites' own recognition that their perception of the Soviet Union was wrong.[8] Kennan's telegram was delivered at precisely the moment when the twin illusions of unbridled US hegemony conferred by the absolute weapon held by some US officials, and an amicable future of Soviet – US cooperation held by others more idealistic were both shattered by Stalin's 9 February 1946

---

[3] John Lewis Gaddis, *Strategies of Containment: A Critical Appraisal of Postwar American National Security Policy* (New York: Oxford University Press, 1982), p. 19.
[4] Dean Acheson, *Present at the Creation: My Years in the State Department* (New York: W.W. Norton & Company, 1969), p. 151
[5] Gaddis, p. 19.
[6] Kuhn, *The Structure of Scientific Revolutions*, pp. 67-68.
[7] Gaddis, p. 19.
[8] Ibid, p. 20.

speech in which he detailed "with brutal clarity the Soviet Union's postwar policy."[9] In his memoirs, Kennan notes that Washington was "ready to receive the given message."[10] It precipitated a Kuhnian change in perception of the Soviet *gestalt*, a paradigm shift that would fundamentally shape the future of both US and Soviet national security policy during the Cold War.

The Soviet Union's capabilities and intent, things encompassed within what Kuhn cites as "the same bundle of data," remained unchanged before Kennan's telegram was cabled to Washington as after it was sent. What changed was the US security elite's perception of these Soviet capabilities and intent, because Kennan had provided at a critical juncture "a different framework" within which to understand the Soviet's declarations, actions, means, and ends. The same data concerning Soviet actions, placed "in a new system of relations with one another by giving them a different framework" allowed the US security elite to "see" the new reality of their security environment and the true nature of the Soviet Union.[11] Kennan pointed to the antelope present in the *gestalt* that had previously been seen only as a bird, to paraphrase Kuhn.[12] Viewed from the old framework of only months before, Stalin's hostile speech, foreshadowed and reinforced by previous Soviet actions, was another glaring anomaly that perspectives based on false understandings of the security environment and the Soviet Union could not reconcile. Soviet actions did not square with a paradigm of the Soviet Union as weaker than or cowed by the United States. Efforts to understand the Soviet Union, whether based on liberal ideology or *realpolitik* attitudes of US nuclear dominance, increasingly began to resemble "a strenuous and devoted attempt to force nature into...conceptual boxes" that did not correspond with reality. At this juncture, Kennan's long telegram provided a paradigm – world view – that *fit* the reality observed.

The concept of containment Kennan fathered described a strategy – *a security policy* – that fit the world political system. The environment conformed to Kaplan's later-articulated model of a loosely bipolar world, but at the time the US national security elite intuitively grasped Kennan's seminal explanation of a US-USSR dominated bipolar world.[13] The paradigm of bipolarity and adoption of a strategy of containment fit the security environment's reality better than previous post-war frameworks of relations with a demonstrably hostile Soviet Union and Stalin. From this changed paradigm cascaded concrete changes in national security policy and its subsequent formulation.

---

[9] Acheson, p. 150.
[10] George F. Kennan, *Memoirs: 1925-1950* (Boston: Little, Brown and Company, 1967), pp. 294-295, cited in Gaddis, p. 21.
[11] Kuhn, *The Structure of Scientific Revolutions*, p. 85.
[12] Ibid.
[13] Morton A. Kaplan, "Variants on Six Models of the International System," in *International Politics and Foreign Policy*, ed. James N. Rosenau (New York: Free Press, 1969), pp. 296-297.

Similarly, a contemporary assertion that the current security environment has undergone a fundamental change should find support in security policies and their formulation.

The challenge facing post-World War II strategists was how to frame the world for policymakers in a useful way. The system was nascent, chaotic, and still malleable. The adoption of a strategy of containment shaped the system. The enormity of the moment facing strategists like Kennan was daunting. A unique, even "absolute," weapon had been invented that was not addressed within the bounds of past doctrines, strategies, or policies resulting in fundamental changes in interstate politics. It was an era of paradigmatic destruction and creation.

To great extent the United States in the post Cold War world faces a similar need for strategic direction in a still inadequately framed world. A decade has passed since the end of the Cold War, and arguably perhaps the easiest opportunities to shape the environment have passed. Regardless, the need to frame the world in a coherent and pragmatic paradigm still exists. Threats will not look to the past, but to the future. Similarly, the paradigm driving policy must also be future oriented, and not imprisoned in the past. Strategic principles must be evaluated for relevance in the new security environment, because unexamined "truisms" can ossify until they are opaque lenses useful only for seeing what they allow to be seen. Many challenges have clearly emerged for US security policy to counter. It is to these we now turn.

Challenges Facing US National Security Policy:

The challenges facing US strategists crafting security policies in the post Cold War world are diverse and in many cases novel. In the wake of the Soviet Union's demise and loss of empire, there has been a global proliferation of WME materials, technology, and knowledge. Additionally, there has been an increase in the number of new states in the system, as well as new non-state actors. The dissolution of the Warsaw Pact means former client states are now free to pursue their own agendas without oversight. These and other consequences of the Soviet Union's collapse have dramatic implications for US national security. Other challenges include the invention of cyberweapons, the impenetrable secrecy of communications that strong encryption, steganography, and digital watermarking affords threat actors, and the rise of various transnational threats. Several key events have also demonstrated new dangers inherent in the security environment. As Stalin's speech influenced and alarmed Kennan's superiors, these incidents have changed how US elites view national security. In turn, this has influenced specific security policies and even created new security policy fields.

Kennan faced an era confronted with the reality of nuclear weapons. Today, global proliferation of WME materials, technology, and knowledge raises concerns about use of WME on American soil.[14] WME are not limited to nuclear missiles, but include even conventional bombs when employed in a fashion that results in mass casualties. Additionally, cyberweapons can effectively strike America's highly-computerized, tightly-interdependent critical infrastructure with mass effects. Chemical and biological agents are within the development capabilities of individuals with relatively modest levels of capital, infrastructure and education. Many biological agents are available through legitimate scientific research channels, at high levels of quality and potency. As an example of WME employment capability, Chechen separatists targeting Izmailovski Park in Moscow have used radiological agents. The group employed Cesium-137, which if it had been dispersed instead of buried as a demonstration of capability would have required a massive cleanup effort.[15] The Chechen separatists intended the burying of the Cesium as strictly a capability demonstration, not an attack. However, a future intent of other actors, and especially non-state actors, may be to demonstrate capability through an effective First Strike employment of WME.

These and other changes and events have led to the creation of the new CIP security policy field. In the past five years there has been an explosion of effort in this new policy field that reflects the inability of past policy approaches to deal with the new security environment, supporting hypothesis one. The CIP policy field is designed to counter emerging threats to the United States' population and key systems. As such, it comprises a new category that spans both domestic and foreign policy arenas, employs existing policies in *ad hoc* fashion, creates new policies, crosscuts diverse public policy sectors from telecommunications to health to law enforcement to issues concerning employment of the military in domestic incident response, and involves every level of government, literally, from local to national. It is a rare development in American public policy, and it raises fundamental issues ranging from civil rights and privacy to the use of the armed forces within

---

[14] Both President Clinton and President Bush have referred to countering terrorist WME employment as a national security issue of paramount importance and urgency. In 1999 President Clinton assessed the likelihood of a chemical or biological attack on American soil, saying it "is highly likely to happen sometime in the next few years." President Bush states: "The grave threat from nuclear, biological and chemical weapons has not gone away with the Cold War. It has evolved into many separate threats, some of them harder to see and harder to answer. And the adversaries seeking these tools of terror are less predicable, more diverse. With advanced technology, we must confront the threats that come on a missile. With shared intelligence and enforcement, we must confront the threats that come in a shipping container or in a suitcase." Quotes, respectively, from *Interview of the President by the New York Times*, White House press release, January 23, 1999 (Washington, DC: White House Office of the Press Secretary), p. 3; and, *Remarks by the President to the Troops and Personnel of US Joint Forces Command*, USJFCOM press release, 13 February, 2001 (Norfolk, VA: US Joint Forces Command), p. 2.

[15] Jessica Stern, *The Ultimate Terrorists* (Cambridge, MA: Harvard University Press, 1999), p. 67.

the continental United States to control the consequences of a WME strike. A noted scholar of public policy states the "emergence of a new category is a signal public policy event. When people start thinking of [new policy fields] entirely new definitions of problems and conceptualizations of solutions come into play."[16] CIP is just such a policy framework shift.

Although some of the legal authorities and policies within the Critical Infrastructure Protection field existed more than five years ago, such as the Computer Security Act of 1987, the creation and subsequent development of the field can be traced to a recently published core of key documents. The table below is a listing of core documents in the field. This is not an exhaustive listing of recent authorities concerning Critical Infrastructure Protection. However, these documents constitute the core of the new policy field.

Within these documents is the evidence that the US security elites are crossing the threshold of Kuhn's paradigm crisis. The failures and inadequacies of past policies rooted in an obsolete paradigm have sparked these attempts to come to grips with the new reality. They span two US Administrations, yet as the second most recent one notes "Serious deficiencies exist that only a significant organizational redesign can remedy."[17]

Core Document	Dated
Presidential Decision Directive (PDD) 39: US Policy on Counterterrorism	21 June 1995
Executive Order 13010: Critical Infrastructure Protection	15 July 1996
Defense Against Weapons of Mass Destruction Act of 1996	23 September 1996
Critical Foundations: Protecting America's Infrastructures - The Report of the President's Commission on Critical Infrastructure Protection	13 October 1997
PDD 62: Combating Terrorism	22 May 1998
PDD 63: Protecting America's Critical Infrastructures	22 May 1998
The Federal Response Plan	April 1999
Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue	7 January 2000
Road Map for National Security: Imperative for Change	31 January 2001
National Security Presidential Directive – 1 (NSPD-1)	15 February 2001

Table 2 - 1: Core Documents in the CIP National Security Policy Field

[16] Kingdon, p. 113. Ironically, Kingdon's Multiple Streams theory of policy change and formulation, however, when viewed from a Kuhnian perspective, resembles the practice of normal science, between paradigm changes. Given a problem, existing tools are employed to craft a solution, and because of this Kingdon's policy stream recycles past solutions into new solutions. This is not an adequate approach to formulating security policy designed to counter new threats in a fundamentally altered security environment, although it is adequate for the practice of Kuhnian "normal science," during a period of stability in a policy paradigm.

[17] *Road Map for National Security: Imperative for Change*, The United States Commission on National Security / 21st Century (31 January 2001), p. x. Document available at http://www.nssg.gov.

Presidential Decision Directive 39: US Policy on Counterterrorism:

On 24 January 1997 in response to a Freedom of Information Act request from the Federation of American Scientists, the White House declassified and released a heavily-redacted copy of PDD 39: US Policy on Counterterrorism. An unclassified FEMA abstract of PDD 39 had previously been released by the National Security Council (NSC) to Mr. John F. Sopko, the Minority Deputy Chief Counsel for the Senate Governmental Affairs Committee, pursuant to a request from Senator Nunn.[18] PDD 39 outlines US policy concerning both terrorist acts employing conventional munitions or armaments as well as Weapons of Mass Destruction (WMD).[19] PDD 39 states that the US strategy for countering terrorist acts is comprised of four points: 1. Reducing vulnerabilities, 2. Deterring terrorism, 3. Responding to terrorism, and, 4. Preparing for WMD terrorism.[20]

The directive specifies several taskings to reduce US vulnerability to terrorism both domestically and abroad. The heads of all federal departments and agencies were officially put on notice that they bear responsibility for their personnel and facilities' safety. The Attorney General was tasked with chairing a cabinet committee to review US facility and critical infrastructure vulnerabilities, and to make recommendations to the President. The Director of the Federal Bureau of Investigation (FBI) was tasked to expand the US counterterrorism program, while the Secretary of State was ordered to reduce vulnerabilities to all personnel and facilities at non-military sites abroad and to American citizens abroad. The Secretary of Defense was instructed to reduce vulnerabilities to US military personnel and facilities. The Secretary of Transportation's responsibilities included the security of all US airports, aircraft, passengers, maritime shipping under US registration or operating within the United States, as well as responsibility for coordinating the security of rail, highway, mass transit, and pipelines. Denying entry into the US or deporting personnel posing a threat was jointly assigned to the Secretary of State and the Director, FBI. The Secretary of the Treasury was instructed to protect the President and other officials from attack, prevent arms trafficking, and control the movement of other assets. The Director, Central Intelligence was tasked to conduct an aggressive intelligence collection effort including covert action to limit vulnerabilities in accordance with the

---

[18] Unclassified FEMA abstract of PDD 39, undated. Available at http://www.fas.org/irp/offdocs/pdd39_fema.htm.

[19] *Presidential Decision Directive 39: US Policy on Counterterrorism* (Washington, DC: Executive Office of the President, 21 June 1995). Document available at http://www.fas.org/irp/offdocs/pdd39.htm as of 8 August 2000.

[20] This study uses the term Weapons of Mass Effect (WME), which encompasses both Weapons of Mass Destruction and Disruption. However, some policy documents use the term of Weapon of Mass Destruction (WMD). During the below discussion of specific policies, the term WMD is used to accurately reflect these documents' tone and context. However, the study maintains a more precise

National Security Act of 1947 and Executive Order 12333: United States Intelligence Activities (EO 12333).

This section of the document dealing with reducing vulnerabilities did not break new ground. It effectively restated status quo responsibilities and cited long-standing legal authorities. For example, EO 12333 was instituted by the Reagan administration on 4 December 1981. However, it did call for the Attorney General to establish a committee to make recommendations to the President concerning vulnerabilities of US *critical infrastructures*, and it also called for an expansion of the FBI's counterterrorism program. These two points foreshadowed the development of an introspective analysis of US critical infrastructure and the increased importance placed on countering asymmetric threats.

The section detailing activity to deter terrorism stated that the US would "seek new legislation to prevent terrorist groups from operating in the United States or using it as a base for recruitment, training, fund raising or other related activities." Additionally, the directive specified that countries harboring or assisting terrorists would become a focus of US attention, with the possibility of unilateral action to "induce cooperation" and the "return of suspects by force...without the cooperation of the host government" being retained as options available to the United States.[21]

Section 2, paragraph C. directed the Secretaries of State, Defense, Treasury, Energy and Transportation, as well as the Attorney General, Director of Central Intelligence, and the Director of the FBI to maintain their own parochial counterterrorism efforts. From this blanket statement to continue to maintain separate, cross-agency counterterrorism efforts and capabilities, it is apparent that PDD 39 did not envisage bringing the multiple programs dispersed across the federal government together in a more coherent, centralized campaign.

This fractured approach was reinforced in section 3, Responding to Terrorism, paragraph D. Lead Agency Responsibilities. The Department of State is the lead federal agency for international terrorist activity outside of US territory. However, when military force has been authorized, the National Command Authority (NCA) would exercise control.[22] The State Department (DoS) and the FBI are tasked to provide Emergency Support Teams (EST), with DoS responsible for foreign incidents, and the FBI responsible for domestic incidents. The Department of Defense (DoD) is tasked to provide transportation to both DoS and the FBI. The Federal Aviation Administration (FAA)

---

term is WME, and uses this term exclusively, excepting when it would not reflect a specific policy document's language.

[21] PDD 39, section 2, unredacted paragraphs 3 and 4.

retained responsibility for all instances of air piracy, with the Department of Justice (DoJ), acting through the FBI, coordinating with DoS, DoD, and the Department of Transportation (DoT) to resolve terrorist hijackings. As this makes clear, response to any terrorist incident, especially those involving an aircraft originating in a foreign country, crossing national borders and ending up in US airspace, is a challenge to coordinate.

A key component of PDD 39 directly bearing on the subsequent development of the Critical Infrastructure Protection policy field was the tasking of responsibility for consequence management to the Federal Emergency Management Agency (FEMA). The Director of FEMA was tasked to "ensure that the Federal Response Plan is adequate to respond to the consequences of terrorism directed against large populations in the United States, including terrorism involving weapons of mass destruction." FEMA also was tasked to ensure that the states' response plans were adequate and capabilities tested. DoS was tasked to jointly develop a plan with the Office of Foreign Disaster Assistance and DoD to assist foreign populations attacked by WMD terrorism. All agencies participating in counterterrorist operations were directed to absorb the costs of participation. Obviously, the lack of dedicated funding supporting counterterrorist operations participation would have detrimental effects on agencies.

The final section of the directive, Weapons of Mass Destruction, detailed a two-edged approach to countering WMD terrorism. First, the US "shall give the highest priority to developing effective capabilities to detect, prevent, defeat and manage the consequences of nuclear, biological or chemical (NBC) materials or weapons use by terrorists." Second, the directive stated that "there is no higher priority than preventing the acquisition of this capability or removing this capability from terrorist groups potentially opposed to the U.S."[23] This approach focuses on defending and defanging.

PDD 39 did not break with the past security policy paradigm. Many of its details were rooted in past policies, and the document does not display a fundamental shift in how policy was considered or crafted. However, PDD 39 did address two new policy considerations. First, it directed the Attorney General to study vulnerabilities of US critical infrastructures in light of asymmetric threats and make recommendations to the President. Second, it introduced the policy notion of consequence management following WMD use. For these reasons, PDD 39 represents a fluctuation from the old paradigm's equilibrium, but not a radical departure from it.

---

[22] The National Command Authority consists of the President and the Secretary of Defense, or their duly deputized alternates or successors.
[23] PDD 39, Section 4, paragraphs 1 and 2.

Executive Order 13010: Critical Infrastructure Protection:[24]

Executive Order 13010: Critical Infrastructure Protection was a key step towards establishing Critical Infrastructure Protection as an emerging policy field. This order explicitly recognized that the incapacitation or destruction of certain sectors of US industry would have a massive impact on US national security.

EO 13010 defines the critical infrastructure sectors as "telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. The threats the order specified against US critical infrastructure were physical threats against tangible property, and cyber threats employing "electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures."[25]

The order additionally established the President's Commission on Critical Infrastructure Protection (PCCIP). The PCCIP was tasked to produce mission objectives, identify and consult with private and public critical infrastructure stakeholders, assess the vulnerabilities of and threats to critical infrastructure, determine legal and policy issues raised, recommend a comprehensive national policy and implementation strategy, propose statutory and regulatory changes, and produce reports and recommendations.[26]

The order noted that there was "a need to increase coordination of existing infrastructure protection efforts in order to better address, and prevent, crises that would have a debilitating regional or national impact."[27] Until the PCCIP could conduct its analysis and publish its report to advise the President, the Infrastructure Protection Task Force (IPTF) was established in the DoJ, chaired by the FBI, to undertake an interim coordination mission of federal agencies and private corporations. The IPTF included representation from other federal agencies, including DoD and the NSA.

The significance of this Executive Order is that it set into motion a formal analysis that would outline the parameters of the emerging Critical Infrastructure Policy field. It further recognized that a high-powered Commission was required to assess the policy requirements entailed in meeting the new challenges of the security environment. The urgency of the matter was such that the Executive Order mandated the creation of an interagency coordination team, the IPTF, to handle the operational aspects

---

[24] EO 13010 was published in the Federal Register on 17 July 1996 as *Executive Order 13010 – Critical Infrastructure Protection*. EO 13010 is also available through the White House electronic library at http://www.whitehouse.gov.
[25] EO 13010, paragraph 1.
[26] Ibid, section 4.

of protecting the US critical infrastructure until the President could receive and consider the Commission's policy recommendations.

The establishment of a Presidential Commission given explicit Executive Branch guidance on structuring their approach and charged with advising the President increased the "weight" of the analysis. This, in turn, added to the momentum started by PDD 39 in this policy direction, and ensured that bureaucratic inertia would not hinder the emerging policy field's direction. EO 13010 moved off of the past policy paradigm's equilibrium, and began to establish the CIP policy field.

Defense Against Weapons of Mass Destruction Act of 1996 (Nunn-Lugar-Dominici):

On 26 June 1996 the U.S. Senate passed the Defense Against Weapons of Mass Destruction Act of 1996 in a vote of 96—0. The vote indicates an overwhelming consensus of a highly diverse body of leaders. The Act was introduced in the House of Representatives by the Honorable Mr. Spratt, acting for himself and the Honorable Mr. McCollum, during the 104th Congress' Second Session on June 27, 1996. The bill, H. R. 3730, was designed "[t]o take measures to protect the security of the United States from proliferation and use of weapons of mass destruction." It was subsequently referred to the Committee on National Security, the Committee on International Relations, and the Judiciary Committee. The bipartisan co-sponsorship of the bill indicated its wide support.[28]

In his remarks for the Congressional Record incident to introducing the bill, Mr. Spratt made explicit mention to various threats, most notably the Khobar Towers Bombing in Dhahran, the attack by Aum Shinrikyo of a Tokyo subway with nerve gas, the World Trade Center bombing, and the Oklahoma City bombing. These threats, according to Mr. Spratt, demonstrated the need for new legislation to counter new threats.

The House Committee on National Security made a request for executive comment from the Department of Defense regarding the bill on 22 July 1996. There were no other requests for comment from the House, and there were no floor actions in the House regarding the bill. The only mention of the bill in the Congressional Record is Mr. Spratt's introductory remarks. Overall, the bill apparently excited little controversy, and from its same day, bipartisan introduction in both the Senate and House enjoyed wide support.

---

[27] Ibid, section 7.

[28] All details of Congressional activity, votes and records concerning the bill are taken from the Library of Congress' web site, Thomas. Document at http://thomas.loc.gov/.

The Act, hereafter referred to as NLD, for the names of its sponsoring senators, Senators Nunn, Lugar, and Domenici, institutes a program of training and domestic preparedness to counter the terrorist use of a WMD in the United States. To this end, 120 cities were selected to participate over five years in a comprehensive program involving DoD, DoE, FEMA, FBI, and other Federal agencies. NLD is divided into sections: Domestic Preparedness, Interdiction of Weapons of Mass Destruction and Related Materials, Control and Disposition of Weapons of Mass Destruction and Related Materials Threatening the United States, Coordination of Policy and Countermeasures Against Proliferation of Weapons of Mass Destruction, and a miscellaneous section.[29]

NLD is a unique and comprehensive piece of legislation. The Act spans issues from directing the establishment of a National Coordinator on Nonproliferation to directing a long-term series of exercises designed to enhance capabilities to deal with the terrorist use of WMD. The Act is a coherent blueprint that includes details of implementation sufficient to enable Federal agencies to begin their programs with little additional clarification of responsibilities.

The development of NLD is interesting from a policy perspective. It would be hard to find another program of equal magnitude, that cuts across all branches of government and Federal agencies, and includes state and local governments, with an equal voting record in the Senate of, literally, no opposition.

The importance of this act did not go unnoticed in the field of political science. In a memorandum to the United States Senate, Graham Allison, Joseph Nye, and other eminent scholars stated:

> The initiative taken by the Congress in 1996 was a vitally important first step, but further efforts are essential if the United States is to overcome its stark vulnerability to weapons of mass destruction. If the 105th Congress does not continue to strengthen U.S. capabilities to prevent and respond to NBC terrorist attacks, the United States will remain unacceptably vulnerable to mass-destruction terrorism. The threat of terrorist attack with weapons of mass destruction delivered by unconventional means is an even clearer and more present danger to American lives and liberty than the threat of attack by ballistic missiles. It should be met by programs of equivalent imagination.[30]

---

[29] Public Law 104-201 National Defense Authorization Act for Fiscal Year 1997, Title XIV, The Defense Against Weapons of Mass Destruction Act of 1996, at http://www.fas.org/spp/starwars/congress/1996/p1104-201-xiv.htm.

[30] Graham Allison, et al, *Defending the United States Against Weapons of Mass Destruction*, open letter to the United States Senate, 2 June 1997.

The act was a necessary first step to counter WMD terrorism. Its initiatives include: a domestic preparedness program to train first responders of the 120 largest cities from Fiscal Year (FY) 1997 through FY 2001 in monitoring equipment operation, agent monitoring, public protection, and decontamination; the establishment of Metropolitan Medical Strike Force Teams; the development of a Department of Defense Chemical/Biological Rapid Response Team capability; the formation of a Department of Energy team to identify, neutralize, and dispose of nuclear weapons; incorporation into the Federal Response Plan guidance on the use and deployment of the rapid response teams by FEMA, emergency preparedness exercise guidance, changes to U.S. Code required to allow DoD support of operations in the case of WMD use, and the procurement of detection equipment to interdict WMD transfer into the U.S. The act tasked the Secretary of Defense with lead official responsibility for the emergency response assistance program until on or after 1 October 1999.

The Act is comprehensive in its approach. It contains programs that attempt to counter WMD employment from its origins to effects within the United States. One action taken to preempt WMD proliferation in accordance with the Act was AUBURN ENDEAVOR, a U.S.-British operation to airlift fissile material from a nuclear research facility in Tbilisi, Georgia, reported by *The New York Times* in a front-page story on 21 April 1998. U.S. efforts in this regard actually predate the Act, with OPERATION SAPPHIRE, the removal of 600 kilograms of HEU from the Ulba Metallurgy plant in Kazakhstan in 1994, being another example. The Carnegie Endowment for International Peace observed regarding AUBURN ENDEAVOR: "The good news: we're airlifting 10 lbs. of nuclear bomb material from an unstable region. The bad news: there's over 1,430,000 lbs. still there."[31]

NLD describes a far-ranging program to counter proliferation, interdict a WMD if possible, and manage the consequences of WMD use by a terrorist against America's population and critical infrastructure. As such, it is directed against the means of attack and the attack's effects. The initiatives prescribed by the program, however, could serve to manage the consequences of other dangers. The release of a toxic or hazardous material due to factory failure or transportation accident could have identical effects as the use of a chemical agent WMD. The tragedy of Bhopal, India is an example of such an accident. Due to a combination of human and technological factors, on 3 December 1984, a cloud of methyl isocyanate gas, used in manufacturing pesticides, escaped from a Union Carbide plant. Casualty estimates were 6,000 immediate victims, with the ultimate loss of an estimated 16,000 deaths, and over 500,000 people with lingering health problems.[32] A situation

---

[31] "Tbilisi: The Tip of the Nuclear Iceberg," *Proliferation Brief*, Vol. 1, No. 1, Carnegie Endowment for International Peace, 23 April 1998. Document at http://www.ceip.org/programs/npp/nppbrf1.htm.
[32] Bryn Thomas, et al, India, 3rd ed. (Hawthorn, Australia: Lonely Planet, 1997), p. 772.

similar to the Three Mile Island Reactor incident, where a nuclear energy facility almost had a core rupture and meltdown, is another imaginable situation where the Domestic Preparedness program would assist consequence management. Clearly, the Domestic Preparedness portion of the act has utility for managing the consequences of a number of potential accidents and disasters.

A review of speeches by officials in the months leading up to the Bill's introduction reveal many making comments on the issue. In testimony on 27 March 1996 before the Senate Armed Services Committee, Dr. Gordon C. Oehler, the CIA's Director of their Nonproliferation Center stated: "The incidents staged in March 1995 by the Japanese cult Aum Shinrikyo demonstrate that the use of WMD is no longer restricted to the battlefield."[33] The Director, Central Intelligence, Dr. John M. Deutch in a speech before scientists from the nation's Los Alamos, Lawrence Livermore, and Sandia laboratories during a conference on proliferation issues organized by Senator Domenici stated: "I find it interesting that Senator Stevens and Senator Lugar and now myself chose as an example of the challenges we face the Japanese cult Aum Shinrikyo and what it did in the subway system in Tokyo."[34]

NLD represents a significant, but still partial, departure from the past policy paradigm's equilibrium. It created new programs to help State and local governments prepare for consequence management, allocated funds, recommended the establishment of a new position in the Executive Branch's NSC, and identified DoD as the lead federal agency for training and other aspects of consequence management. The Act fails, however, to approach the problem within a new framework, for example a framework of critical infrastructures. It also fails to consider WME other than NBC, specifically cyberweaponry. Nevertheless, the Act significantly advanced the development of the emerging CIP policy field and represents a major effort of the US Congress in beginning to lay the legislative foundations for future efforts.

Critical Foundations: Protecting America's Infrastructures - The Report of the President's Commission on Critical Infrastructure Protection:

The President's Commission on Critical Infrastructure Protection (PCCIP) was the first public – private, interagency national effort to examine vulnerabilities in light of the changed security environment and guided by a new framework of critical infrastructures as opposed to a Cold War paradigm of primarily regions or state actors. This approach fundamentally changed the perspective of

[33] Dr. Gordon C. Oehler, Director, Central Intelligence Agency Nonproliferation Center, in remarks to the U.S. Senate's Armed Services Committee, Washington, D.C., 27 March 1996, document available at http://www.odci.gov/cia/public_affairs/speeches/archives/1996/go_testimony_032796.html.

national security policy analysis from a past geographic and ideological extroversion to a more introspective analysis of Self.[35]

The Commission was established in July 1996 by EO 13010, and was tasked to formulate a comprehensive national strategy for protecting US infrastructures. Chaired by former US Air Force general Tom Marsh, it included senior representatives from industry, academia, and government. The Commission operated in five teams representing eight infrastructures. These teams were:

1. Information & Communications, responsible for evaluating the telecommunications, computers & software, Internet, satellites, and fiber optic industries and systems.
2. Physical Distribution, tasked with examining railroads, air traffic, maritime, intermodal, and pipeline distribution infrastructures.
3. Energy, charged with analysis of the electrical power, natural gas, petroleum, production, distribution and storage national systems.
4. Banking & Finance, responsible for conducting an examination of the financial transactions, stock and bond markets, and the Federal Reserve systems.
5. Vital Human Services, encompassing the national systems for water, emergency services, as well as government services.

The Commission completed its report, *Critical Foundations: Protecting America's Infrastructures*, in October 1997 and submitted it to the President. The report generated significant activity in government, as evidenced by the Executive Orders, PDDs, legislation, and regulations that stem from its recommendations. Although EO 13010 had specified various US critical infrastructures in its tasking to the Committee, the *Critical Foundations* report was the first national document to recommend an integrated national security policy approach that comprehensively addressed the realities of the fundamentally changed security environment.

Until the Commission's effort, the national security elite recognized and countered new threats and vulnerabilities, in varying degrees, by Executive Orders or even *ad hoc* policy responses. For example, *EO 12938: Proliferation of Weapons of Mass Destruction* was published on 14 November 1994. This order stated that "the proliferation of nuclear, biological, and chemical weapons ("weapons of mass destruction") and of the means of delivering such weapons, constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States, and

---

[34] Dr. John M. Deutch, Director, Central Intelligence, Los Alamos, New Mexico, 23 May 1996, document available at http://www.odci.cia/public_affairs/speeches/archives/1996/dci_speech_052396.html.

[President Clinton] hereby declare[d] a national emergency to deal with that threat."[36] Similarly, *EO 13010: Critical Infrastructure Protection*, recognized that the security environment presented a new reality that national security policies could only address through a change in approach so radical it demanded the abandonment of the Cold War paradigm and the adoption of a wholly new framework. These orders and other policy documents, however, foreshadowed the more comprehensive and integrative national strategy recommended by the PCCIP, and did not themselves constitute a comprehensive strategy.

The Commission assessed that US infrastructures were connected in a fragile and complex net of interdependence and potential systemic points of failure. They found that this "interlinkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risk."[37] Other findings that illustrated a fundamental change from the Cold War's past framework were that national borders were irrelevant, government was dependent on private industry protection of the infrastructures necessary to conduct its essential business, and economic security had increased in importance as a national security concern relative to conventional military forces. Several concrete policy recommendations were made by the Commission, paralleling the Commission's following findings:

1. Information sharing across public-private, interagency, intra-industry, and inter-industry actors is inadequate to enable efforts to protect US critical infrastructures.
2. Responsibility for critical infrastructure protection is widely distributed across uncoordinated federal actors, but a large portion of the burden is carried by private industry itself.
3. Infrastructure protection requires integrated capabilities of diverse federal agencies, and special means for coordinating federal response to ensure these capabilities are joined effectively.
4. The challenge facing those charged with protecting critical infrastructures is one of adapting to a changing culture.
5. The federal government has important roles in the new infrastructure protection alliance with industry and state and local governments.
6. The existing legal framework is inadequate for dealing with cyber attacks against infrastructures.

---

[35] Chapter 3 will expand on the concept of how attributes of Self can interdependently influence threats.

[36] *Executive Order 12938: Proliferation of Weapons of Mass Destruction* (Washington, DC: Executive Office of the President, 14 November 1994), p. 1. Document at http://www.fas.org/irp/offdocs/eo12938.htm.

[37] *Critical Foundations*, p. ix.

7. Research and development are not presently adequate to support infrastructure protection efforts.[38]

The above findings reveal the inadequacy of relying on past approaches that have demonstrably failed to address novel problems they were never designed to counter. Looking at the same incidents of past WME use, the PCCIP came to a different conclusion than previous agents; radical change, not incremental fixes were required. The PCCIP made dozens of concrete recommendations to improve the capabilities of the federal government to protect national infrastructures, ranging from legal authorities to legislation to promoting research and development across many disciplines. By their own estimation, the most important conclusion reached by the PCCIP, however, was that there was no basis to conclude anything; rather, it was the start of a process of abandoning past policies and beginning to create completely new policies. This echoes Kuhn's assertion that past paradigms must be destroyed and new paradigms adopted during a crisis. The commissioners state that this "is anything but conclusion. In fact, it is a beginning. Our entire effort is prologue to a new era of infrastructure assurance...Our nation is in the midst of a tremendous cultural change, which will have a profound effect on our institutions."[39]

The PCCIP constituted the Executive Branch's own critical assessment of the security environment, and its recommendations serve as the foundations for a new policy field: critical infrastructure protection. Efforts in this field are predominately not aimed at salvaging past policies, but rather for radically revamping both existing national security policies and federal institutions. The PCCIP's report was preceded by three major articulations of national security policy: PDD 39, EO 13010, and the Defense Against Weapons of Mass Destruction Act of 1996. These policies, in addressing the issue of critical infrastructure protection, demonstrated the need for change of the past approach's framework, and foreshadowed the sharp punctuation of the equilibrium of national security policy. These three policies can best be understood to constitute stop-gap measures. The PCCIP, however, was the first complete recognition of how profound the changes in national security policy would have to be in order to be effective in countering emerging threats, and why. The security policies that followed the PCCIP attempted to abandon old notions rooted in the Cold War, and to fundamentally change the security policies of the United States. As will become evident below, some were more successful than others. However, the PCCIP called for a sharp break with the past. As such it constitutes the best definable point where the new paradigm eclipsed the old approach.

---

[38] Ibid, pp. 21-23.
[39] Ibid, p. 101.

PDD 62: Combating Terrorism:[40]

A White House press release of May 22, 1998 sketched key details of a new counter-terrorism initiative: PDD-62. The directive remains reportedly classified as "For Official Use Only." However, the press release indicates this directive outlines a security environment characterized by the asymmetric attack of America through terrorism using unconventional tools, including weapons of mass destruction and cyber weapons. The directive "creates a new and more systematic approach to fighting the terrorist threat" and establishes the office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism.[41] PDD-62 establishes four interagency groups as a comprehensive structure to address counter-terrorism issues.[42]

According to The New York Times, the occupant of this office is "the man who protects America from terrorism."[43] The position is imbued with a wide scope of powers: "The National Coordinator will oversee the broad variety of relevant policies and programs including such areas as counter-terrorism, protection of critical infrastructure, preparedness and consequence management for weapons of mass destruction." The National Coordinator reports to the President through the Assistant to the President for National Security Affairs, and provides advice on budgets and crisis management guidelines development.[44]

The US Department of Justice (DoJ) published an unclassified abstract of PDD 62. DoJ refers to PDD 62 by the title "Protection Against Unconventional Threats to the Homeland and Americans Overseas."[45] According to this unclassified abstract, PDD 62 reaffirms key provisions of the earlier PDD 39: United States Policy on Counterterrorism, dated 21 June 1995.[46] The abstract cites

---

[40] The White House press release, dated 22 May 1998, refers to PDD 62 by the title of Combating Terrorism. A Joint Doctrine Working Party Information Briefing, dated 15 October 1998, refers to PDD 62 by the title of Protection Against Unconventional Threats to the Homeland and Americans Overseas. The White House press release is at http://www.ciao.gov/press_release/WhiteHouseFactSheet_PDD62.htm. The Joint Doctrine Working Party Information Briefing is at http://www.fas.org/spp/starwars/program/homeland/hdefen/tsld006.htm.

[41] White House Press Release, *Combating Terrorism: Presidential Decision Directive 62* (Washington, D.C.: Office of the Press Secretary, May 22, 1998), pp. 1-2.

[42] Statement of Dr. Jeffrey A. Hunker, Director of the Critical Infrastructure Assurance Office before the House National Security Committee, Washington, D.C., June 11, 1998, at http://www.ciao.gov/sbhunker11june1998.html

[43] Weiner, Tim, "The Man Who Protects America From Terrorism," The New York Times, February 1, 1999.

[44] White House Press Release, *Combating Terrorism*, p. 1.

[45] *Presidential Decision Directive-62*, US Department of Justice Office for State and Local Domestic Preparedness Support unclassified abstract. Document available at http://blackstone.ljp.usdoj.gov/osldps/lib_pdd62.htm.

[46] A redacted version of PDD 39 is available at http://www.fas.org/irp/offdocs/direct.htm.

increased support for counterterrorist operations, including expanded legal authorities, funding, increase in policy agenda status, and international cooperation as positive factors contributing to the effective countering of terrorist acts. Challenges facing counterterrorism policies, including PDD 62, are: terrorist groups' capabilities to employ asymmetric attacks and means; proliferation of knowledge, skills, and WMD capabilities; the decrease in US "cold war" civil defense programs; proliferation of advanced technology; and the United States' heavy reliance on computers to operate and maintain critical infrastructures supporting the US population and economy. In the event of a WME attack, PDD 62 designates the FBI as the lead federal agency, according to this abstract, for crisis management and operational response. FEMA is the lead federal agency for consequence management of the aftermath of a WME's employment. According to this abstract, the Department of Health and Human Services (DHHS) is responsible for supporting efforts to provide medical capabilities resulting from a WME incident.

The tandem release of PDD 62 with its sister PDD 63 reinforces the complimentary nature of the two documents. President Clinton in remarks to the midshipmen at the United States Naval Academy Commencement on 22 May 1998 made clear the close integration between the documents. He announced three national security policy initiatives during his remarks. The first was a "new integrated approach to intensify the fight against all forms of terrorism -- to capture terrorists, no matter where they hide; to work with other nations to eliminate terrorist sanctuaries overseas; to respond rapidly and effectively to protect Americans from terrorism at home and abroad."[47] This first initiative detailed by President Clinton corresponds to PDD 62. In addressing the second initiative, President Clinton described it as a "comprehensive plan to detect, deter, and defend against attacks on...critical infrastructures."[48] This initiative corresponds to PDD 63. Lastly, President Clinton described a "concerted effort to prevent the spread and use of biological weapons."[49]

These three national security policy initiatives considered together comprise a comprehensive strategy to combat asymmetric threats employing a broad span of means from cyberweaponry to biological agents. The policies foresee such employment as most likely in the context of a terrorist attack. The publication of PDD 62 and its companion PDD 63 comprise the publicly-acknowledged benchmark of initial Executive Branch policy for the creation of a critical infrastructure protection policy field. Following the PCCIP's *Critical Foundations* report these three documents fueled the CIP field's momentum. Earlier efforts foreshadowed these documents, but the PDDs are the Executive

---

[47] President William J. Clinton, *Remarks by the President at the United States Naval Academy Commencement* (Annapolis, MD: Office of the Press Secretary EOP, 22 May 1998), p. 2.
[48] Ibid.
[49] Ibid.

Branch's codification, following the PCCIP's lead, of all previous, nascent policy efforts in a publicly available format.

PDD 63: Protecting America's Critical Infrastructures:

The White Paper, *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, was published on 22 May 1998. It is the unclassified version of PDD 63, and is commonly referred to as PDD 63, although that actual document remains classified. The paper outlined the Clinton Administration's policy on critical infrastructure protection.

As noted above, PDD 63 was among the first major Executive Branch policy documents that defined and formally codified a strategic change in thinking in how US military strength, traditionally the instrument of power associated with a great power's influence, could be negated in the foreseeable future by enemies. It proposed that threats, "whether nations, groups or individuals," could attack the United States in "non-traditional ways including attacks within the United States."[50]

Protecting infrastructures is not a novel thought in the history of war. However, the United States had grown accustomed over many decades to the protection afforded by its oceans separating it from past theaters of conflict. PDD 63 also was a forerunner in recognizing that the changing security environment included the increased threat of attacks on the homeland itself. This was a major change in framework for federal and state agencies. Additionally, PDD 63 called for a partnership between the US government and its agencies and American corporations operating its critical infrastructures. Industry has been a major component in every conflict to which America committed, however, this new role for the private sector was different in that now industry was on the "front lines," as seen from PDD 63's perspective. This, of course, was a significant change in perspective for modern corporate leaders who, if they had ever supported a war effort at all with their products, had supported from the sanctuary of American soil, and not in the role of a quasi-combatant.

PDD 63 adopted the structure of critical infrastructure sectors contained within the Marsh Commission's report *Critical Foundations* and EO 13010. This structure was better suited to the security environment's reality of a diverse universe of potential threat actors, hence an increased need to comprehend Self as a critical element in the national security policy calculus. The adoption of critical infrastructures as an organizing framework is an introspective approach to determining what is important and what is vulnerable, hence what must be protected. This is a more intelligent methodology in a security environment where the number and nature of potential threats is too diverse

[50] *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, White House Executive Office of the President, 22 May 1998, p. 1.

to provide the sole compass pointing to the development of a strategy safeguarding national interests. Unfortunately, as Kuhn pointed out, old paradigms sometimes linger. This, coupled with the inherent inertia present in any massive bureaucracy, accounts for the failure to bridge the vision of the CIP policy articulated in the PCCIP report, PDD 62, and PDD 63 to execution in the 1999 version of the Federal Response Plan (FRP), as examined below.

The Federal Response Plan (FRP):

The FRP, an inter-agency plan issued by FEMA in its role of lead federal agency for the plan's coordination addresses "the consequences of any disaster o[r] emergency situation in which there is a need for Federal response assistance under the authorities of the Stafford Act."[51] The plan was first published in 1992, and was updated in 1999. It details twelve Emergency Support Functions (ESFs) by sectors, each under the management of a lead federal agency, ranging from energy, transportation, communications, health and medical services, to public works and engineering, among others. The fact that PDD 63 organized national critical infrastructure protection efforts in accordance with eight critical infrastructures makes clear at the start of even a cursory analysis the potential for disconnects between FEMA's FRP as a coordinated action plan involving dozens of federal agencies and the core policy documents of the CIP national security effort. This is the FRP's critical flaw. Table 2 – 3 shows the disconnects that exist regarding sector designation and lead agencies between the FRP and other core CIP policy documents.

The challenge of national CIP calls for a far-ranging, comprehensive, holistic solution. The scope of the challenge dictates that the entire spectrum of the public and private sectors at the federal, regional, state, and local levels, across multiple sectors, be involved in this solution. The urgency of the problem is such that the solution is virtually required now. Bureaucracies, however, are not known for rapid development of comprehensive solutions to complex problems that cross the boundaries of multiple agencies. The FRP is one of a very few documents that exhibit the basic required traits of a plan that could serve as a comprehensive CIP security policy. Supporting this role, the FRP is an extant, vetted agreement of twenty-three major federal agencies specifying disaster response actions of those agencies, and it represents a significant accomplishment of countless working groups. It was first published in April 1992, and has been successfully implemented in various crises and degrees to respond to natural disasters. Unfortunately, however, it does not structurally conform with the CIP policy field's direction and architecture as outlined by the Executive Branch and core CIP policy documents. Because of this, the potential for considerable confusion exists.

Executive Order 13010 Infrastructures	PCCIP Infrastructures	PCCIP Proposed Lead	PDD – 63 Sectors	PDD – 63 Lead Agencies	FRP Sectors	FRP Lead Agencies
Tele-communications	Information & Communications	Joint DoD & Commerce	Information & Communications	Commerce	ESF 2: Communications	National Communications System
Electric Power	Electric Energy	DoE	Electric Power	DoE	ESF 12: Energy	DoE
Gas & Oil	Gasoline / Oil Production & Storage	DoE	Oil & Gas Production & Storage	DoE	ESF 12: Energy	DoE
Banking & Finance	Banking & Finance	Treasury	Banking & Finance	Treasury		
Transportation	All Sub-sectors	DoT	Avn, Hwy, Mass Trans, Pipelines, Rail, Waterborne Commerce	DoT	ESF 1: Transportation	DoT
Water	Water Supply	EPA	Water Supply	EPA	ESF 3: Public Works & Engineering	DoD/ Army Corps of Engineers
Emergency Services	Emergency Services	FEMA	Emergency Law	DoJ / FBI		
			Emergency Fire Service	FEMA	ESF 4: Firefighting	Ag Forest
			Public Health Services	DHHS	ESF 6: Mass Care	Red Cross
					ESF 8: Health Medical	DHHS
Continuity of Government	Government Services	Office of National Infrastructure Assurance	Continuity of Government Services	FEMA	No Counterpart:	
					ESF 5: Information & Planning	FEMA
			Special Functions:		ESF 7: Resource Support	GSA
			Law Enforcement & Internal Security	DoJ / FBI		
			Foreign Intelligence	CIA	ESF 9: Urban Search & Rescue	FEMA (DoD)
			Foreign Affairs	DoS	ESF 10: HAZMAT	EPA
			National Defense	DoD	ESF 11: Food	Ag

Table 2 – 2: Critical Infrastructures and Lead Agencies by Core CIP Policy Documents

Portions of the 1999 version of the FRP are prompted by *PDD 39: US Policy on Counterterrorism*. This PDD established policy to reduce US vulnerability to terrorism, deter and counter terrorist acts, and improve the government's ability to prevent, defeat and manage the consequences of terrorism. The context of PDD 39 is clearly to protect the US population and critical

[51] The Stafford Act is the legal authority for the Federal Government to respond to emergencies and disasters using military forces; Federal Response Plan, Basic Plan Section 1. Introduction, paragraph 2, at http://www.fema.gov/fema/plan1.html, updated October 11, 1996.

infrastructures, as well as overseas personnel, facilities, and other resources from terrorist attack. The document places special emphasis on WME; in its section four the PDD states:

> The United States shall give the highest priority to developing effective capabilities to detect, prevent, defeat and manage the consequences of nuclear, biological or chemical (NBC) materials or weapons use by terrorists. The acquisition of weapons of mass destruction by a terrorist group, through theft or manufacture, is unacceptable. There is no higher priority than preventing the acquisition of this capability or removing this capability from terrorist groups potentially opposed to the U.S.[52]

PDD 39 was the Clinton Administration's counterterrorism policy that was grounded in the possibility of terrorist WME employment. The PDD also couched the vulnerabilities to terrorist attack in terms of critical infrastructures as an organizing structure. The DoJ unclassified abstract of PDD 39 states that FEMA will ensure the FRP supports consequence management of terrorist attacks against the US population, and if large-scale casualties and infrastructure damage occur, the President may appoint a Personal Representative for these efforts. Additionally, FEMA is responsible for ensuring state response plans and capabilities are adequate and tested.[53] However, the FRP is in fundamental disagreement with the Executive Branch's vision of how CIP is to be accomplished. The twelve ESFs of the FRP cannot be reconciled with the eight critical infrastructures of the other core CIP policy documents, especially in light of the different assignments of lead federal agencies in like functional areas, such as water. Executive Order 13010 through PDD 63 all designate the lead agency for the water infrastructure as the EPA; however, the FRP does not have a water sector, *per se*, but subsumes the water sector within ESF 3: Public Works and Engineering, and assigns lead federal agent status to DoD, specifically the US Army Corp of Engineers.

These disconnects between the FRP and the other core CIP policy documents reveal what is an obvious failure to bridge the Executive Branch's vision of CIP to planned execution by federal agencies. The vision of national infrastructure protection is valid, but the most obvious policy solution, even in its mandated revision following the publication of PDD 63, fails to change to the new reality and disregards the Executive Branch's policy statements.

Turning again to table 2 – 3, this ESF-structured design of the FRP, which predates the designation of eight critical infrastructure sectors designated by PDD-63, is identical to the 1992 FRP version and is outdated in light of prior Executive Branch guidance. The revamped 1999 FRP overlaps

---

[52] *PDD 39*, p. 9.

[53] US Department of Justice, Unclassified Synopsis of Presidential Decision Directive – 39, p. 3. Document available at http://blackstone.ojp.usdoj.gov/osldps/lib_pdd39.htm.

some sector designations with the PDD and other core CIP policy documents, namely communications, energy, and transportation. Other ESFs in the FRP correspond to sub-sectors of PDD 63's Emergency Services sector, specifically firefighting and health. However, other sectors between the two documents do not align and lead agencies designated by the two documents do not always match. As further examples of structural incompatibility, the FRP specifies an ESF for food, which is not addressed by the PDD, and the FRP does not have a Banking and Finance ESF that corresponds to the PDD. The situation is exacerbated by differences in agencies tasked as lead within sectors by the two documents. Obviously, the PDD as a concrete policy articulation of the Executive Branch takes precedence and supercedes the FRP's guidance, itself published by a subordinate agency within the Executive Branch. But, until the FRP is completely restructured and updated, the discrepancies could create confusion during a national crisis.[54]

Clearly, all plans must converge in their intents and taskings, or they will work to cross-purposes. Just as clearly, there can not be a single plan that answers all possible contingencies. However, having different agencies designated as the lead for similar sectors under different policy authorities is inviting, at least, significant confusion during a crisis. Efficiency and efficacy demand that the FRP conform to core CIP policy documents, which it does not in its 1999 version, although ostensibly revamped to conform to emerging CIP policy. PDD-63, because it only deals with cyberstrikes against *critical* infrastructures to the nation, may not address *everything* within the FRP; but, where there is common ground, the plans' concepts of operations, intents, taskings, and other characteristics must converge harmoniously. Matters not addressed by PDD-63 and other core CIP policy documents, such as food distribution or the wide-spread release of CBRN agents, must be addressed by the FRP in a fashion that does not preclude later implementation of other actions under core CIP policy concepts. This is, however, a short-term fix. What is needed is a National Plan that details the protection of critical infrastructures and population, regardless of causes. This plan should be a new FRP, fundamentally overhauled to conform with CIP policy direction, and founded on a different architecture.

Here is the policy challenge: the FRP must address not only natural disasters, but also disasters caused by malicious attacks against US critical infrastructures and population. In many scenarios, the difference in effects will not be affected by a difference in cause. The results of a chemical cloud release, whether due to terrorist attack, normal accidents, or natural causes is identical. The FRP must be applicable to effects regardless of cause, and this will have the additional benefit of

[54] Analysis of the Federal Response Plan and PDD-63 in a cross-walk of the two documents taskings, structure, and other policy details reveals the numerous discrepancies.

making every response to natural disasters a dress rehearsal for disasters caused by Red actors attacking critical infrastructures and population.

If the FRP is to fulfill its stated purpose of addressing "the consequences of any disaster o[r] emergency situation in which there is a need for Federal response assistance," then the design of the FRP and other major Federal directives must converge in their intents and effects. Disjointed tasking of agencies across a spectrum of sectors and scenarios by different plans is dangerous. At the national level there must be a prescriptive, coherent, strategic overview. This is because of the potential for a series of simultaneous threat strikes across the country, staggered in time, and spanning multiple infrastructures, and perhaps concurrent with, or triggered by, a natural disaster. Responding to a national crisis under the aegis of one contingency plan must not render responding to a simultaneous crisis under another plan infeasible. As currently in effect, the FRP contradicts higher policy guidance, and makes a coherent national response to a threat attack on infrastructure problematic. The FRP, after revision in light of PDD-63 and other core CIP policy documents, the Bush Administration's NSPD-1, and subsequent Executive Branch policy guidance concerning CIP, should be the nation's strategic plan to respond to a major crisis. Other plans' intents and effects should converge, not clash, with it.

Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue:

PDD 63 directed the development of a national plan, the National Infrastructure Assurance Plan. On 7 January 2000 the White House published the *National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue.* The short title of the plan, *Defending America's Cyberspace*, accurately reflects the focus of the plan. PDD 63 specifically tasked the National Coordinator, an NSC position it itself created, with the "overall coordination and the integration" of the plan, including subordinate sector plans.[55] The plan was directed to address not only cyber threats, but also physical threats. The plan as published, however, focuses exclusively on the cyber aspects of CIP.

The National Coordinator states the plan at this stage "does not lay out in great detail what will be done to secure and defend" networks, but rather presents a common framework for action.[56] A second plan dealing with how government can assist private industry in securing their infrastructures from disruption is forthcoming. As of April 2001, sectors were involved in drafting input to the National Plan, version two. The plan in its current version 1.0 edition is best understood as a general

[55] PDD 63, p. 4.
[56] *Defending America's Cyberspace*, p. iv.

overview of the issues involved and the tasks ahead. It reviews the threats confronting critical infrastructures, and addresses concerns such as privacy and civil liberties. The plan also makes explicit a series of milestones within a sub-system of ten programs that provides a direction for progress in the CIP policy field.

The plan is organized around three broad objectives. The first objective is to *prepare and prevent*. This objective addresses those actions required to minimize the possibility of an effective attack of critical infrastructures. The second broad objective of the plan is to *detect and respond*. This encompasses rapid detection, quick recovery, and reconstitution of infrastructures following an attack. The last objective is to *build strong foundations*. This final objective of the plan includes the formulation of laws, institutions, and ways to project an enhanced security status into the future.[57]

The plan details ten programs that provide its framework. This programs include:

1. Identify Critical Infrastructure Assets and Shared Interdependencies and Address Vulnerabilities.
2. Detect Attacks and Unauthorized Intrusions.
3. Develop Robust Intelligence and Law Enforcement Capabilities to Protect Critical Information Systems, Consistent with the Law.
4. Share Attack Warnings and Information in a Timely Manner.
5. Create Capabilities for Response, Reconstitution, and Recovery.
6. Enhance Research and Development in Support of Programs 1-5.
7. Train and Employ Adequate Numbers of Information Security Specialists.
8. Outreach to Make Americans Aware of the Need for Improved Cyber-Security.
9. Adopt Legislation and Appropriations in Support of Programs 1-8.
10. In Every Step and Component of the Plan, Ensure the Full Protection of American Citizens' Civil Liberties, Their Rights to Privacy, and Their Rights to the Protection of Proprietary Data.

The program titles are self-explanatory, and collectively the different programs provide a framework within which milestones are specified as intermediate objectives. This programmatic approach is appropriate for a nascent policy field, where many of the facts concerning the issues are not yet conclusively determined or understood. However, it is necessarily an approach with limited utility in specifically addressing particular weaknesses with prescriptive solutions. This situation is

[57] Ibid, p. xi.

further exacerbated by the National Coordinator's lack of formal authority to exercise bureaucratic "coercive" power over the agencies and institutions most responsible for securing infrastructures. Possessing limited authority, and attempting to coordinate such a vast program under conditions of uncertainty and among actors with no formal obligation to cooperate presents a formidable challenge.

Road Map for National Security: Imperative for Change:

The US Commission on National Security / 21st Century was established originally as a Secretary of Defense chartered Senior Advisory Board in July 1998. It was later re-established as a United States Committee under Public Law 92-463, the Federal Advisory Committee Act, and the name changed to its current title in 1999. The Commission's charter was to "conduct a comprehensive review of the early 21st Century global security environment."[58] The USCNS/21 accomplished this in three phases, each with a phase report, and ended their mission in January 2001 with the phase III report *Road Map for National Security: Imperative for Change*. The Commission was a bipartisan panel of fourteen nationally recognized experts and public servants, all with considerable credentials in the field of national security policy.

The Commission made fifty major policy recommendations in their final report, divided into five areas of concentration: Securing the National Homeland, Recapitalizing America's Strengths in Science and Education, Institutional Redesign, the Human Requirements for National Security, and, finally, the Role of Congress. This study concerns chiefly the seven recommendations under the Securing the National Homeland category. However, several other recommendations in the Institutional Redesign category have importance for CIP policy, and the Bush Administration has adopted them in its first NSC national security policy document, NSPD-1, detailed below.

The seven recommendations concerning securing the National Homeland are:

1. "The President should develop a comprehensive strategy to heighten America's ability to prevent and protect against all forms of attacks on the homeland, and to respond to such attacks if prevention and protection fail.
2. The President should propose, and Congress should agree, to create a National Homeland Security Agency (NHSA) with responsibility for planning, coordinating, and integrating various US government activities involved in homeland security. They should use the Federal Emergency Management Agency (FEMA) as a key building block in this effort.

[58]US Commission on National Security / 21st Century, *Road Map for National Security: Imperative for Change* (31 January 2001), p. 1. Document available at http://www.nssg.gov/About_Us/Charter.htm.

3. The President should propose to Congress the transfer of the Customs Service, the Border Patrol, and Coast Guard to the National Homeland Security Agency, while preserving them as distinct entities.
4. The President should ensure that the National Intelligence Council include homeland security and asymmetric threats as an area of analysis; assign that portfolio to a National Intelligence Officer; and produce National Intelligence Estimates on these threats.
5. The President should propose to Congress the establishment of an Assistant Secretary of Defense for Homeland Security within the Office of the Secretary of Defense, reporting directly to the Secretary.
6. The Secretary of Defense, at the President's direction, should make homeland security a primary mission of the National Guard, and the Guard should be reorganized, properly trained, and adequately equipped to undertake that mission.
7. Congress should establish a special body to deal with homeland security issues, as has been done with intelligence oversight. Members should be chosen for their expertise in foreign policy, defense, intelligence, law enforcement, and appropriations. This body should also include members of all relevant Congressional committees as well as ex-officio members from the leadership of both Houses of Congress."[59]

National Security Presidential Directive – 1 (NSPD-1):

The second Bush Administration replaced the PDD document series of the Clinton Administration with a new series of Executive Branch national security documents: the National Security Presidential Directives (NSPD). These document series serve as the instrument for communicating presidential national security decisions, with each Administration starting a new series upon assuming office.

NSPD-1 affirms the continuation of many long-standing NSC conventions, such as the statutory members and advisors, as well as the non-statutory membership of the NSC. The NSC Principals Committee (NSC/PC) and Deputies Committee (NSC/DC) are also continued, and the membership and roles made explicit.

The document abolishes the Clinton Administration's system of Interagency Working Groups (IWG), and establishes NSC Policy Coordination Committees (NSC/PCC). The NSC/PCCs are the main vehicle for continuing actions requiring interagency coordination of policy. They provide the collaborative work and policy analysis that informs the more senior NSC/PC and NSC/DC committees. Each PCC has representatives from the relevant agencies represented on the NSC/DC.

The Bush Administration has adopted both regional and functional areas for the PCCs. Six regional PCCs, chaired by an Under Secretary or Assistant Secretary designated by the Secretary of State, are established. They include a PCC for Europe and Eurasia, the Western Hemisphere, East Asia, South Asia, the Near East and North Africa, and Africa.

Eleven PCCs are established for functional areas, several of which are especially relevant for the focus of this study. The PCCs, and their Chair designation authorities, are shown in the table below:

Functional Topic PCC	Chair Designation Authority
Democracy, Human Rights, and International Operations	Assistant to the President for National Security Affairs
International Development and Humanitarian Assistance	Secretary of State
Global Environment	Assistant to the President for National Security Affairs and the Assistant to the President for Economic Policy in concert
International Finance	Secretary of the Treasury
Transnational Economic Issues	Assistant to the President for Economic Policy
Counter-Terrorism and National Preparedness	Assistant to the President for National Security Affairs
Defense Strategy, Force Structure, and Planning	Secretary of Defense
Arms Control	Assistant to the President for National Security Affairs
Proliferation, Counterproliferation, and Homeland Defense	Assistant to the President for National Security Affairs
Intelligence and Counterintelligence	Assistant to the President for National Security Affairs
Records Access and Information Security	Assistant to the President for National Security Affairs

Table 2-3: NSC Policy Coordination Committees Established by NSPD-1

The Assistant to the President for National Security Affairs, at the President's direction and in consultation with the key NSC statutory members may establish additional PCCs. Each PCC has an Executive Secretary from the staff of the NSC, designated by the Assistant to the President for National Security Affairs.

The Clinton Administration's working groups most relevant for the purpose of this study have been transferred to the PCC on Counter-Terrorism and National Preparedness. These include the Counter-Terrorism Security Group, Critical Infrastructure Coordination Group, Weapons of Mass Destruction Preparedness Group, Consequences Management and Protection Group, and the interagency working group on Enduring Constitutional Government. Also of importance to this study,

[59] Ibid, p. 118.

the Clinton Administration's National Counterintelligence Policy Group has been incorporated into the Intelligence and Counterintelligence PCC, and the Standing Committee on Nonproliferation has been transferred to the Proliferation, Counterproliferation, and Homeland Defense PCC.

The establishment and duties of two PCCs are especially indicative of the recognition of emerging threats employing WME against the US population and critical infrastructure: The Counter-Terrorism and National Preparedness PCC, and the Proliferation, Counterproliferation, and Homeland Defense PCC. These two PCCs, both under the authority of the Assistant to the President for National Security Affairs, are new policy entities active in the CIP policy field. The changed nature of threats are illustrated by the fact that a large number of previously separate national security committees were pooled to better address the threat. This is a clear indication that existing agencies and institutions, even those relatively recently formed under the Clinton Administration, were inadequate to effectively address the national security policy issue of emerging threats to US population and critical infrastructure. This dynamic supports the first and second hypotheses detailed at the beginning of the chapter.

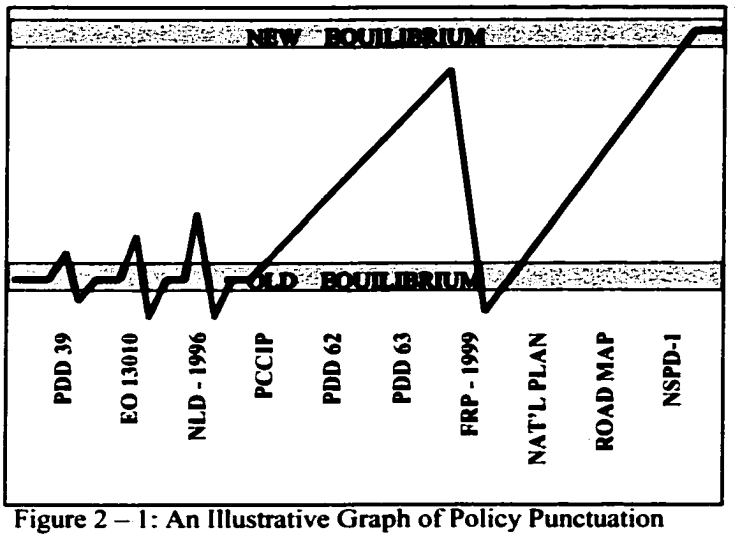


Figure 2 – 1: An Illustrative Graph of Policy Punctuation

Figure 2 – 1 is a strictly illustrative depiction of the punctuations caused by the core CIP policies. Each policy acted to deviate from the old policy paradigm's equilibrium, with the exception of the FRP. The FRP was an attempt to return to the old paradigm's equilibrium following the PCCIP and PDD 62 & 63 series. Before EO 13010 national security policy exhibited a constancy of approach within a band of minor deviation in dealing with unique challenges of the new security environment. This approach can be typified by separate policies founded on a state-centric paradigm dealing with threats in ways that had strong parallels in Cold War policies. PDD 39 was a minor departure from

such a policy of continuation of the obsolete equilibrium. EO 13010 communicated a new vision, although nascent, of a different structure, organized around an introspective assessment of Self, specifically critical infrastructures. It broke from the past approach of crafting national security policy predominately on the basis of an extroverted view of threats within the security environment. The Weapons of Mass Destruction Act of 1996 addressed different threats, but did not structurally depart from a state-centric view of the security environment and an extroverted analysis of threat. Although some mention of non-state actors was superficially discussed, it dealt with principally the danger of proliferation of CBRN agents, technology, and knowledge from Russia and the former Soviet empire. NLD is an important piece of legislation with great utility, but it remains grounded in a past paradigm that largely fails to recognize the landscape of the new security environment. This strictly illustrative line in Figure 2-1 tracing the development of security policy punctuation changed drastically with the publication of the PCCIP's *Critical Foundations*. This document articulated the first coherent vision for national security policy countering emerging threats, and resulted in the Executive Branch's publication of the seminal, core policy documents of the new CIP national security policy field: PDD 62 and PDD 63. These twin PDDs, issued on the same day, fundamental broke with the past paradigm and enthusiastically embrace a framework for policy based on critical infrastructures. The 1999 version of the FRP, however, constituted a significant retrenchment due to bureaucratic inertia and the failure to consider the security environment's context as well as explicit, coherent Executive Branch policy guidance issued the previous year in other core CIP documents. The 1999 FRP can only be characterized as the loss of a significant opportunity to craft a comprehensive, authoritative, and prescriptive policy document supporting the evolution of the CIP policy field and the Executive Branch's policy vision. The National Plan, version 1.0, put the development of the CIP policy field back on track with the emerging paradigm, a trend that has been reinforced by the subsequently published Hart-Rudman Commission's *Roadmap for National Security* and the Bush Administration's NSPD-1.

Figure 2-1's graphing of a strictly illustrative line points out that before a major punctuation of an equilibrium there are sometimes smaller pre-shocks that foreshadow policy directions emerging as practitioners recognize the inadequacy of the current community paradigm. The small shocks are potentially missed in the larger continuity of other policies, but they eventually successfully signal a Kuhnian pre-paradigmatic crisis, and suggest that paradigm shifts are not necessarily complete surprises, provided one only captures the signals within the noise. The shape of the new equilibrium that will eventually emerge after continued growth and maturity in the CIP policy field is still being formed. As mentioned in chapter one, one purpose of this study is to influence this shaping of the policy field. Nevertheless, following the transition of a Presidential Administration, and the inclusion of the new policy framework within the first Executive Branch articulation of national security policy,

NSPD-1, it is likely that the old paradigm will not be revived. Ten years have passed since the end of the Cold War. The US national security elite's community paradigm crisis has caught up with the reality of the security environment.

CIP is a policy field based on normative foundations.[60] Furthermore, it can be described as a valence issue, where only one position can be legitimately maintained.[61] The only tenable domestic position, for example, affirms the desirability of protecting the US population and critical infrastructures from attack. However, differences in priorities, existing bureaucratic turf borders, and the broad, crosscutting nature of the policy field, exacerbated by its rudimentary state of formulation and rapid-paced legislative activity have sparked much controversy concerning the means to achieve the commonly-agreed end. Although everyone may agree that protection is a certifiable good thing, how to obtain that protection can be a contentious issue.

Federal institutions have been created *de novo* to come to grips with these challenges, and other recommendations far more sweeping for changing the Federal institutional structure have been advanced.[62] For example, the Department of Justice founded the National Infrastructure Protection Center (NIPC) within the FBI, acting in response to Presidential directives in PDD 63. Other Federal institutions are also undergoing a process of fundamental change to cope with the challenges posed by emerging threats to US critical infrastructure. Virtually every Cabinet department and dozens of major federal agencies are directly affected by and involved in forging this new policy field.

NIPC is the national focal point for gathering information on threats to US critical infrastructure. It is linked electronically with other warning and operation centers, including Information Sharing and Analysis Centers (ISAC) led by private sector organizations within each of the critical infrastructures. ISACs, at a minimum, maintain secure databases, analytic tools, information gathering and distribution facilities, and subject matter experts. Authorized individuals, corporations, and government agencies submit either anonymous or attributed reports concerning threats, vulnerabilties, incidents, and security solutions to the infrastructure's membership. These reports facilitate the dissemination of security-critical information, early warning and indications, as well as trend analysis, metrics, and benchmarks.

---

[60] James E. Anderson, *Public Policymaking* (New York: Houghton Mifflin, 1997), pp. 53, 141-143. See also Kenneth J. Meier, *The Politics of Sin* (New York: M.E. Sharpe, 1994), pp. 8, 13.
[61] Baumgartner and Jones, *Agendas and Instability in American Politics*, p. 150.
[62] Below a radical proposal is examined that calls for restructuring the US Coast Guard, Border Patrol, FEMA, the US Customs Service, and other federal agencies into a single agency, headed by a newly-

The establishment of ISACs, led by private industry, is "a frank acknowledgement that risk management must be expanded to take into account the potential for devastating effects on a national scale."[63] In the current security environment, the protection of critical infrastructures is beyond the capabilities of both the state and federal governments, and devolves to the private industries that own the infrastructure. The government, however, has the intelligence agencies, law enforcement organizations, and other assets to inform the infrastructure owners of impending strikes. The arrangement is a curious joining where industry has the actual wherewithal and requisite expertise to protect their infrastructures, but no national intelligence feeds or significant legal authority to do so, and the government has the intelligence assets and legal authority to do so, but neither the wherewithal nor the expertise. The ISACs are private – public entities, with membership including multiple industry corporations and groups, that were called for by PDD 63.[64] This arrangement illustrates the changed nature of the security environment; the government is the *consumer* of security provided by private entities, a situation that places Hobbes' Leviathan on its head. The Partnership for Critical Infrastructure Security's (PCIS) *Public Policy White Paper* states:

> To ensure that America's critical infrastructures are protected, the government must work closely with the private sector. In the past, this was simply a question of setting up a command-and-control structure, but there are several reasons why this framework needs to be changed. First, there is a question of resources. By pooling resources, the government can leverage private sector assets, while at the same time, individual companies can tap into larger resources to better safeguard their private interests as well.[65]

The presumption is that private industry will cooperate with state and federal government in protecting infrastructure. But if Hobbes' Leviathan is to be protected by Hobbes' Man, then government must exchange information and intelligence regarding threats with private industry. George Campbell notes, however, that the current relationship between the private sector and the government is a very one-sided arrangement.[66] The private sector's "desire for information...is an often unfruitful, unidirectional activity," but that national security "will increasingly rely upon developing a new order

---

created Cabinet official, called the National Homeland Security Agency. This was the second major policy recommendation of the Hart – Rudman Commission's Phase III report, discussed above.

[63] United States Department of Commerce Press Release (Washington, DC: Office of the Secretary, 16 January 2001), document at http://www.ntia.doc.gov/ntiahome/press/2001/itsac011601.htm.

[64] There are currently three operational ISACs: Telecommunications, Financial Services, and Information Technology. See *Commerce Secretary Mineta Announces New Information Technology (IT) Information Sharing and Analysis Center (ISAC)*, United States Department of Commerce press release 01-16-01 ITSAC (Washington, DC: US Department of Commerce, 16 January 2001), p. 1.

[65] *Public Policy White Paper*, Partnership for Critical Infrastructure Security (March 2001), p. 3. Document available at http://www.pcis-forum.org.

of the business-government relationship to include these private assets as players of critical value in the chain of protection."[67] In short, Campbell believes if Leviathan wishes for protection from Man (specifically, major corporations in this context) then it (the federal government) must cooperate.

This is, of course, by no means an exhaustive listing of the challenges facing national security policy designed to protect the US population and critical infrastructure. New actors armed with novel weapons are able to strike the American homeland directly. The US government at all levels is no longer the provider of security, but is instead increasingly protected by private industry which has no direct, monetary-based interest in protecting the government. Existing institutional arrangements are inadequate to meet the challenges, but entrenched, bureaucratic inertia and turf concerns hamper effective change. Nevertheless, change is occurring, stimulated by the demonstrated failure of past policies to counter threats resulting in tragic events. It is to these types of events stimulating policy change that we now turn.

Background Leading to Change – "Triggering" Events:

Policy is never created *ex nihilo*, and change does not occur without a stimulus. The environment is one exogenous factor that shapes the eventual design of policy. Understanding the milieu surrounding the policy process can provide insight into why policy takes certain designs, as well as why and how change occurs.

The United States has been subjected to or observed a series of extraordinarily spectacular attacks, representative of some emerging threats in the new security environment and contributing to creation of the CIP policy field, in a relatively short period of time. These events served as key "triggering" events as detailed by PE theory."[68] Each of these events involve a non-state actor employing a WME against the United States, a state actor. This study argues that these events, as such, represent the "most probable" future; a security environment where anonymous, non-state actors pursue their ideological, religious, or other agendas using asymmetric attacks (methods) that employ

---

[66] George Campbell is the President of Fidelity Security Services, Inc. He directs Fidelity Investments global corporate security organization. Fidelity is the world's largest privately-owned financial services firm.

[67] George K. Campbell, "Security Expectations for Transnational Corporations," in Max G. Manwaring, ed., *...to insure domestic Tranquility, provide for the common defence...* " (Carlisle, PA: Strategic Studies Institute, 2000), p. 75.

[68] Kingdon uses the term "focusing event" and Baumgartner and Jones use the term "triggering" event. Both are similar. See John W. Kingdon, *Agendas, Alternatives, and Public Policies*, 2nd ed. (New York: HarperCollins, 1995), pp. 94-100; Frank R. Baumgartner and Bryan D. Jones, *Agendas and Instability in American Politics* (Chicago: University of Chicago Press, 1993), pp. 129-130. Although only the PE theory is examined here, the concept of events, or "shocks," precipitating policy change and influencing policy formulation is not limited to just the PE theory.

WME (means) against the US population and critical infrastructures (targets). A brief synopsis of these events is required here:

Event	Date
World Trade Center Bombing	26 February 1993
Aum Shinrikyo Sarin Gas Attack	20 March 1995
Oklahoma City Bombing	19 April 1995
Khobar Towers Bombing	25 June 1996

Table 2 - 4: "Triggering" Events contributing to CIP National Security Policy Field Formation

The World Trade Center Bombing

On 26 February 1993 a large truck bomb exploded in the parking garage under one of the twin towers of the World Trade Center. The attack killed six people and injured more than 1,000. The explosion was the work of two international terrorists: Ramzi Yousef, and his accomplice Eyad Ismoil. The bomb design and placement was intended to collapse one of the two World Trade Center towers into its sister tower, in domino fashion, with both structures then collapsing into surrounding buildings. Open sources suggest that sodium cyanide powder was incorporated into the bomb design to create a lethal cloud in the densely-populated, urban office area. The powder burned, however, instead of vaporizing. Sodium cyanide was found in the bomber's warehouse after the attack. Had the plan fully succeeded some casualty estimates projected up to 50,000 Americans killed. [69]

Because it was a dramatic event, with live coverage showing terrified people fleeing the smoking structure, it had an impact on the public. Classically, terrorists seek publicity of their actions, and this event received massive coverage. Although the bomb itself was of conventional construction, leaving aside the issue of whether it actually did contain sodium cyanide, its size and targeting made the bomb a WME. The number of casualties that potentially could have been inflicted, extensive media coverage, and the fact that at that time it was the most spectacular terrorist strike to date on American soil, ensured it played a significant role as a focusing event for national security policymakers and the American public.

On the eve of the bombing, Yousef boarded a plane to Pakistan, and Ismoil fled to Jordan. The bombers eluded capture until Yousef was tracked down in Pakistan in February 1995, and Ismoil was discovered in Jordan in August 1995. Both terrorists were extradited back to the United States.

The dramatic nature of the event, multiplied by the effects of live television coverage, and the sheer scope of damage, both actual and potential, demonstrated that terrorists were planning operations

[69] Stern, p. 76.

that far eclipsed past terrorist operations both in desired casualties and means employed. The successful escape of the terrorists and their eluding capture for two years underscored as much as the bombing itself the vulnerability of the United States to anonomous, asymmetric attack by individuals using a WMD. It also served to increase the perception of a problem issue that policymakers would ultimately have to confront.

Aum Shinrikyo

Aum Shinrikyo (Supreme Truth) is a Japanese cult founded in 1987 by Shoko Asahara, then a forty-year old legally blind yoga teacher. In 1995 the cult had between 40,000 to 60,000 members around the world, and assets exceeding $1 billion.[70] The cult was responsible for the 20 March 1995 sarin nerve gas attack on a Tokyo subway.[71] Less well known is the cult successfully infiltrated Japanese government and industry, including major corporations, law enforcement and military organizations, and developed an extensive arsenal of chemical and biological weapons. The cult had previously used sarin in at least one other attack, as well as anthrax.[72] The cult had a cadre of highly-educated members to assist them in their production of WMD. The WMD development program was not limited to sarin and anthrax; cult scientists had also travelled to Zaire to obtain a sample of the Ebola virus, as well as manufactured and employed in murders the even more lethal nerve agent VX.

On 27 June 1994, Aum members sprayed the Japanese city of Matsumoto with sarin in a test run before attacking Tokyo. The cult used a specially modified truck equipped with heaters to turn the liquid sarin into a gas for dispersal and motor-driven spray nozzles. Seven people eventually died, and over 500 were injured, with many lapsing into long-term comas.[73]

In another precursor attack on 15 March 1995, the Aum left three attache cases at the Kasumigaseki subway station. Each contained a small tank to hold a liquid, a small motorized fan, a battery, and a vent. These attache cases were dispersion devices for either chemical or biological agents.[74]

On 20 March 1995, the Aum employed containers of sarin positioned on five trains scheduled to arrive within four minutes of each other at the Kasumigaseki subway station during Tokyo's

---

[70] "Global Proliferation of Weapons of Mass Destruction: A Case Study on the Aum Shinrikyo," Senate Government Affairs Permanent Subcommittee on Investigations Staff Statement (Washington, D.C.: U.S. Senate, October 31, 1995), section IV.C. Financial Operations.
[71] The nerve agent sarin is a colorless, odorless liquid that is 500 times more toxic than cyanide gas. Only half a milligram of sarin can kill a person. Exposure to sarin vapor can lead to loss of consciousness in seconds, followed by convulsions, and death by asphyxiation in minutes.
[72] "Global Proliferation," Section II: Preliminary Findings & Questions.
[73] Ibid, Section V, para. B. Matsumoto: A Dry Run For Tokyo.

morning rush hour. The Kasumigaseki station is one of the largest in Tokyo, and is located in the heart of the government office district. The Ministries of Foreign Affairs, Finance, Tax Administration, Labor, Health and Welfare, and both the Tokyo Police and the National Police Agency (the Japanese equivalent of the FBI) are located within walking distance of the subway station. The plan called for cult members to puncture the containers of sarin, targeting commuters within and on trains travelling through the station. The Aum members carried out the attack as planned, but a miscalculation in the preparation of the sarin rendered it less effective than it could have been. Despite the reduced potency of the sarin, the attack killed twelve people and injured 5,500. If not for the faulty preparation and poor dissemination technique, chemical weapons experts calculate causalities would have easily reached the tens of thousands.[75]

The international media carried the story to an incredulous global audience. The intent of the terrorists, taking down a "world city" and a major nation's government institutions, was unprecedented. Even more significant, the terrorists possessed not only the intent, but also the *means* to accomplish their ambitious intent.

The Tokyo subway attack demonstrated that a non-state actor employing WME could directly and effectively attack a sovereign government. Had a simple mistake not been made in preparing the batch of sarin, the ability of the Japanese government to govern would have been potentially compromised due to the loss of thousands of key government personnel in the critical ministries in a single strike.

The Oklahoma City Bombing

Just over a year after the Tokyo subway nerve gas attack, terrorism struck America's heartland. On 19 April 1995, a large truck bomb destroyed the Alfred P. Murrah Federal Building in Oklahoma City. The attack targeted federal governmental institutions. The federal agencies housed in the Murrah Building included the Bureau of Alcohol, Tobacco, and Firearms; the Drug Enforcement Administration; the Secret Service; the Department of Housing and Urban Development; the Social Security Administration; US Army and Marine Corps recruiting offices; the Veterans Administration; the General Accounting Office; the Department of Health and Human Services; the Department of Defense; the US Customs Service; the Department of Agriculture; the Department of Transportation; and the General Services Administration.[76]

---

[74] Ibid, Section IV, subpara. 2: Biological Weapons.
[75] Ibid, Section V, para. C. Tokyo: A Nightmare in the Morning.
[76] *After Action Report: Alfred P. Murrah Federal Building Bombing, 19 April 1995 in Oklahoma City, Oklahoma* (Oklahoma City: Oklahoma Department of Civil Emergency Management), p. 1. Document at http://www.onenet.net/~odcem/aar-final_1_a.htm, as of 13 August 2000.

Consequence management efforts proceeded immediately, with Governor Frank Keating ordering a state of emergency within 45 minutes of the explosion. Representatives from FEMA, FBI, and numerous other agencies including government, business, and volunteer were supporting consequence management efforts within hours. Agencies included the Oklahoma National Guard, the Red Cross, and many other organizations routinely associated with disaster assistance. Some organizations whose support was critical, however, are not typically involved in the consequence management policy planning process. One example is Southwestern Bell Telephone Company which issued free cell-phones to response personnel and provided a dedicated mobile cellular communications control node at the site. This example of private sector support was immensely valuable to consequence management efforts, however, it resulted not from an informed and well-executed contingency plan, but from an *ad hoc* response. The United Parcel Service supported responders with free parcel delivery service, which greatly aided in the shipping of large amounts of equipment required by the responders. Again, the many tons of materials and equipment that was required for the consequence management efforts arrived on – scene because of an *ad hoc*, altruistic contribution of a private entity, not FEMA or any other agency in the US government. The Oklahoma Restaurant Association established free on-site 24-hour food service for responders, a significant logistical operation given the long duration and large size of the response force. Again, an *ad hoc* response of the private sector. This illustrates that the assets available for consequence management are not confined to the public sector. Some of the most potent support, whether logistical, expertise, or operational, resides squarely in the private sector. Yet the past paradigm's policy process failed to adequately address coordination between the public and private sector. Coordination of the private sector's contributions, in fact, were cited as a major deficiency in the official After-Action Review (AAR).[77] This is a major policy design and planning flaw, attributable to its anchoring in an obsolete paradigm of government provision of all security needs.

The conspirators were Americans, unaffiliated with any organization, acting in a small cell. The key attacker acted, to great extent, alone. The bomb's design, targeting, and effects classify it as a WME. The effect was mass casualties; fatalities totaled 168, with 426 people wounded.[78] The principal terrorist, Timothy McVeigh, was only apprehended because of an unrelated traffic stop. These facts illustrate the dilemma confronting critical infrastructure protection policy: literally, a single lone-wolf terrorist can obtain a WME and inflict terrible damage. A small, disciplined cell of terrorists, even if only superficially aware of counter-surveillance techniques to mask their activity, can

[77] Ibid, pp. 4-7.
[78] Ibid, Statistics annex, pp. 1-3.

strike critical infrastructure or the population with a WME at will, and be reasonably confident of remaining anonymous.

Compounding the challenge is the fact that terrorists interested in such attacks include American citizens, in addition to foreign nationals. The domestic terrorist can operate invisibly in American society, which aids in his planning, reconnaissance, targeting, rehearsals, WME weapon procurement, access, and execution of a WME attack against critical infrastructure and population. Given the availability of off-the-shelf technology supporting activities as diverse as secure data transmission to biological agent development, the reality of future WME terrorism is undeniable.

Government agencies are incapable of meeting the requirements of consequence management without the significant resources and expertise of the private sector. This fact necessitates a radical change in how the policy process for dealing with WME consequence management is conducted.

The Khobar Towers Bombing

In November 1995 a car bomb exploded outside a US military installation in Riyadh. The bomb used in that attack contained approximately 250 pounds of explosives. Seven people were killed, including five Americans, and 35 others were injured. This was a rare event in Saudi Arabia, which had before then experienced few terrorist acts. Intelligence indicated that terrorists were targeting US facilities and personnel in Saudi Arabia.[79]

The intelligence proved accurate. Khobar Towers was a high-rise housing complex for US service personnel near the King Abdul Aziz Air Base in Saudi Arabia supporting Operation Southern Watch, charged with enforcing the no-fly zone in southern Iraq. The complex was located in a densely populated, urban environment. On 25 June 1996, two men parked a fuel truck in a parking lot about eighty feet from the base of the building. Sentries immediately initiated an evacuation of the building, but the huge truck bomb exploded minutes after being parked. The force of the explosion caused the high-rise to partially collapse, and killed nineteen American service members. Hundreds of other people, both US and Saudi, were injured. A study conducted by the US Defense Special Weapons Agency concluded that the power of the bomb was equivalent to 20,000 pounds of TNT.[80]

The footage of the devastated building was reminiscent for the American public of the Oklahoma City Bombing. The method of attack, region, and the target also immediately brought to mind the bombing of the US Marines' barracks in Beirut during the Reagan administration. These two

---

[79] William S. Cohen, *Personal Accountability for Force Protection at Khobar Towers* (Washington, DC: Office of the Secretary of Defense, 31 July 1997), p. 1. Document available at http://dtics5.dtic.mil/pubs/khobar/report.html.

[80] Ibid.

bombings followed in quick succession the World Trade Center bombing, the Aum Shinrikyo attack, and the Oklahoma City Bombing. This accentuated the power and reinforcing momentum of the separate incidents as focusing events that called into question existing policy, demonstrated to the American public and security elite that the post Cold War security environment was unfriendly to American interests, that individuals and small groups possessed the capabilities, intent, and opportunities to attack the United States, and that terrorism using WME was a reality.

These four incidents, within a relatively short span of just over three years, fueled the growing consensus within the US national security community to critically analyze vulnerabilities in US infrastructure, both in the continental United States and abroad, from terrorist attack, as well as the nature of threat in the changed security environment. They also conclusively demonstrated the ability of non-state actors to employ WME in novel ways to attack state actors from Asia to the Middle East, as well as in the American heartland. These triggering events when viewed from a state-centric paradigm appear as violent anomalies perpetrated by terrorists. However, the increasing frequency of such attacks, the employment of means and methods designed to inflict massive casualties and not stage "terrorism [as] theatre,"[81] and the asymmetric attack of a state actor by a non-state actor can only be understood within a new paradigm, the Red, Gray, and Blue framework. New theoretical frameworks demand new policy processes.

The intent of all the attacks was similar: cause mass casualties using WME. Following the attacks, it was clear to the US security elite that they were involved in a different environment than the Cold War. Understanding the background, we can now turn to a theory in the policy field to explain the change in national security policy.

Baumgartner and Jones' Punctuated – Equilibrium Theory:

Baumgartner and Jones' Punctuated – Equilibrium (PE) theory of policy change and formulation closely resembles Kuhn's structure of scientific revolutions, and offers a superior theory of security policy formulation given the changed nature of the security environment. The PE theory explains not only policy change, but also policy continuity and formulation. It "emphasizes two related elements of the policy process: issue definition and agenda setting."[82] Issue definition influences the subsequent formulation of policy. They note "As issues are defined in public discourse in different ways, and as issues rise and fall in the public agenda, existing policies can be either

[81] Brian M. Jenkins, "International Terrorism: A New Mode of Conflict," in David Carlton and Carlo Schaerf, eds., *International Terrorism and World Security* (London: Croom Helm, 1975), p. 16.
[82] True, Jones, and Baumgartner, p. 97.

reinforced or questioned. Reinforcement creates great obstacles to anything but modest change, but the questioning of policies at the most fundamental levels creates opportunities for dramatic reversals in policy outcomes."[83]

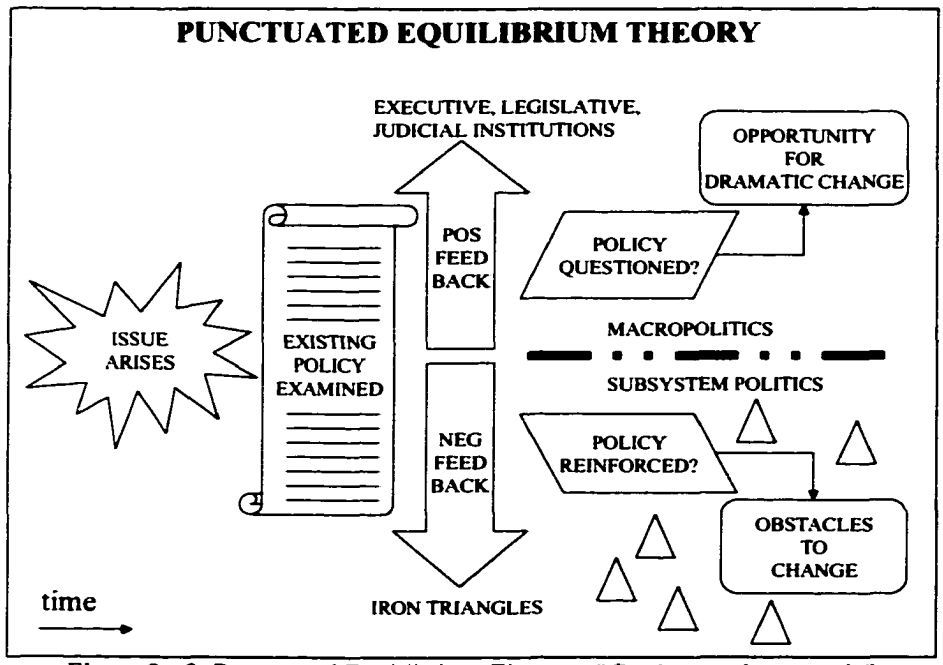


Figure 2 - 2: Punctuated Equilibrium Theory - "Getting on the Agenda"

Baumgartner and Jones state they "demonstrate the validity of a single model of the policy process and of agenda-setting that can explain both stability and rapid change."[84] This treatment of both stability and rapid change corresponds to Kuhn's normal science and paradigm change, respectively. The theory details two levels: a macropolitical system that processes policy issues serially, and a subsystem comprised of many issue networks that processes issues in parallel fashion. The macropolitical level is where the "politics of punctuation" take place, or large-scale change in policy. Within the subsystem level, stasis or incremental change occurs.

The punctuated-equilibrium framework presents public policy as intervals of stability "punctuated," or interrupted, by change. The periods of stability, which Kuhn would see as the practice of normal science by a community within an established and accepted paradigm, are "maintained over long periods of time by two major devices: the existing structure of political

[83] Ibid, pp. 97-98.
[84] Baumgartner and Jones, *Agendas and Instability in American Politics*, p. 4.

institutions and the definition of the issues processed by those institutions."[85] This is a structure-induced equilibrium where the issue definition and institutions form the parameters of the policy field. Change is initiated when either of these two factors is altered. The mechanisms capable of changing the structure-induced equilibria are "policy image and existing institutional venues."[86]

In the CIP security policy case, the "triggering events" in Table 2 - 5 changed the policy image and issue definition of the CIP policy field. No longer were terrorists, for example, seen from a paradigm that *a priori* stereotyped them as a few airplane hijackers in Europe, or bombers in Northern Ireland, or assassins targeting key individuals in the Middle East. The new policy image, spawned by Aum Shinrikyo, was the specter of WME terrorism mounted by a non-state actor achieving system-relevant effects from violence in world-cities like Washington, Berlin, or London. The new issue definition was not how to prevent handguns from being taken onto airplanes or prevent car bombs from being parked next to federal office buildings, but how to prevent the release of nerve gas or biological agents in a large, American city. Following these events, non-state actors came to be viewed as potential threats operating at the strategic level of conflict, and capable of inflicting significant damage to national security interests and challenging sovereign state governments.

According to the PE theory a policy image is how "a policy is understood and discussed." Baumgartner and Jones point out that "every public policy problem is usually understood, even by the politically sophisticated, in simplified and symbolic terms."[87] This is due to the need for policy specialists in the field to communicate the issues and justify the policy to those who lack expert knowledge of the field. Congressional committee members, judges, and senior governmental bureaucrats are all examples of individuals that must understand the core elements of a policy, but who lack the time to learn technical details.

Image is an important matter in the process of formulating policy. How a problem or issue is defined determines which actors can influence the policy. For example, an issue defined as a national security concern will fall within the purview of a specific circle of institutions, committees, and interest groups. However, defining the same issue as a civil rights issue engages different institutions, committees and interest groups. CIP, as a nascent policy field, is still in the throes of undergoing image-shaping by multiple institutions and policy entrepreneurs vying to some extent to gain or maintain influence. This is especially evident following the transition from the Clinton Administration to the Bush Administration; at the time of this writing it is still very much in flux. It will continue until

[85] Ibid, p. 15.
[86] Ibid, p. 38.
[87] Ibid, pp. 25-26.

the new Administration decides on the CIP policy community's boundaries and direction through multiple policy articulations reinforced by action.

This maneuvering in shaping policy image is evident in a recent Senate Judiciary Subcommittee on Technology, Terrorism and Government Information hearing. The hearing was convened to discuss the privacy implications of a national plan for information systems protection. Senator Robert Bennett (Republican, Utah) is not a member of the subcommittee, but has since been named Chairman of the US Senate's Critical Infrastructure Protection Working Group. Bennett presented to the subcommittee his view that cybersecurity is not necessarily a matter for the FBI, but for DoD and NSA. He also pointed out that $2.4 billion allocated to the effort has been spread over 15 agencies, making it difficult to "follow the money." This advocacy of DoD involvement is mirrored in a press release describing how Senator Bennett has introduced legislation requiring DoD to report to Congress on its efforts to "identify, detect and counter the global threat of information warfare."[88] The pressure to directly involve the US Armed Forces in providing "domestic" security by US Senators, Congressmen, and senior career bureaucrats is a different scenario than existed before the fall of the Soviet Union. It reflects both the changed reality and the paradigm shift evident in the CIP field.

"Policy images are a mixture of empirical information and emotive appeals. The factual content of any policy or program can have many different aspects, and it can affect different people in different ways."[89] One of the most powerful tools for portraying emotive images to the broad public is live television coverage. As noted above in the discussion of the triggering events, all of these attacks received significant, intense, sustained media coverage. In the middle of an on-going crisis, the American public is mesmerized by the image of a television reporter expressing shock at the scale of a catastrophe against a video backdrop of destruction. Whether the incident is a bombing or a hurricane, the live coverage propels the incident onto America's consciousness, and often onto macro-political agendas simultaneously. The PE theory states that it is at the macro-political level that the politics of punctuation occur. The television coverage of the Japanese government's efforts to decontaminate the scene after the Aum Shinrikyo's sarin nerve agent attack was a horrific spectacle for many Americans. Long inured to viewing bloody images of bombed streets in Belfast, the bizarre, alien image of workers in bulky space suits moving in a nerve-gas contaminated subway tunnel removing bodies was itself a paradigm shift of sorts for many. International terrorism had long been equated with bloody images of individual victims wounded by bomb blasts or gunshots, and frequently the terrorists were

---

[88] *Bennett Requires Pentagon to Report on Cyber-Defense Plans*, press release of US Senator Robert Bennett, Republican, Utah (Washington, DC, 8 June 2000), p. 1. Document available at http://www.senate.gov/~bennett/bennett_requires_pentagon_to_r.html.

[89] True, Jones, and Baumgartner, p. 101.

also among the casualties in the wake of a counterterrorist team's assault. However, this surreal, sterile portrayal of the consequence management efforts of the Japanese government in the Kasumigaseki subway station visually symbolized the change in threat the new security environment brought with it.

The government is portrayed in PE theory as incapable of dealing with all issues confronting it simultaneously. Yet, attention to the issues is required. Therefore, the majority of issues are managed at the subsystem level, where hundreds of separate issue niches composed of concerned institutions and interested policy actors manage the technical and bureaucratic details. When the subsystem for a given policy is dominated by a single institution that subsystem may be characterized as a policy monopoly. The existence of a policy monopoly is usually reinforced with a powerful "image" that justifies its dominance of a specific issue. As noted, the potential future scene of WME terrorism in American cities is a different image from past images of airplane hijackings. This shift in image can create access into a policy subsystem for different actors, and break up a monopoly of policy influence.[90]

For example, the past policy stance has been that terrorism within the United States is a law-enforcement concern. However, law enforcement agencies lack the expertise, resources, and logistical wherewithal to manage the response to a large-scale CNBR agent attack in an urban area. This has begged the question of whether the issue can be defined as a law enforcement issue by Senator Bennett, and illustrates that the topic is at the macro-political level where the PE theory instructs us that "rapid change" can occur.

The subsystem level consists of numerous "iron triangles," "issue niches," "policy subsystems," or "issue networks."[91] All of these concepts of subsystemic policy entities connote relatively narrow expertise, concern, and focused institutions. The field's actors manage, and in the case of a policy monopoly dominate, the policy. This leads to a phenomenon of "negative feedback," or the inhibition of forces of change. This negative feedback results from established procedures and rules that dictate how the policy subfield will be managed, and also from the protection of status by the subfield's major actors. The FRP's 1999 reversion to its 1992 structure was just such a negative feedback, as portrayed graphically in Figure 2-1. It represented an established policy position coordinated with 23 major actors. Because of this, it is deeply entrenched in bureaucratic inertia. FEMA's failure to conform to the Executive Branch's clear CIP policy direction, as explicitly set forth in higher-level policy documents was an effort to remain rooted in a past policy paradigm.

---

[90] Ibid, pp. 98-101.
[91] Ibid, p. 99.

The triggering events referred to in Table 2 – 4 worked at the emotive appeal level on the American public, and both the emotive and empirical level for the subsystem actors of national security policy. Figure 2 - 2, from left to right, shows the triggering device as an "issue arises" explosion graphic. The existing policy did not survive critical examination, as the scale and intent of the WME attacks by non-state actors were obviously beyond the past conception of what was likely in such an attack, as well as beyond the past capabilities of non-state actors. Clearly, it was a new reality, calling for new policy, and the US national security elite came to realize this fact.

The negative feedback of existing policy subsystem actors did not significantly counter the extreme positive feedback caused by then President Clinton's personal attention and concern. The matter of CIP and WME terrorism rapidly became the highest national security priority: "There is no higher priority than preventing the acquisition of [WME] capability or removing this capability from terrorist groups potentially opposed to the U.S.".[92] Following Figure 2 - 2, existing policy was questioned, and the opportunity existed for dramatic change at the macropolitical level.

Figure 2 - 3 details how the punctuation in a policy era is carried out. Once an issue has ascended to the macropolitical level represented by the positive feedback arrow from the lower level of subsystem politics, it is a high-visibility issue. The institutions of government, as well as other actors including interest groups, actively work the issue. It is here, at this macropolitical level, that past policy subsystems are torn apart, and reconstructed in accordance with the new policy image and issue definition, and then return to the subsystem politics level once the policy field's structure, issue definition, and policy image is deemed complete. This process is continuing as of this writing, as the second Bush Administration begins to articulate its policy guidance.

Because of this, the CIP policy field is still being formed at the macropolitical level, and as stated in chapter one, this study is intended to contribute to that process. Although many initiatives have been accomplished, judging the policy subsystem complete for self-governance and return to the level of subsystem politics is premature. As PDD-39 and subsequently NSPD – 1 showed, it is at the highest national security level, and many issues concerning a myriad of different actors and policy communities are unresolved. From the aspect of cybersecurity, privacy and watchdog interest groups are bringing litigation to bear through the Federal judicial system in efforts to shape the policy field's outlines through the federal judicial venue. The hesitancy of DoD to assume some duties with "domestic" ramifications is a well-known aversion and itself is a subtler attempt to influence the field's shape.

---

[92] PDD-39, p. 9.

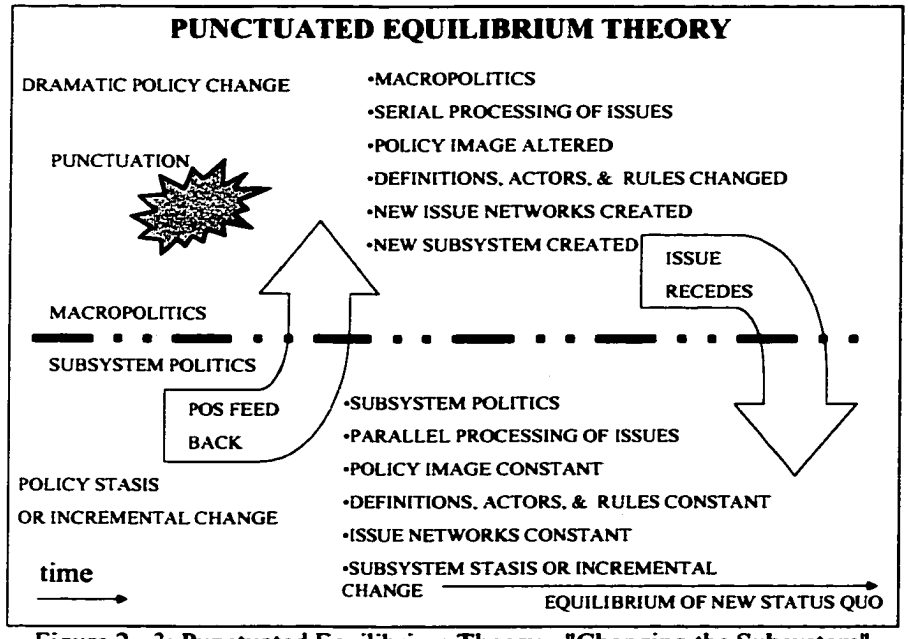


Figure 2 - 3: Punctuated Equilibrium Theory - "Changing the Subsystem"

The goal of an unprecedented long era of consistent US national security policy, the fall of the Soviet Union, is accomplished. Kennan's epiphany has served US security policy well. But, the resulting change in the security environment now demands a new paradigm, as well as theories of policy formulation that explain the changes in security policy and its formulation.

The threat of non-state actors employing WME has prompted an intense effort to mitigate the risk. As table 2 - 1 showed, it has so far generated four publicly-acknowledged Presidential policy documents across two administrations. Congress has allocated billions of dollars to the effort and passed far-reaching legislation. CIP security policy is a dynamic field, and it is rapidly evolving under the Bush Administration's influence.

The PE theory explains in a very simple, straightforward fashion how CIP policy achieved agenda status. However, PE least satisfactorily explains which modifications are probable at the macropolitical level. Beyond stating that new images will be crafted, new rules made, and new issue networks created, it doesn't suggest how any of this will be influenced by past policies. That suggests that the field is in a Kuhnian paradigmatic crisis, where a clear contending paradigm is required to usurp, and in Kuhnian fashion destroy, the old paradigm.

The National Homeland Security Agency and HR 1158:

The US Commission on National Security / 21st Century (USCNS/21) was chartered by the Secretary of Defense in July 1998, and was later established as a federal panel in accordance with the Federal Advisory Committee Act, Public Law 92-463. In its charter the commission was explicitly tasked to recommend changes to the national security apparatus required to implement policies relevant to the changed security environment. Because of this charter's comprehensive reach, the USCNS/21 was the policy vehicle chosen to show the changes required to move from the old security paradigm to a new one. Their response, as shown below, was radical in keeping with the Kuhnian imperative to destroy the old world-view and create a new framework during a period of paradigmatic crisis. It also conforms to the expectations generated by Baumgartner and Jones' explanation of the macro-political level of policy change.

USCNS/21 released its phase III report, *Road Map for National Security: Imperative for Change*, in January 2001. The second recommendation made by the commission to President Bush was to "create a National Homeland Security Agency (NHSA) with responsibility for planning, coordinating, and integrating various U.S. government activities involved in homeland security... [and]... use the Federal Emergency Management Agency (FEMA) as a key building block in this effort."[93] The argument made by the commission is that FEMA is the necessary, but insufficient, key federal agency in safeguarding the United States from asymmetric attacks on its critical infrastructure and responding to terrorist WME employment. Other agencies that are necessary are the US Customs Service, the US Border Patrol, and the US Coast Guard. However, these three "border defense" agencies "are spread across three different U.S. Cabinet departments," and "far from the mainstream of [their] parent department's agenda."[94] The commission argues that melding these agencies into the NHSA will create synergy in their related efforts.

USCNS/21 also called for the President to take steps to recapitalize the three organizations. These agencies are currently underfunded to accomplish their missions, it is argued, and by simultaneously joining the organizations and providing increased resources the agencies would benefit from reduced expenditures for overhead, as well as maintenance and training. Furthermore, the consolidated organization would be able to more easily share critical, time-sensitive information regarding threats. Key to this increased effectiveness is the procurement of an improved information and tracking system, including sensors at the hundreds of access ports to the United States that are

[93] *Road Map for National Security: Imperative for Change*, p. 118.
[94] Ibid, p. 15.

capable of detecting both conventional and nuclear explosives, chemical and biological agents, and other dangerous materials.

The commissioners proposed that the NHSA be composed of three principal directorates: The Directorate of Prevention, Directorate of Critical Infrastructure Protection, and a Directorate of Emergency Preparedness and Response. Additionally, there would be an Office of Science and Technology to advise on research and development, as well as priorities for the NHSA. Within NHSA the commission recommended the establishment of a National Crisis Action Center (NCAC), to coordinate emergency management and federal support during either a natural or man-made crisis. This operation, headed by a two-star National Guard general with full-time representation from appropriate federal agencies, would oversee federal agencies' operations supporting consequence management of a crisis.

The Director of Prevention would oversee and coordinate activities at the terrestrial, maritime, and air points of entry into the United States. The Directorate of Critical Infrastructure Protection is seen as responsible for defending against and countering both physical and cyber threats to the nation's critical infrastructures. This directorate has two vital responsibilities: oversee the physical and cyber components of the US critical infrastructure, as well as coordinate remediation efforts to address vulnerabilities to attacks. In this responsibility the directorate would be operating as the Critical Information Technology, Assurance, and Security Office (CITASO). CITASO is further envisioned by the commissioners as coordinating the Federal Communications Commission (FCC), the Office of Management and Budget (OMB), and the Chief Information Officer Council (CIO Council) contributions regarding cyber policies. Finally, the third directorate, the Directorate of Emergency Preparedness and Response, would broaden FEMA's traditional mission of responding to natural disasters by including responsibility for consequence management of WME employment and other man-made disasters. This directorate is further seen as responsible for integrating DoD and the National Guard, as well as other federal agencies, into the FRP, and including private corporations and sectors, including medical, into the government's efforts to protect critical infrastructure. The National Domestic Preparedness Office (NDPO) within the FBI would be transferred to the NHSA, as well. The commissioners see the transferred NDPO as assuming the task of organizing training for local and state first responders.

The commission additionally foresaw that the NHSA would require a very close working relationship with DoD and the Intelligence Community (IC). Liaison would also be in place with the counter-terrorism centers of the FBI and the CIA. The commissioners envision this liaison as

including not only domestic, but also international liaison with intelligence entities. Given the NHSA's planned role in critical infrastructure protection, the NHSA would also have folded within it existing agencies charged with roles in protecting the nation's infrastructure. These would include the ISACs established by PDD 63, the Critical Infrastructure Assurance Office (CIAO), the National Infrastructure Protection Center (NIPC), and the Institute for Information Infrastructure Protection (I3P).

In the event of federalization by the President of National Guard forces, the commissioners recommended that the Joint Forces Command (JFCOM) assume all responsibility for military operations, and the Secretary of Defense appoint a Defense Coordinating Officer (DCO). During a crisis, the DCO would actually work for a Federal Coordinating Officer (FCO). The President, based on the recommendation from the civilian director of the NHSA, would appoint the FCO. The FCO would oversee all federal efforts during a crisis, and could be the director of the NHSA itself. Thus, NHSA not only would exercise significant law enforcement authorities, but would also exercise control of military forces during a national emergency.

The commissioners additionally recommended that the President order the creation of a homeland security and asymmetric threats portfolio and a corresponding position of a National Intelligence Officer (NIO) within the National Intelligence Council (NIC). Another position to be established would be that of an Assistant Secretary of Defense for Homeland Security within the Office of the Secretary of Defense (OSD). This position would consolidate multiple positions that currently exist within OSD and DoD, and would represent the Secretary during the NSC interagency processes. Creation of these positions elevates the importance of the CIP policy field, and provides it with tangible intelligence and defense resources, including in-house advocates.

This brief and by no means exhaustive overview of the proposed NHSA shows that the policies being advanced to counter emerging threats to US critical infrastructures are radical departures from the incremental policies anchored in the past security paradigm. This major policy punctuation at the macro-political level is indicative of an abandonment of the past policy equilibrium, and the transition to a wholly different equilibrium, in accordance with Baumgartner and Jones' PE theory of policy change and formulation.

The process, as of the time of this writing, is on going, but moving at a rapid pace. The phase III recommendations of USCNS/21 were published on 31 January 2001. On 21 March 2001, less than two months later, the Honorable Mac Thornberry, Republican representative of Texas' 13th District,

introduced in the House of Representatives during the 107th Congress HR 1158, the National Homeland Security Agency Act. This resolution is a comprehensive lift from the USCNS/21 recommendation, which advocates the transfer of authorities, functions, personnel, and assets of multiple federal agencies' departments, like the US Coast Guard and Border Patrol, to the new NHSA, and chaired by a cabinet-level officer. HR 1158 is a mirror of the USCNS/21 recommendations outlined above for the NHSA.

Six days after introducing HR 1158 in the House, the House Committee on Government Reform's subcommittee on National Security, Veterans Affairs, and International Relations held hearings. This is an extremely rapid scheduling of hearings, and indicates broad support for the resolution. The witnesses were:

- The Honorable Warren B. Rudman, co-chair of the USCNS/21 commission.
- General (R) Charles G. Boyd, the Executive Director of the USCNS/21.
- Dr. Bruce Hoffman, a RAND expert on terrorism.
- Lieutenant General (R) James Clapper, Jr., the Vice Chairman of the Advisory Panel to Assess the Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction.
- And, Mr. Frank Cilluffo, Chairman of the Report on Combating Chemical, Biological, Radiological, and Nuclear Terrorism, of the Center for Strategic and International Studies.

Additionally, the Government Accounting Office (GAO) submitted testimony to the sub-committee.

The hearing was convened by Congressman Christopher Shays (R-CT), Chairman of the Subcommittee. This House subcommittee has oversight responsibility of departments and agencies managing programs and activities related to national security, including DoD, FEMA, CIA, and others.

Shays' opening statement confirms expectations generated by the PE theory regarding this policy issue's change and formulation, as well as provides strong support for both the first and second hypotheses detailed at the beginning of the chapter. "Despite large increases in funding to combat terrorism in the last four years, the U.S. government still has no unified threat assessment, no real risk analysis and no coordinated approach to planning, training or funding. We continue to lurch from crisis to crisis using *an accumulated patchwork of presidential directives and agency-specific plans.*

It's time for a more focused, coordinated approach to a pressing national security problem."[95] This "accumulated patchwork" of policy and plans is the product of the PE theory's subsystem politics depicted in Figure 2-3, based on an old policy paradigm that then supported diffusion of roles across multiple federal agencies because the issue was not critical under that paradigm during the Cold War era. The CIP issue's transition, however, to the macro-political level where policy images are altered has changed the policy landscape; definitions, actors, and rules are changing; new issue networks are being created, and a new subsystem is now being established. This is the current state of the CIP policy field, and the "NHSA" in some future form, as made obvious by the above discussion of its proposed roles, composition, and authorities, may become a major new policy actor.

This brief tracing of a CIP policy proposal from a commission's recommendation, to a House of Representatives resolution, to actual hearings, all within two months illustrates the PE theory's serial processing at the macro-political level of a dramatic recommended policy change. As Figures 2-2 and 2-3 illustrate, the PE theory predicts that following significant change at the macro-political level, a new equilibrium will be established and the issue will recede into a newly created subsystem politics level. Currently, however, this process is still on-going, although the issue's past conformation to the PE theory's pattern strongly suggests that the CIP policy field is well on the way to being codified in formal political institutions. Thus, this example of CIP policy reinforces all three hypotheses advanced at the beginning of the chapter.

Conclusion:

This chapter began with three hypotheses. First, if the national security policy community's paradigm framing reality has become obsolete, then policy formulated under this obsolete paradigm will be inadequate to address the new reality, i.e., past policies will prove inadequate in countering emerging threats in the changed security environment. Second, if there has been a shift in that paradigm, then security policy formulation should be changing in an attempt to keep pace with the changed framework as members of the policy community recognize the inadequacy of the old paradigm. Third, if the paradigm is directly relevant to the security policy change and formulation process, then that process must be capable of paralleling the paradigm's pattern of change. This chapter concludes that all three hypotheses are strongly supported by the discussion above.

---

[95] Christopher Shays, Chairman of the House Subcommittee on National Security, Veterans Affairs, and International Relations, Press Release (Washington, DC: 20 March 2001), p. 1. Document at http://www.house.gov/reform/ns/web_resources/news_release_march_27.htm. Italics added.

The PE theory adequately describes how the policy change and formulation process can either experience stasis or undergo dramatic change. The history of the CIP policy field demonstrates both conditions, and corresponds to the paradigm held at a particular moment by the US security elite. The triggering events specified in Table 2-4 led to the formulation of the CIP policy field's core documents detailed in Table 2-1. This corresponds to the PE theory's prediction that a trigger event will prompt the examination of existing policy, as illustrated in Figure 2-2. The negative feedback of an established paradigm is significant, as evidenced by the incremental nature of early CIP policy documents. However as the triggering events continued in a relatively short period of time, and as the US national security policy elite began to question their paradigm, the positive feedback described by the PE theory became stronger. As shown illustratively in Figure 2-1, this positive feedback ultimately succeeded in elevating the issue to the macro-political level, where it is currently undergoing serial processing as of this writing. It is probable, given the CIP policy field's conformation to the PE theory to date, that what will emerge will be a radical departure from past policies, and the establishment of a new equilibrium that conforms to the new paradigm. This process of the PE theory, evidenced by the progress of the CIP policy field, also parallels the process described by Kuhn during a paradigmatic crisis. Baumgartner and Jones' PE theory and Kuhn's theory of Scientific Revolution are remarkable complementary and similar. But anticipating that a new policy equilibrium will be established that conforms to a new paradigm is simply a descriptive analysis of the past and current progress and status of the CIP policy field. That is not a trivial task, but it does not examine, in prescriptive fashion, what the future paradigm should be in the minds of the US national security elite. The study now turns in chapter three to how the US national security elite should view their new world order.

Chapter Three: Red, Gray, and Blue

How do political leaders in varying political cultures and institutional structures approach the task of making calculations, of deciding what objectives to select, and how to deal with uncertainty and risk - that is, more generally, how to relate means and ends, etc.? What styles of political calculation and strategies are developed for this purpose by different leaders?[1]

The purpose of this chapter is to bridge the gap from paradigmatic discussion to an explicit framework that can guide policymakers in formulating security policy.[2] The first chapter presented the current security environment as undergoing a paradigmatic crisis. The second chapter argued three hypotheses, discussion of which demonstrated the need for a new approach guiding national security policy and its formulation. This chapter explicates a security environment approach – Red, Gray, and Blue – that can frame the security environment in a way that meaningfully and pragmatically contributes to defining the problems that security policy must address during this paradigmatic crisis. This framework is graphically depicted in Figure 3-1, and its components constitute the structure of this chapter's sections. Seven possible models of conflict within this framework are introduced.

Alexander George, answering his own question in the above epigraph, argued that understanding the leader's "operational code" was important to understanding the decisions taken and policies adopted. He opens his classic article "The 'Operational Code': A Neglected Approach to the Study of Political Leaders and Decision-Making," by citing Louis Halle, a former State Department planner:

> the foreign policy of a nation addresses itself not to the external world, as is commonly stated, but rather to "the image of the external world" that is in the minds of those who make foreign policy. Halle concludes his book on American foreign policy with a sober warning: 'In the degree that the image is false, actually and philosophically false, no technicians, however proficient, can make the policy that is based on it sound.'[3]

Halle echoes Van Evera's point emphasized above that all policy is based on a paradigm, or as Halle describes "image." George points out that a leader's operational code is comprised of two categories: the philosophical and the instrumental. The philosophical component deals with "what is the 'essential' nature of political life? Is the political universe essentially one of harmony or conflict?

---

[1] Alexander L. George, "The 'Operational Code': A Neglected Approach to the Study of Political Leaders and Decision-Making," *International Studies Quarterly*, Vol. 13, No. 2 (June 1969), p. 198.
[2] Alexander L. George, "Some Guides for Bridging the Gap," *Mershon International Studies Review*, Vol. 38 (April 1994), pp. 171-172.
[3] George, "Operational Code" pp. 190-191.

What is the fundamental character of one's political opponents?"[4] This component of the operational code is at the Kuhnian paradigmatic level of abstraction, or, alternatively, contained within the Lakatosian hard core of a research program. The instrumental portion of a policymaker's operational code concerns "what is the best approach for selecting goals or objectives for political action?"[5] This component of George's construct is at the level of model, or Kuhn's exemplar.

The second chapter's argument demonstrated that Halle's image upon which national security policy is formulated has changed following the end of the Cold War, and that a new one is needed. As he noted, flawed policy remains irreparable until the foundation upon which it rests is made to conform to a more accurate approximation of the reality with which it deals. This chapter presents a graphic depiction and explanation of a security environment approach, presents a model of the approach, and develops the model through a game theory construct, *Stalker*, that dissects conflict between a Self and Other(s) that include anonymous, asymmetric, and asynchronous threat actors. As such the chapter's structure flows from a paradigmatic level of abstraction to seven models based on the Red, Gray, and Blue framework that explicitly depict reality abstractly as well as represent theory. The Red, Gray, and Blue framework and the models based upon it can in a useful, concrete fashion bridge the gap, following George's admonition to scholars researching national security policy. As such the Red, Gray, and Blue framework corresponds to George's philosophical component of the operational code, and the models correspond to the instrumental component.

In chapter 4 the seven models are further detailed and expanded into threat attack decision trees that show threat relationships, decision points, courses of action, windows for perception of threat, and seven different plateaus of threat activity patterns. These decision trees support understanding of the Stalker game's variants the actors are playing, and as such can assist decisionmakers in selecting courses of action, thus corresponding to the instrumental portion of a policymaker's operational code.

Towards an Ontologically Primitive Strategic Framework:

Robert Jervis cites the Law of the Instrument as the aphorism "give a man a hammer and he will find that everything needs pounding."[6] This belief that pounding can solve every problem is partly fostered by the fact that the only tool our "Law of the Instrument man" has for coping with any problem is a hammer. To see a problem as incapable of being solved by his only means available is to

---

[4] Ibid, pp. 201-202.
[5] Ibid, p. 205.
[6] Jervis, *Perception and Misperception in International Politics*, p. 108.

admit his impotence in dealing with a situation. Before conceding helplessness, Jervis' man begins pounding, because it is all he knows.

His action is also partly fostered by familiarity with the tool. His experience in solving problems is limited to the capabilities of the hammer, and his first-hand experience with the tool and its effects condition his perspective – framework – of problems and solutions. He believes, based on first-hand experience, a crushed walnut is the normal, inevitable, and acceptable solution of the problem of cracking it. He has never experienced any other outcome from employing a hammer to crack a walnut, nor has he ever cracked a walnut in any other fashion. His past experiences in his environment have shaped his beliefs. Kuhn notes "what a man sees depends both upon what he looks at and also upon what his previous visual-conceptual experience has taught him to see."[7]

Policymakers, like Jervis' hypothetical man, possess beliefs, which "deal with the most basic images about the nature of the political world and the place and role of the person in it and with the most effective means by which to realize goals."[8] What they know is shaped to some extent by what they have personally seen and experienced first-hand, and their beliefs are influenced by their perceptions. First-hand experience and repetitive use, in turn, creates a "hot cognition" that dominates a policymaker's decisionmaking processes and views of the environment. Strong reliance on these beliefs is a contributing factor to premature cognitive closure regarding the nature of the problem confronting him.[9]

Take the hammer from the man and he will be confused as to how to solve problems. Provide him with a new tool and he will, perhaps painfully, discover its capabilities and limitations as he employs it. The outcomes he experiences may demonstrate to him the superior utility of the new tool in solving certain problems. Place a policymaker in a completely novel situation, with which he has no experience, and he will rely on knowledge and cognitive "intellectual tools" that have served him in the past.[10] Instruct him in the dynamics of the situation, including frame of reference, appropriate role, and action and he will perhaps use this new knowledge. If employed successfully, he will add this "hot cognition" to his repertoire.

---

[7] Kuhn, *The Structure of Scientific Revolutions*, p. 113.
[8] Yaacov Y.I. Vertzberger, *The World in Their Minds: Information Processing, Cognition, and Perception in Foreign Policy Decisionmaking* (Stanford, CA: Stanford University Press, 1990), p. 114.
[9] Ibid, p. 325.
[10] Kuhn, *The Structure of Scientific Revolutions*, p. 46.

In this aspect of learning the man in Jervis' Law of the Instrument, or the policymaker, resembles Plato's prisoners in the cave. His understanding of the environment is predicated on what he has observed, as Plato's prisoners base their understanding of reality on their observation of shadows cast on the wall of the cave by the real world outside.[11] Our man's difficulty in employing a new tool is analogous to the prisoners' pain in Plato's allegory upon being dragged outside of the cave into the bright sunlight. The policymaker's uncertainty and awkwardness in a novel situation is akin to this as well.

A policymaker's beliefs are his intellectual tools, and are not easily changed. Margaret Hermann states "by *beliefs* we mean the political leader's fundamental assumptions about the world and, in particular, political reality. Are events predictable, is conflict basic to human interaction, can one have some control over events, is the maintenance of national sovereignty and superiority an important objective of most nations? Answers to questions such as these suggest some of a political leader's beliefs. A political leader's beliefs are proposed by many...to affect his interpretation of his environment and, in turn, the strategies which he employs."[12] As Plato points out in *The Republic* concerning the prisoners' perspective "men would believe the truth to be nothing else than the shadows."[13] Shadows have been all they have experienced in their past. Hermann's point reflects Plato's thought that a "political leader's fundamental assumptions" define his political reality and shape the strategies he employs. In effect, beliefs, values, and stereotypes relevant to the security environment shape a political leader's definition of a situation and his strategic framework.

The fundamental nature of beliefs, and their importance to political leaders in navigating complex issues, makes them resistant to change. Jervis points out that the Iranian revolution surprised most policymakers because they believed the Shah was strong and in control of SAVAK, the large and brutal internal security force of Iran's Ministry of Security. Other beliefs also contributed to policymakers' inability to recognize imminent revolution in Iran, including the belief that the Shah, as a modernizing force, enjoyed the support of the political elite, and that religious-based opposition did not constitute a serious political threat.[14] These beliefs, or intellectual tools, informed the policymakers' strategic framework of Iran's actors and environment. The framework ultimately

---

[11] Plato, *The Republic*, book XII, sections 514a – 521b, in G.M.A. Grube, trans., *Plato's Republic* (Indianapolis: Hackett, 1974), pp. 167-173.
[12] Margaret G. Hermann, "Introduction: A Statement of Issues," in Margaret G. Hermann and Thomas W. Milburn, eds., *A Psychological Examination of Political Leaders* (New York: Free Press, 1977), p. 21.
[13] Plato, book XII, section 515c.

proved false causing the policymakers to be surprised at the Shah's overthrow by the Ayatollah Khomeini. They misinterpreted the platonic "shadows" of Iran, the nature of the Iranian revolution, the Iranian people, the Shah, and the Ayatollah on the wall of their perception of the security environment – their platonic cave. They misinterpreted the situation, or shadows, because their beliefs, or intellectual tools, were inappropriate for interpreting objective truth. Their strategic framework was in error. They conformed with Jervis' Law of the Instrument; what they believed defined their perception, instead of the reality defining the perspective.

A strategic framework is not synonymous with operational code. Operational code is tied to an individual actor, whereas strategic framework is at a prior, higher level of abstraction and may be shared by many individual actors. Additionally, a strategic framework is theoretical in purpose, in that it is a "world view" of how the security environment runs. An operational code is more operational in purpose, oriented toward providing decisionmaking tools in resolving issues. As such, it is more pragmatic in nature.

A group's collective beliefs, values, perspectives, and stereotypes comprise a shared strategic framework of the security environment. The Reagan administration's strategic framework, simplistically sketched here to illustrate only a basic point, was that the security environment consisted of two camps. The free world's nations were the forces of good, and the Soviet Union was an "evil empire."[15] The essence of the relationship was ideologically-based conflict. The objective of the opponent was to maximize power, influence, and control and to pursue an expansionist policy of global communist revolution to the end of oppressing free peoples. The best counter to the opponent was to confront him from a position of strength. George Kennan's authorship of the policy of containment founded this strategic framework of the security environment. In his Long Telegram, Kennan first described Red:

> In summary, we have here a political force committed fanatically to the belief that with US there can be no permanent modus vivendi, that it is desirable and necessary that the internal harmony of our society be disrupted, our traditional way of life be destroyed, the international authority of our state be broken, if Soviet power is to be secure. This political force has complete power of disposition over energies of one of world's greatest peoples and resources of world's richest national territory, and is borne along by deep and powerful currents of Russian nationalism. In addition, it has

---

[14] Robert Jervis, "Perceiving and Coping with Threat," in Robert Jervis, Richard Ned Lebow, and Janice Gross Stein, *Psychology and Deterrence* (Baltimore: The Johns Hopkins University Press, 1985), p. 19.

[15] Ronald Reagan, *Remarks at the Annual Convention of the National Association of Evangelicals in Orlando, Florida*, March 8, 1983. Document available at http://www.reagan.utexas.edu/reagan/resource/speeches/1983/30883b.htm

> an elaborate and far flung apparatus for exertion of its influence in other countries, an apparatus of amazing flexibility and versatility, managed by people whose experience and skill in underground methods are presumably without parallel in history. Finally, it is seemingly inaccessible to considerations of reality in its basic reactions. For it, the vast fund of objective fact about human society is not, as with us, the measure against which outlook is constantly being tested and re-formed, but a grab bag from which individual items are selected arbitrarily and tendenciously to bolster an outlook already preconceived. This is admittedly not a pleasant picture.[16]

In the beginning of his Long Telegram, Kennan sketched the international security environment – Gray – from a Soviet perspective. The environment described by Kennan from the Soviet perspective was Hobbesian and pragmatic *realpolitik*. Kennan then made concrete recommendations from this previous analysis of Red and Gray for Blue. Of course, he did not explicitly follow the Red, Gray, and Blue framework, yet in reading the Long Telegram this is the telegram's structure. In a phrase strongly paralleling Clausewitz's dictum that the first strategic step is to understand what one is confronting, Kennan stated that "Our first step must be to apprehend, and recognize for what it is, the nature of the movement with which we are dealing."[17] Such was Kennan's epiphany of a framework, as detailed in chapter two. Each Administration, explicitly or implicitly, consciously or unwittingly, has a framework.

The Clinton administration's strategic framework of the security environment differed markedly from the Reagan administration's framework. Following the Clinton administration's perspective, again at a high level of abstraction to concisely communicate its gist, the security environment is comprised of states as the principal political actors, and the triumph of capitalism has destroyed competing ideologies. The relationship between states is one primarily of trade and the expansion of shared liberal values. Those states not yet fully integrated into the core would be well-served by adopting democratic forms of government and actively seeking increased participation in the "world village."[18]

A policymaker's strategic framework is analogous to the Law of the Instrument man's hammer, or Plato's prisoners' understanding of the shadows on the wall of the cave. A strategic

---

[16] George F. Kennan, "The Long Telegram," transcribed from Foreign Relations of the United States, 1946, vol. VI: Eastern Europe, The Soviet Union. Department of State Publication 8470, (Washington, DC: Goverment Printing Office, 1969), pp. 696-709, part 5.
[17] Ibid. Clausewitz noted "The first, the supreme, the most far-reaching act of judgement that the statesman and commander have to make is to establish by that test the kind of war on which they are embarking; neither mistaking it for, nor trying to turn it into, something that is alien to its nature. This is the first of all strategic questions and the most comprehensive." *On War*, pp. 88-89.
[18] William J. Clinton, *A National Security Strategy for a New Century* (Washington, DC: Executive Office of the President, December 1999).

framework shapes how individuals and groups comprehend the security environment and national security issues. It includes beliefs and stereotypes relating to the security environment, as well as accepted theories of how the security environment works. As it pertains to security issues, aspects of a strategic framework can be shared among a small "in-group" of elite policymakers.

This study's security environment approach – the Red, Gray, and Blue paradigm – is examined next.

A Security Environment Approach:

Kuhn cites Bacon's dictum "Truth emerges more readily from error than from confusion" as a worthy starting point for research.[19] To this end, assumptions made are best made explicitly. Every theory assumes some conditions. When made explicit, the assumptions guide researchers and critics to the limitations of a theory. But Van Evera cautions researchers, stating:

> One does not test a theory by assessing the validity of its assumptions...A test asks: 'Does the theory operate if the conditions that it claims to require for its operation are present?'...The validity of a theory's assumptions does affect its utility, however. Assumptions that never hold give rise to theories that operate only in an imaginary world and thus cannot explain reality or generate policy prescriptions. The most useful theories are those whose assumptions match reality in at least some important cases.[20]

Lakatos, like Van Evera, agrees that a theory's hard core assumptions are not tested: "All scientific research programmes may be characterized by their '*hard core*'. The negative heuristic of the programme forbids us to direct the *modus tollens* at this 'hard core'."[21] Although assumptions are not tested, understanding when and where a theory is relevant, as Van Evera points out, requires knowing the theory's assumptions. This, in turn, requires they be made explicit.

First, this study takes the position that First and Second Image Actors are unitary, and intend to be rational, caveating the concept of rationality with the observation that culture, and especially metaphysical beliefs, may dictate what appears rational to a particular actor. Second, the study takes the relationship between systemic actors in the world political system as essentially conflictual. The possibility of cooperation and the insights of Wendt's constructivism, however, are not only conceded but adopted as evident below. The conflictual nature of a primitive anarchy does not mean that all relationships and outcomes of actors' interactions must necessarily be conflict in a deterministic sense.

---

[19] Kuhn, *The Structure of Scientific Revolutions*, p. 18.
[20] Van Evera, p. 40.

Third, the framework views the world political system as anarchic. Fourth, systemic actors pursue ends through employment of power. Morgenthau's concept of power is adopted, specifically:

> Power may comprise anything that establishes and maintains the control of man over man. Thus power covers all social relationships which serve that end, from physical violence to the most subtle psychological ties by which one mind controls another. Power covers the domination of man by man, both when it is disciplined by moral ends and controlled by constitutional safeguards, as in Western democracies, and when it is that untamed and barbaric force which finds its laws in nothing but its own strength and its sole justification in its aggrandizement.[22]

However, the Red, Gray, and Blue framework does not accept, as Morgenthau does, that power is necessarily *the* end. Power is fundamentally a means, and in cases where the aggrandizement of power is the end of a specific policy, it begs the question of why more power is sought. If viewed as an end, power can only be an intermediate objective that later serves as the means toward a subsequent end. This study adopts Wendt's formulation that identity determines interests: "In sum, the ontology of international life that I have advocated is 'social' in the sense that it is through ideas that states [actors] ultimately relate to one another, and 'constructivist' in the sense that these ideas help define who and what states [actors] are."[23] In turn, interests dictate whether and how power is exercised, as well as which types of power are relevant. Again, Wendt points out "Power may be everywhere these days, but its forms vary in importance, and the power to engage in organized violence is one of the most basic. How it is distributed and regulated is a crucial problem."[24] Wendt and Morgenthau agree that power is constituted in many forms, but they part company over the question of whether power is an end. Wendt, consciously or not, follows Clausewitz's classic dictum when he states that interests are the drivers of an actor's behavior and the various forms of power merely tools.

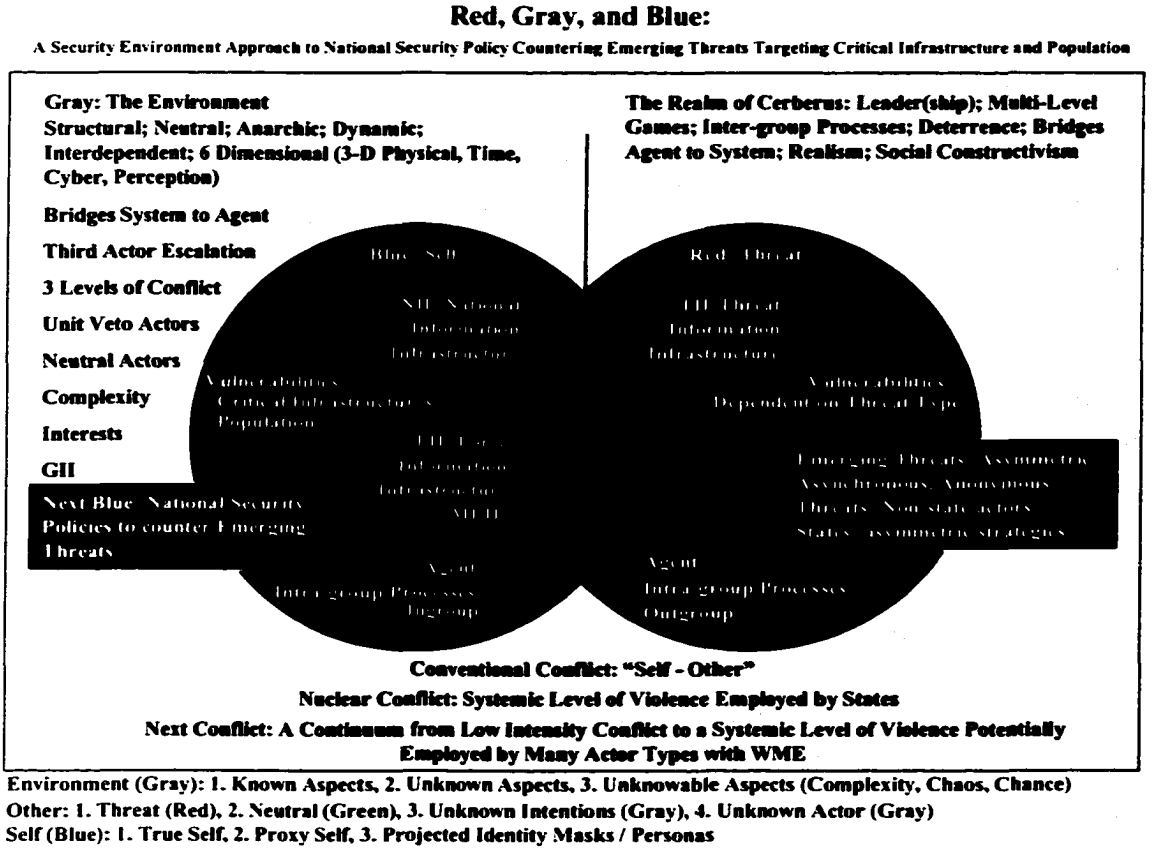
The Red, Gray, and Blue Framework:

The Red, Gray, and Blue framework depicted in Figure 3-1 below is not only the topic of this chapter, but also this chapter's concrete structure. The sections below discuss and explain the concepts behind each of the framework's major components listed in the graphic.

---

[21] Lakatos, p. 133.
[22] Hans J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*, p. 9.
[23] Wendt, *Social Theory of International Politics*, p. 372
[24] Wendt, *Social Theory of International Politics*, p. 8.

This framework of a security environment approach to national security policy countering emerging threats targeting critical infrastructure and population is the functionally adequate paradigm for describing and explaining the altered security environment.



Environment (Gray): 1. Known Aspects, 2. Unknown Aspects, 3. Unknowable Aspects (Complexity, Chaos, Chance)
Other: 1. Threat (Red), 2. Neutral (Green), 3. Unknown Intentions (Gray), 4. Unknown Actor (Gray)
Self (Blue): 1. True Self, 2. Proxy Self, 3. Projected Identity Masks / Personas

Figure 3 – 1: The Red, Gray, and Blue Framework

The Security Environment and the Security Dilemma:

The security environment in which an actor finds itself is constituted by three elements: Self, Other(s), and the Environment. These three constitutive elements of the security environment are interdependent in shaping their individual and collective identity, each subject to the influence of the others.

The concept of Self and Other being mutually constitutive is a core element of conventional constructivism, and is perhaps most famously detailed in Hegel's analysis of lordship and bondage

(*Herrschaft und Knechtschaft*) in chapter four of his *The Phenomenology of Spirit*. A simple analysis of the intersubjective relationship between Self and Other(s), however, potentially ignores the effects of Environment. At best, such an analysis of a strictly bounded Self – Other relationship is a dyadic study of a conditional, fleeting reality that excludes influences exogenous to the dyad, including space, time, roles, persistent interests, and other variables. A specific situational context may or may not be important, but, in any event, it is not complete.

The environment is the medium (or, media) within which Self and Other operate. The environment is not limited to physical space, although it may have physical dimensions. The environment is also constituted by intangibles such as interests and may not occupy any physical space. For example, an interest in the control of oil brings together in a common security environment several diverse actors who otherwise may not have interacted with each other in the same way, if at all. This security environment can be described as those actors concerned with control of oil. The specific aspects of an environment influence which actors participate in a shared security environment. The control of oil, of course, also has geographic, economic, and many other implications. This fact leads to other security issues concerning territory, alliances, and trade that will influence other actors to enter the security environment as a participant. The environment is constituted by an interest in the control of oil, among other factors.

The security environment should be understood as triune in nature. A common metaphor depicting triune entities is a shamrock. Although comprised of three leaves, it, nevertheless, only constitutes one shamrock. The security environment in which an actor exists should be understood analogously as constituted by three elements: Self, Other(s), and Environment.

Unlike the leaves of a shamrock, the elements within a security environment can significantly influence the characteristics of the other elements. This is a key insight of the constructivist approach. Unlike a simplistic interpretation of neorealism that views actors in the international system as undifferentiated entities called states, with undifferentiated interests and capabilities,[25] the constructivist approach allows a broader ontology of actors which, by not accepting an *a priori* conception of the constitutive elements of the security environment increases theoretical richness of description, explanation, and prediction, albeit at the expense of parsimony and, thus, arguably theoretical power.

---

[25] This is not Waltz's view. Waltz asserts that states are the predominant actors in the system, not the only actors, and that "structures are defined not by all of the actors that flourish within them but by the major ones." He continues by stating "Although states are like units functionally, they differ vastly in their capabilities." Waltz, *Theory of International Politics*, p. 93, p. 105.

Self (Blue in Figure 3-1), as one of the constitutive elements of the security environment, can be further delineated into true Self, the actual identity of the actor; proxy Selves, or other actors that ally with true Self to achieve objectives supporting ends that true Self desires; and Identity Masks, representative of a Self created to obscure or alter aspects of Self's nature. Identity Masks are explained in further detail below. Close allies may be regarded as proxy Selves, in so far as they pursue objectives supporting ends that true Self desires. True Self may be assisted by proxy Selves when its ends require the attainment of objectives that true Self may be constrained in pursuing. The means employed in attaining specific objectives supporting desired ends may only be capable of being employed by a proxy Self. An example is the activation of a specific intelligence asset or technique possessed by proxy Self, on behalf of true Self. A hypothetical example would be Israel's Mossad operationally assisting the Central Intelligence Agency. The diverse capabilities of allies can act together in a synergistic fashion to make the attainment of objectives supporting common ends possible, whereas a unilateral course of action would perhaps be less capable of achieving these objectives.

Other, the second constitutive element of the security environment, can be understood as having four sub-categories. The first sub-category is Threat (Red), an actor that has both the capability and intent to harm Self. The second sub-element is a neutral actor (Green), which is neither for nor against Self. A neutral actor, however, potentially may be turned to either an ally or a threat, dependent on the social interaction between Self and the neutral actor. The third sub-category is an actor of unknown intentions (Gray), which may be friendly, neutral, or hostile. It is important that Self act in a friendly, but guarded manner, when interacting with an actor of unknown intentions, as the social interaction itself may influence how the relationship evolves; treating an actor of unknown intention as an enemy may prove a self-fulfilling prophecy. The fourth sub-category of Other is an unknown actor (Gray). Within the security environment there exist many actors, some of which are virtually unknown. It is a mistake to infer that an unknown actor is an inconsequential actor. The Japanese cult Aum Shinrikyo, for example, was a virtually unknown actor on the international scene until it attacked a Tokyo subway station with sarin. Unknown actors may be very capable entities with hostile intent, or may be unanticipated allies. Gray actors partially constitute the environment's effects.

The third constitutive element of the security environment is the Environment (Gray). The environment is, in turn, comprised of three elements. The first sub-category are the *known aspects* of the environment that influence actors and their capabilities, intents, actions and other aspects. The

second sub-category are those traits of the environment that are unknown, *unknown aspects*, but which could be determined and assessed given awareness of their existence. These unknown aspects of the environment may be discovered through study and analysis of the environment (in which case, they then become members of the first sub-category: *known aspects*), or they may be created as a result of technological or other change. These unknown aspects can be understood at the same level of comprehension as the first sub-category of known traits if they are discovered. The two Gray actors, an actor of unknown intentions and an unknown actor, exert influence through this unknown aspects category. The influence exerted by the unknown aspects may be constant, or they may be variable. The third sub-category of the environment are *unknowable aspects*. Some aspects of the Environment can not be fully comprehended, calculated, or accounted for in models such as the play of the elements of chance, complexity, and chaos.

Other	Environment (Gray)	Self (Blue)
Threat (Red)	Known aspects	True Self
Neutral Actor (Green)	Unknown aspects	Proxy Self (should there be a proxy, then true Self and proxy Self mutually constitute Blue)
Actor of unknown intentions (Gray)[26]	Unknowable aspects	Identity Mask
Unknown Actor (Gray)		

Table 3-1: *Constitutive Elements of the Security Environment*

Neorealism is an influential theory of international politics. However, it is limited in its utility for analyzing the politics between unlike actors and non-state actors. During several periods of history, states were, arguably, almost exclusively the actors operating at the systemic level of politics. Neorealism serves well as a theoretical framework for security environments so constituted. Increasingly, however, non-state actors have attained capabilities that are able to affect system influence. Failure to appreciate change in the security environment, and thus the need to potentially change theoretical perspectives, is a dangerous mistake for a national security policymaker.

The concept of security environment is not synonymous with the world political system, except at the most macro-level. Security environments can be defined by different variables, including geography, time, and functional issues. For example, a geographically defined security environment would be a regional arrangement. And viewed over time, security environments can change in the

[26] An actor of unknown intentions and an unknown actor are categories of Other, however their effects and influence, since incalculable as an independent variable are encompassed within the unknown aspects category of the environment. In a multivariate regression model these effects are encompassed within alpha (α) and epsilon (ε) in the equation $Y = \alpha + \beta_1 X_1 + \beta_2 X_2 + \ldots + \beta_i X_i + \varepsilon$.

composition of their constitutive elements. An example of a functionally defined, changing security environment would be the nuclear powers. Although security environments could be defined by a single factor, like geography, it is more realistic to expect that multiple factors influence whether a specific actor participates in a given security environment. For example, the United States is simultaneously considered an important actor in both the European and Asian regional security environments, although geographically it is, obviously, not located in either Europe or Asia. A combination of factors, including economic interests, military presence, and historic involvement work to integrate the United States into a security environment that is otherwise in the first instance defined by geographic considerations. Actors, except at the most global level where the world political system is itself the security environment of interest, find that they are embedded in some security environments, but not others. Additionally, actors can choose to enter (depart) some security environments, but are necessarily included (excluded) from others.

Where / when an actor's security environment is comprised of states as the principal actors, neorealism, and other theories, offer useful insights. It has attained the status of the dominant, mainstream theory of international politics for good reason. However, a neorealist perspective overlaid onto a completely different security environment is inappropriate and dangerously misleading. National security policy makers must operate from theoretical perspectives that are relevant to their security environment(s). This demands the ability to employ different theoretical *perspectives, or frameworks,* for differently constituted security environments. For major actors in the international system, like the United States, this spans a diverse universe from nuclear deterrence to counter-terrorism.

A security dilemma between two actors is contingent on the participation of both actors in the same security environment. A hypothetical security environment defined by interests strictly and exclusively associated with geography, and with participation based solely on this factor will exclude extra-regional actors. By definition, there is no security dilemma between the actors in this scenario, if there is no common geographic interest. Within this specific security environment a security dilemma cannot arise between an actor participating in the security environment, and an extra-regional actor. There is no tractable, or conductive, medium within which conflict can occur between the two actors in this strictly geographically based security environment. As an example, in empirical analysis of the Correlates of War project, proximity was identified as a contributing factor in explaining the (non)occurrence of war between two actors.[27] Obviously, wars have occurred between actors that did

[27] J. D. Singer and M. Small, *The Wages of War, 1816 – 1965: A Statistical Handbook* (New York: Wiley, 1972).

not share contiguous boundaries or other interest tied to geography, but this suggests that other interests influenced the participation of both actors in a common security environment, thus providing the tractable medium for conflict.

Where there is no shared environment defined by interests, thus conductive, tractable medium within which conflict can occur, there cannot arise a security dilemma between actors. If there is no security dilemma between actors, then conflict is improbable. Stated differently, a shared Environment is a necessary condition for a security dilemma, which, in turn, is a necessary condition for conflict. At the extreme, two actors both oblivious of the Other's existence are not aware of an Environment shared with that Other, hence there can arise no consciously known security dilemma between the two actors, and thus conflict between them is unlikely unless one becomes cognizant of the Other.

It is possible for a shared Environment to exist, and a security dilemma to arise, in which only one actor is aware of the existence of an Other. Mutual recognition of hostility towards each other is not a necessary condition for conflict to occur; a surprise attack is possible where the attacked actor did not perceive a threat. However, awareness of an Other by one actor, while necessary for the development of a security dilemma, is not sufficient. The Other must also be perceived as a threat or a target. The awareness of an Other by at least one actor is a necessary condition for a security dilemma, but the perception of threat or interest is what results in a security dilemma.

At the most macro-level, the world political system, all actors are within a shared environment. Viewed globally, Costa Rica and Switzerland both participate in a shared security environment. Practically, however, security environments of lesser comprehensiveness offer better chances of perhaps understanding why conflicts occur. Both Costa Rica and Switzerland participate in a shared security environment when viewed from a global perspective, but war is unlikely between these two actors. Analysis of "not-war" (in formal logic symbolized by "~ war," or peace) events is important to understanding the totality of war as a phenomenon, but a more fruitful examination of the non-occurrence of conflict can perhaps be conducted at less grand a level. It is perhaps intuitively obvious to some that war was improbable between Costa Rica and Switzerland in the past, but research into this fact is likely to arrive at the "so what" revelation that they didn't have any real or perceived reason to fight, in other words, there was no security environment they shared other than the world political system. We must look to the characteristics of Self, Other, and Environment that constitute a shared security environment to understand the potential causes of threat perception and interests that lead to security dilemmas, and ultimately conflict.

Environment – Gray:

The security environment approach accounts for the interdependent nature of the system and the actors within it. The environment is the "Gray" of the Red, Gray, and Blue framework of the security environment approach. At the level of paradigm citing Gray as an influence or framework component is adequate for description and explanation. At the finer resolutions required for modeling, however, Gray must be analyzed to explicate its endogenous structure and composition. This is a *sine qua non* for building both generic and case-specific models of the environment to determine Gray's influence on conflict. At the level of case-specific analysis, Gray may be modeled as an extremely detailed sub-system schematic of a specific complex system, with highly quantifiable factors and processes outlined and simulated using computers. This section details the composition of Gray at a higher level of abstraction than a case-specific model's sub-system built by analysts for use in a particular situational context. By going beyond citing the environment – Gray – as a factor at simply the most macro, abstract level, however, and delineating common components and attributes of Gray in generic case models, the study suggests how to tailor a case-specific analysis aimed at a higher resolution of detail. Context specific cases can build on this generic model to achieve greater modeling detail and finer resolution to support their particular needs.

The Environment is Neutral:

An understanding of one's environment is essential in conflict. To the extent that one operates under a false impression of one's environment, at both the levels of philosophy and routine activity, one increases the risk involved in conducting operations within that environment. At the extreme, failure to comprehend the true nature of the environment results in crafting inappropriate policy, which in turn results in failed implementation of policy during actual operations. In designing security policy, the environment, if considered explicitly at all, is sometimes regarded as a hostile entity to be overcome in addition to the threat. A failure to consider environment, or consideration of the environment as hostile, or for that matter friendly, are all flawed frameworks upon which to craft national security policy.

The fact is the environment is neutral. This neutrality of the environment is relative to both the Self and the Other – both Blue and, in this case, Red. The environment is neither "Blue" or "Red," but "Gray," and its attributes and characteristics simply exist for both Blue and Red. The environment can serve as either a condition variable or an antecedent condition, or it may not. This depends, however, not on the environment's traits, which simply "are," but rather the activity that occurs within

the environment. Actors that correctly judge the characteristics of the environment and adapt their activities to it may prevail in their efforts or achieve advantages, allowing for the ever-present role of chaos, chance, and complexity. Actors that do not adapt to the environment will almost certainly fail.

The environment is animate, yet unthinking. Influencing the environment are the traits of the actors themselves, which shape the shallow structure of the environment, which in turn works through a feedback mechanism in shaping the actors. The process is interactive, simultaneous, and involves considerations of chaos, chance, and complexity. This study argues that ignoring the environment in crafting national security policy is an ultimately bankrupt approach. The security environment approach – Red, Gray, and Blue – is a sophisticated, comprehensive, and realistic approach to formulating national security policy. The Red, Gray, and Blue framework does not present the environment as a single entity with fixed attributes that means the same thing to all actors at all times. The environment within which an actor operates is influenced by the actor's traits and choices, and whether this works to the actor's advantage or disadvantage is dependent on that actor's traits, decisions, and actions. At the deep level of environmental structure all actors are affected by common environmental attributes, for example, in the physical world by factors like gravity, temperature, etc. In the shallow structure of the environment, however, the composition of the environment is partially constituted by the actor's choices of, among others, with whom to interact, how to interact, when to interact, and other decisions and factors that shape the environment. For example, at the micro-level of analysis one's circle of friends constitutes an important portion of one's environment. Should one choose to associate with felons, there are real consequences for the shape of the micro-environment that will surround one. The dynamic applies to systemic-level actors as well. This is not a trivial point. Wendt points out in discussion of the agent – structure problem that both agent and structure are mutually constitutive, and also simultaneously points out the inadequacies of past frameworks as approaches to crafting security policy:

> While neorealism and world-system theory both claim to be "structural" theories of international relations, they embody very different understandings of system structure and structural explanation. Neorealists conceptualize system structures in individualist terms as constraining the choices of preexisting state agents, whereas world—system theorists conceptualize system structures in structuralist terms as generating state agents themselves. These differences stem from what are, in some respects, fundamentally opposed solutions to the "agent-structure" or "micro-macro" problem. This opposition, however, itself reflects a deeper failure of each theory to recognize the mutually constitutive nature of human agents and system structures-a failure which leads to deep-seated inadequacies in their respective explanations of state [actor] action.[28]

[28] Wendt, "The Agent-Structure Problem in International Relations Theory," p. 335.

Gray consists of both deep structure and shallow structure traits, both influenced by and influencing the actors within it. And it is neutral; it does not inherently favor or disadvantage either Blue or Red, *a priori*. It affects different actors *impartially*, because it is unthinking. But it does not affect different actors *equally*, because different actors themselves possess traits that render Gray either a comfortable or uncomfortable environment. Because Gray exists across all dimensions, it cannot be escaped; the conduct of conflict in any dimension cannot be reduced to a simple dyad of Red against Blue. The simplest possible conflict between actors is a single Red against a single Blue *against a background of Gray*, or the first variant of the game of *Stalker*. Thus, in any conflict the environment itself is a factor *that favors or disadvantages an actor based on that actor's own characteristics.*

An anecdote illustrates the point. Sir Frederick Spencer Chapman was a British officer during World War II. He served as a commando behind Japanese lines in Malaya. He relates that the greatest challenge for those fighting in a jungle environment was predominately a mental, and not a physical, challenge. His experience was

> ...that the length of life of the British private soldier accidentally left behind in the Malayan jungle was only a few months, while the average [non-commissioned officer], being more intelligent, might last a year or even longer. To them the jungle seemed predominately hostile, being full of [dangers]...They were unable to adapt themselves...they expected to be dead within a few weeks – and as a rule they were...The truth is that the jungle is neutral. It provides any amount of fresh water, and unlimited cover for friend as well as foe – an armed neutrality, if you like, but neutrality nevertheless. It is the attitude of mind that determines whether you go under or survive. 'There is nothing either good or bad, but thinking makes it so.' The jungle itself is neutral.[29]

Whether actors involved in a specific conflict are operating within a jungle or cyberspace, the environment is neutral. Failure to include environment in the decision calculus of crafting security policy is an error, as equally is considering the environment either friendly or hostile. The environment, Gray, is animate, dynamic, and powerful. Yet it is unthinking, and the effects and influence of the environment are dictated by the traits, policies, and actions of the actors themselves. As Gray influences both Red and Blue, as well as is influenced by Red and Blue, failure to monitor the environment will lead to a failure to understand the situational context of a conflict and adequately adapt to changes. This, in turn, potentially hampers and may perhaps defeat attempts to implement policy founded on such a flawed foundation.

The Environment is Anarchic and *Disorderly*:

Hedley Bull in his classic *The Anarchical Society* argued that the international system was anarchic, but for the most part orderly. Although there exists no overarching authority that commands the world political system, it is not a chaotic anarchy, but rather an orderly anarchy. This is fundamentally so, according to Bull, because all societies seek to ensure life against violent death, ensure agreements are kept, and that property rights remain stable.[30] These three goals, following Bull, constitute the elementary and primary goals common to all social life, and as such constitute norms for interaction between societies, even under anarchy. The specific society Bull treats is a society of states, although he concedes the existence of other actors. This society of states he defines as existing "when a group of states, conscious of certain common interests and common values, form a society in the sense they conceive themselves to be bound by a common set of rules in their relations with one another, and share in the working of common institutions."[31] Within this society of states exist four shared goals: 1) preservation of the society of states, 2) maintenance of independence of states, 3) peace, and, 4) the three elementary goals cited above common to all societies.

Bull points out that within the international system all three of the political traditions co-exist simultaneously, namely the Hobbesian, Kantian, and Grotian traditions.[32] However, for Bull's anarchical society, he finds that Realists overstate the Hobbesian nature of the system because of over reliance on the "domestic analogy." The domestic analogy is the argument that states, like individuals within a state, are incapable of being ruled without a central government. Bull finds that the Hobbesian view of the system fails to understand that the domestic analogy is flawed, and "the fact that states form a society without government reflects features of their situation that are unique."[33] Thus, Bull asserts Realists inappropriately draw conclusions concerning the interaction of Second Image actors from First Image observations.

Another reason Bull asserts that Realists overstate the danger in the international system is that "states are not vulnerable to violent attack to the same degree that individuals are." This second reason is caveated by the observation "it is only in the context of nuclear weapons and other recent military technology" that war can approximate, in Clausewitzian terms, "the form of a single,

---

[29] Frederick Spencer Chapman, *The Jungle is Neutral* (New York: W.W. Norton & Company, 1949), pp. 125-126.
[30] Hedley Bull, *The Anarchical Society* (New York: Columbia University Press, 1977), pp. 4-5.
[31] Bull, *The Anarchical Society*, p. 15.
[32] Alexander Wendt has refurbished this categorization as the Hobbesian, Lockean, and Kantian cultures of anarchy. See Wendt, *Social Theory of International Politics*, pp. 246-308.
[33] Bull, *The Anarchical Society*, pp. 46-51, quote p. 51.

instantaneous blow."[34] So, summarizing Bull, the Realist argument that the international system is Hobbesian fails on three points: the systemic actors are states and not individuals, states are not vulnerable like individuals, and a systemic-level of violence does not consist of a single blow. This study, however, refutes Bull's argument and asserts it is no longer relevant given the current security environment. What has changed is that individuals armed with WME technology, knowledge, and means can, in fact, affect system relevant influence, can injure states through targeting population and critical infrastructures, and can do so in a single blow.

The Environment is Dynamic:

Implicit in the meaning of structure is continuity of form even if only for an instant in time. An actor must ascertain the form of the structure before it can intelligently manipulate the environment or develop courses of action within its context. To the extent that the environmental structure remains constant, actors can increase their knowledge of its form and the inherent implications of that form, and thus improve their crafting and implementation of security policies. The total absence of form connotes an inchoate environment that is not readily manipulated with foreseeable results, or even understandable. Likewise, the complete absence of change in form dictates an environmental condition of stasis, with the potential for the eventual development of optimal policy courses of action within its specific spatial and temporal context. In reality the environment, however, undergoes change between these two extremes of total inchoateness and perfect stasis.

The environment, although dynamic, is still susceptible to analysis and understanding by an actor. This presents opportunity to those actors successful in accurately modeling the environment, because they better understand it which makes possible the creation of a competitive edge through a knowledge advantage. The extent of a specific environment's dynamism is a function of that environment's endogenous traits. Generically, perfect inchoateness and stasis are not seen outside of the realm of theory. The extent to which a particular environment changes, however, is at a case-specific level of analysis, and may vary across time and other dimensions.

Writing in 1986 Gaddis analyzed the international security environment concluding that there existed structural and behavioral elements of stability within it. The structural elements of stability included bipolarity and independence of ties between the United States and the Soviet Union, while the behavioral elements of stability included nuclear weapons as deterrents, operational transparency due

[34] Bull, pp. 46-51.

to the reconnaissance capabilities of satellites, and ideological moderation over time.[35] Gaddis' elements of stability, like the Cold War security environment, proceeded from a state-centric paradigm. The elements of stability in the Long Peace were eventually countered three years later by elements of change within the same environment. The elements of continuity, or stability, within the environment were well understood; the fact that the end of the Cold War came as a surprise to all suggests that the elements of change within that security environment, as well as the true nature of the security environment itself, were not understood.

A dynamic security environment will include both elements of stability and change as it is neither perfectly inchoate nor static. As Baumgartner and Jones' PE theory, detailed in chapter two, explains there exist both "positive feedback" and "negative feedback" forces that simultaneously act to provide both continuity of stability and call for change. Gaddis correctly identified the elements of stability, but failed, as did everyone, to adequately understand and address the elements of change within the environment.

The development of a model of a specific environment must account for factors of both stability and change. Preoccupation with either positive or negative feedback forces, or elements of change or stability, is a biased analytical methodology. The static international system of Neorealism as well as the intractable vagueness of radical post-modernism must be avoided as well. What is required is an approach that accounts for dynamic change of an environment between the extremes of perfect inchoateness and stasis, and a structure that exists between a rigid, functionally undifferentiated system and a completely ambiguous system. At the generic level of modeling, the security environment approach meets these two criteria. Expanding on this base model's requirements to account for dynamic change within a comprehensible system, a case-specific environment can be created.

Interdependency of the Environment:

As used in this study, the term interdependence "refers to situations characterized by reciprocal effects among" actors.[36] Although Keohane and Nye use this term primarily in the

[35] John Lewis Gaddis, "The Long Peace: Elements of Stability in the Postwar International System," *International Security*, Vol. 10, No. 4 (Spring, 1986), pp. 99-142.
[36] Robert O. Keohane and Joseph S. Nye, Jr., *Power and Interdependence: World Politics in Transition* (Boston: Little, Brown, 1977).

economic sense, Gilpin points out that interdependence can also refer to a power relationship.[37] Gilpin continues in subsequent work to point out that economic relations, although very important, are less important than political relations.[38] Wendt extends this concept of interdependence from the economic to the purely political concept of interdependence of actors in constituting their identities, and thus returns to Hegel's earlier concept of the role identities of lordship and bondage (*Herrschaft und Knechtschaft*) in chapter 4 of his *The Phenomenology of Spirit*, mentioned above. Wendt states:

> Shared ideas can be conflictual or cooperative, which means that 'enemy' can be as much a role identity as 'friend.' Finally, as the enemy example indicates, what really matters in defining roles is not institutionalization but the degree of interdependence or 'intimacy' between Self and Other. When intimacy is high, as in the Arab – Israeli conflict, role identities might not be just a matter of choice that can be easily discarded, but positions forced on actors by the representations of significant Others. In this situation even if a state [actor] wants to abandon a role it may be unable to do so because the Other resists out of a desire to maintain *its* identity.[39]

This study adopts Wendt's view of interdependence. Without actors within a system, there can be no actors known as Self and Other. The two actors are mutually constitutive, and interdependent in partially constituting each other's role and identity, as Hegel's master and slave were interdependent in their roles and identities.

Demonstrating generically above that actors are mutually interdependent concerning roles and identities, it follows that a case-specific modeling effort would identify those Others that are constituted by Self. In a famous reply, when asked why he robbed banks, Willie Sutton replied "because that's where they keep the money." The activity of storing money partially constitutes the very identity and role of a bank, which, in turn, partially constitutes automatically the identities of hostile Others with interests antithetical to those inherent in the role of Self. A bank, by its very existence, constitutes its stereotypical enemies, bank robbers. Were it not a bank, but another type of Self, then bank robbers would not be constituted as its natural enemy.

Likewise, the environment is interdependent for its identity with those actors that are active within it. Revisiting the example of a security environment constituted by those actors concerned with oil supply, the security issue of control of oil defines the security environment of those actors in the dimensions of geography, commodity, means, intelligence requirements, interests, business models,

---

[37] Robert Gilpin, *The Political Economy of International Relations* (Princeton, NJ: Princeton University Press, 1987), pp. 17-18.
[38] Robert Gilpin, *The Challenge of Global Capitalism* (Princeton: Princeton University Press, 2000), pp. 193-194.
[39] Wendt, *Social Theory of International Politics*, p. 228. Original italics.

and other factors. If the principal interest of the actors involved in that environment, however, changed from control of oil to a radically new security issue, for example, reversing the invasion of one actor by another, the very nature of the environment would change because of the change in the actors' collective interests. This is essentially what happened when Iraq invaded Kuwait in 1991. A common interest in pan-Arabism, regional stability supporting oil production and distribution, religious homogeneity, and reticence to allow large-scale stationing of "Western," i.e. US, forces in theater changed almost overnight, with a corresponding radical change in the make-up of the Middle East regional security environment.

The three constitutive elements of the security environment – Self, Other, and Environment – are mutually constitutive and politically interdependent with each other. This collective interdependence defines roles, identities, and interests. This interdependence may possess economic or other components, but it is principally a political and social relationship.

Known Aspects of the Environment:

The composition of the environment in which an actor is embedded has ramifications for the successful conduct of operations by that actor. These activities may be the prosecution of conflict, or may be simply the implementation of passive security policies. Without assessing the environment's characteristics, however, actors will effectively be operating without understanding the environment.

This assessment of environment is necessarily multidisciplinary, and includes quantification techniques, qualitative analysis, the development of refined typologies, and the exercise of judgement informed by intuition by senior decisionmakers. If possible, it is modeled so the actor's activities can be simulated before actual execution in reality to gain insights and determine probabilities of success. The assessment of the environment is continuous and feeds back into analysis. Modeling the environment as a static, given backdrop against which activity is conducted is to lose the fine-grained resolution of the interdependent nature of the environment's influence on an actor's activities. For example, a model of the physical world would include transition from a daylight scenario to a night scenario. Failure to capture the environment's actual dynamics as closely as possible limits the utility of analysis of modeled activity. A model of conflict conducted in simulated daylight conditions on a computer will have little validity for that same model of conflict under the conditions of night, provided that the activity is influenced by the factor of available ambient light.

The perfect model, of course, would perfectly duplicate the effects and dynamics of the environment. However, as perfection is just as obviously unattainable, the analyst must decide on which dynamic elements of the environment have a significant impact on the planned, modeled activity. These factors must be captured to as high a resolution of fidelity as possible to improve the model. Other factors that may have little importance for answering the questions at hand are not critical to model, provided the analyst is correct in assessing such factors as insignificant.

The environmental model need not be physically complex. Dependent on the system analyzed, the physical environment may be a climate-controlled computer space with limited factors relevant to the planned analysis; the important component of this environment may be described as a limited expanse of cyberspace containing a single operating system. Simulating the physical conditions of an indoor piece of equipment may only incorporate temperature, humidity, and other basic conditions, easily replicable by a laboratory's equipment and monitors to assess risk. However, modeling the network of cyberspace within the system may involve significant allocation of computer forensic analysis resources.

Unknown Aspects of the Environment:

Few if any policymakers, if asked directly, would declare they completely understand everything there is to know about their environment. Yet, frequently in the decisionmaking and policy crafting process what is not known is not considered. The requirement is not that what is not known somehow become known, but rather that the decisionmaker *critically* views the process, remaining conscious of the fact that it does not account for all existing factors, but only *known* factors. Whether what is known and considered in the process is functionally adequate to meet the actual challenge faced is dependent on the situation. When it is not functionally adequate, however, it is what is unknown that has contributed to failure. With a policy's success or failure being influenced by unknown aspects of the environment, one would expect that what is unknown would receive attention during the decision process. To only consider what is known is to only look, by definition, at a partial set of factors that can contribute to success or failure. It is roughly analogous to the familiar example of a drunk looking under a street light for his keys, because that is where the light shines and where he can see what he is doing.

A counter-argument can be made that attempting to consider unknown factors' bearing on the success or failure of a policy is an impossibly difficult task. How can one assess what is unknown? If one was to proceed in a strictly inductive fashion, this would be a fair argument. Any number of

things, perhaps even an infinite number of hypothetical variables, could conceivably be imagined as existing unknown beyond the circle of the metaphoric street light. But an analyst should not then fabricate tortured scenarios from wild imagination in a frantic effort to account for the unknown in the policy process. Haphazardly operationalizing and assessing variables is a theoretical cul-de-sac, exceptionally intensive in resources, and not a sound systematic approach.

Proceeding deductively offers a more efficient and economical approach. One can examine Self critically and deduce those factors, that if existed in the environment or if a threat brought to bear, would injure Self or defeat Self's security policy. Self knows, or should know, its weaknesses even if it does not know all the aspects of the environment. Knowing its desired endstate, its capabilities and intent, the proposed structure of its policy or course of action, and those knowable aspects of environment and existing threats that do exist, Self can craft policy or operations that counter the unknown.

A comprehensive assessment of Self informs knowledge of what can harm Self. This understanding, even if only at a general level, of those threat actions and means or environmental effects enable counters to be crafted that prevent, preempt, and mitigate potential incidents. For those specifically known factors, specific counters can be established. However, what Self does not know can also hurt it. Denied the opportunity to craft specific counters, Self must, nevertheless, still craft counters. This is possible, even when dealing with unknown factors, by conforming to security policy design criteria tailored to mitigate unknown aspects of the environment. These criteria enhance security policy survivability against unknown factors, and additionally allow the rapid crafting and implementation of more specific counters from an established base when additional knowledge of specific threats becomes known. Key criteria that security policy must adhere to in order to counter unknown factors include:

- Robustness – The robustness of a policy or operation refers to its power in overcoming negative effects and obstacles. A national security policy of launching a strategic nuclear attack against a threat invasion force would be more robust than a security policy of defending with conventional forces. One measure of robustness would be a gross imbalance of assets employed by the security policy against the threat. Overwhelming force is a technique for increasing the robustness of a policy.
- Redundancy – A security policy that is well crafted will not rely on a single-point-of-failure system. Multiple systems increase the probability that at least one of the systems employed will be successful. Reliance upon a single system, especially when that system is complex, may find

that it fails, and thus the security policy fails. The employment of a "back-up" system increases probability of success.

- Resilience – A resilient means is not inflexible, brittle, or dependent on the existence of narrow environmental constraints for successful employment. In mechanical systems, resiliency can be a function of loose tolerances that allow for successful operation in differing climatic conditions. In cybersystems, a resilient system is one that can isolate a modular component's failure and continue to operate.
- Recuperability – A recuperable policy or system is one that has the inherent capability to "self-heal." A security policy that contains codified mechanisms to allow for continued operations or employment even during internal disruption is recuperable. An example is a security policy involving two actors, with "built-in" mechanisms to resolve internal disagreement even during operations or employment. The pre-defined mechanism, perhaps in this example a senior advisor's committee meeting, can address such internal disruption without placing the on-going operation at jeopardy. Without recuperability of a system or policy, any disruption regardless of cause could stymie operations.
- Reparability – The criterion of reparability enables a means to suffer damage, but still be effective following repair. A system that is not rapidly repairable, or repairable with available means, does not meet this criterion. This criterion is not limited to just mechanical or other systems. Whereas the criterion of recuperability addressed the "healing" of relations between actors, the criterion of reparability addresses the capability of replacing actors in a security arrangement with functionally adequate substitute partners.
- Distribution – The criterion of distribution recognizes that increased centralization of processes increases vulnerability to a *coup de main* attack. Distributed operations have multiple, functionally adequate nodes of control dispersed in space, time, and cyberspace. This complicates threat targeting, and ameliorates any localized environmental disturbance.
- Diversity - Another criterion that increases a policy's or course of action's ability to withstand unknown aspects of the environment is diversity of means. One technique where diversity of means is employed is the intelligent targeting of critical nodes using different weapon systems. Should an unknown aspect of the environment defeat one weapon system, a different weapon system may be unaffected by that unknown factor. Diversity of means lessens vulnerability to unknown aspects of the environment.

An example of such a security policy approach countering uncertainty is the Internet. Although great effort was made to model and simulate the effects of a nuclear war between the Soviet Union and the United States, there remained significant unknown factors and effects resulting from

strategic nuclear conflict. Recognizing this, the US national security community designed and built the forerunner to the Internet. Because of its highly distributed nature and other inherent traits, the Internet meets the generic criteria above for increasing the probability of success of a security policy or system even when unknown factors come into play. The Internet is, of course, evolving. However, the productive longevity of the design in a future environment and role that could not have been imagined when it was employed evidences the utility of the above criteria in crafting security policy and courses of action given unknown aspects (past, present, and future) within the environment.

The environment cannot be perfectly known. Ignoring unknown aspects of the environment is not a responsible action when crafting national security policy. Policymakers and strategists should consider the above criteria in designing policy and security systems. The Internet is a good example of how intelligent design can counter unknown aspects of the environment decades into the future.

Unknowable Aspects of the Environment – Complexity, Chaos, and Chance:

Discussion of the known and unknown aspects of the environment leads logically to consideration of those aspects of the environment that are unknowable, thus exhausting the range of possible environmental aspect categories. As discussed above, analysis proceeds in sophistication from consideration of what is known, advancing through consideration of what is unknown, and terminating in the highest level of sophistication of analysis: consideration of what is unknowable. The value added by each of the steps is dependent on the situation. However, in any situation of even moderate complexity all three categories exist. Only the simplest environment could, arguably, have a universe consisting wholly of known aspects, and this only likely in a theoretical world.

Examination of the unknowable aspects of the environment leads to reflection on the fundamental nature of conflict. What is it in an environment of conflict that is unknowable? The Prussian general Clausewitz, in his classic rumination on the essence of war, conceived of two trinities; the first trinity at the theoretical and abstract nature of war's essence, and the second trinity more concretely anchored in his era:

> War is more than a true chameleon that slightly adapts its characteristics to the given case. As a total phenomenon its dominant tendencies always make war a paradoxical trinity - composed of primordial violence, hatred, and enmity, which are to be regarded as a blind natural force; of the play of chance and probability within which the creative spirit is free to roam; and of its element of subordination, as an instrument of policy, which makes it subject to reason alone. The first of these three aspects mainly concerns the people; the second the commander and his army; the third the government. The passions that are to be kindled in war must already be

> inherent in the people; the scope which the play of courage and talent will enjoy in the realm of probability and chance depends on the particular character of the commander and the army; but the political aims are the business of government alone. These three tendencies are like three different codes of law, deep-rooted in their subject and yet variable in their relationship to one another. A theory that ignores any one of them or seeks to fix an arbitrary relationship between them would conflict with reality to such an extent that for this reason alone it would be totally useless.[40]

We will leave aside Clausewitz's second trinity comprised of the people, the commander and his army, and the government. This study is anchored in a different period, and although Clausewitz's formulation of the concrete nature of the trinity of war still applies to state on state conflict in even this more modern era, that topic is not the focus of this study's efforts. The theoretical construction of his more abstract trinity, however, is directly relevant to this study.

The component of "primordial violence, hatred, and enmity" corresponds to the socially constructed relationship existing between the involved actors. The second component of "the play of chance and probability" corresponds to unknowable aspects of the environment. The third component of war's "element of subordination, as an instrument of policy, which makes it subject to reason alone" aligns with this study's later examination in chapter four of threat typologies and decision trees in the seven variants of the game of Stalker. This section deals with the unknowable aspects of the environment, and as such addresses Clausewitz's second component of his trinity, namely chance, complexity, and chaos.

The unknowable aspects of the environment are similar to the unknown aspects of the environment discussed above. The chief difference is that whereas unknown aspects may eventually transition to the known aspects category as a scenario progresses, unknowable aspects remain incomprehensible in their causal chains and effects. However, planning can also take into account the effects of the unknowable aspects to some extent. As with the unknown aspects, this does not mean that specific counters are crafted, because specific factors to counter are obviously, again, not known. Rather it is the prudent recognition that there exist measures that will ameliorate certain future effects, regardless of their cause or origin, and that the causal chain of events and probability of occurrence that led to the effects is an operationally moot topic if the effects do, in fact, occur. Should an unknowable aspect of the environment exercise an effect, the *ex post facto* analysis of the effect's causal chain and situational dependent probability of occurrence is essentially a topic of historical interest, and not an immediate operational concern. Upon occurrence the effect *is*, and the immediate

---

[40] Carl von Clausewitz, *On War*, Michael Howard and Peter Paret, eds. (Princeton, New Jersey: Princeton University Press, 1976), p. 89.

operational concern will be to counter it. To this end, intelligent foresight and design can serve to mitigate the effects of unknowable aspects of the environment.

Complex systems have an inherently greater potential of unknowable aspects exerting effects. Perrow points out "as systems grow in size and in the number of diverse functions they serve, and are built to function in ever more hostile environments, increasing their ties to other systems, they experience more and more incomprehensible or unexpected interactions. They become more vulnerable to unavoidable system accidents."[41] This dynamic entails two points important for policymakers and strategists to understand. First, the more complex the system, the more unknowable aspects exist within that system. Second, the more complex the system the greater the number of potential breakpoints. Thus, both the unknowable aspects and the potential points of failure increase. These two factors combine to make the likelihood of unknowable aspects affecting a policy or system exponentially greater.[42] The actual curve this follows, of course, depends on the system or environment in question. However, at the generic level of modeling, it is instructive and important for policymakers to consider in designing or modeling a specific system. Simplicity may be commonly recognized as a "certifiable good thing," yet unless policymakers and strategists keep the fact of the exponential increase in probability of failure as complexity increases before them in their analysis, they may not realize how fragile a particular security environment may actually be. Before the occurrence of negative effects, even a complex, fragile system appears to be stable. After the occurrence of an unknowable aspect's negative effects, a complex system may be beyond stopping in the resulting destructive chain of events. The time for policymakers to exercise thoughtful analysis of the environment and intelligent design of policy is before the catastrophe.

Countering the effects of unknowable aspects of the environment begins with a quasi reverse engineering methodology, where the desired endstate of a policy is known. A thorough assessment of Self then provides the start point, and between these two known conditions a critical path can be identified that the proposed policy must accomplish to achieve the endstate. This critical path must be

---

[41] Charles Perrow, *Normal Acccidents: Living with High-Risk Technologies* (New York: Basic Books, 1984) p. 72.

[42] Perrow notes: "I suggest that only 1 percent of all possible parts or units in a linear system are capable of producing 'complex' interactions, while about 10 percent of those in a complex system will be capable of doing so. But that 10 percent represents more than a tenfold increase in the potential for system accidents. The potential interactions produced by, say, four parts or units that are interrelated in a complex, rather than linear way, is twelve. (There are twelve possible paths between the four parts.) Suppose this exists in a system where there are 400 parts or units. If 10 percent of the units had such characteristics, rather than an order of 1 percent, there would be forty such parts or units. The potential complex interactions of each one of these with the remaining 399 would be in the millions, since the possible paths increase exponentially." Ibid, pp. 75-76.

safeguarded from interdiction, and its composition and traits partially determine the environmental conditions and threats that could injure Self. From analysis of the critical path, a general universe of environment aspects can be deduced that could break or damage the successful implementation of policy. Measures then can be instituted that forestall the critical path from interdiction by such environmental aspects. Although a specific environmental aspect capable of interrupting the critical path, hence achievement of the desired endstate, is not identified and remains unknowable, measures that preempt the unknowable aspects' negative effects capable of interdicting the critical path are incorporated into the policy and the probability of success is increased.

A Macro Portrayal of Information Infrastructures:

Communications are sources of intelligence, aid in command and control of systems, and facilitate security policy planning and implementation. Political actors depend on communication infrastructures; the quality, reliability, speed, bandwidth and other details of an information infrastructure have national security ramifications. This is especially true with a technologically advanced actor dependent on computer networks.

An information infrastructure is simultaneously a target and a targeting means, as well as the means to defend other infrastructures while itself constituting an infrastructure. Understanding security policy and the conduct of conflict in the new security environment dictates first understanding the framework's information infrastructures.

The Red, Gray, and Blue model presents five information infrastructures. These are the Global Information Infrastructure (GII), the Threat Information Infrastructure (TII), the National Information Infrastructure (NII), the Force Information Infrastructure (FII), and the Minimum Essential Information Infrastructure (MEII).[43]

Targeting an information infrastructure successfully has potentially significant effects on a dependent infrastructure's operations. For example, electric utilities, public water utilities, telecommunication networks, pipeline systems, and other infrastructures use an information infrastructure of backbone operation systems termed Supervisory Control and Data Acquisition

[43] The terms GII and NII are concepts in the Joint publication 3-13, cited below as the source of these term's definitions. The term TII is this study's concept. The term MEII was coined by Richard Mesic during planning for a series of information warfare exercises conducted under RAND direction from 1995 to the present. See Robert H. Anderson, Phillip M. Feldman, Scott Gerwehr, et al, *Securing the*

(SCADA). This information infrastructure controls the operations of other infrastructures. As such, it represents a high-payoff target. Disruption of this information infrastructure renders the dependent infrastructure, for example the electrical distribution system for a city, inoperable. The effects of attack do not have to take place in distributed physical space, but can occur in cyberspace in a very short period of time. This makes attacking a SCADA network, if possible, a very effective and very cost-effective targeting preference for asymmetric actors interested in striking critical infrastructure systems.[44]

Delineating different information infrastructures has utility for understanding Self, Other, and environment. Using terms precisely, in accordance with explicit definitions, aids in clarity. To this end the above terms are employed as follows:

GII: "The worldwide interconnection of communications networks, computers, databases, and consumer electronic devices that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly [, neutral,] and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure."[45]

The global information infrastructure, by definition, is the most encompassing. It includes within it Self's information infrastructures, as well as the information infrastructures of all Others. The environment's aspects, for example level of interference of communication transmissions resulting from solar flares, affects both Self and Other(s). This GII is, like the environment which it partially constitutes, in dynamic flux. There is a continual current of change in the GII, dependent on factors as diverse as physical conditions, like solar flares, to the introduction and deployment of new technologies. The GII is dynamic, and this means that dominance of the GII is a case-dependent proposition.

NII: "The nation-wide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The

---

U.S. Defense Information Infrastructure: A Proposed Approach (Santa Monica, CA: RAND, 1999), p. iii.

[44] *Understanding SCADA System Security Vulnerabilities*, Riptech, Inc. White Paper (Alexandria, VA: January 2001), pp. 2-4.

national information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly [, neutral,] and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the national information infrastructure."[46]

The NII, like the GII, is dynamic. In a culturally isolated political actor, for example the state of North Korea under its current political status, the NII may be ossified and relatively static. However, exogenous environmental factors affect some change even on these information infrastructures. Such an actor may be vulnerable to having its NII mapped to a relatively fine degree of resolution, thus increasing vulnerability. Paradoxically, a technologically advanced and open political actor, however, may be relatively difficult to map, because of its inherent dynamism achieved through the introduction of new technologies, and the decentralized nature of its operation. This potentially makes targeting the information infrastructure more difficult, but may increase vulnerability to attack if it is successfully mapped.

TII: The TII is similarly defined as the GII and the NII, with the exception, of course, that it is threat-wide. The composition of the threat's information infrastructure is dependent on a specific case. As a conceptual tool, the TII is the threat's means of exercising command and control of systems, planning and implementing security policy, and is a rich source of intelligence regarding the threat's systems and policies.

Similar to the NII, the TII also exists on a continuum of traits. Understanding the essential nature of the TII suggests threat vulnerabilities, hence targets. It also provides insight into a threat's capabilities. A political actor with a relatively low degree of advanced technology capabilities will possess different capabilities and vulnerabilities than a highly advanced technological actor.

FII: The FII is, likewise, similarly defined as the above information infrastructures. It is the information infrastructure that supports a friendly force engaged in conflict with the threat. This may be an information warfare team's internal communication networks, or in conventional, tactical

---

[45] *Joint Doctrine for Information Operations*, Joint Pub 3-13 (Washington, D.C.: Chairman of the Joint Chiefs of Staff, 9 October 1998), p. GL-6, bracketed inclusion of "neutral" is author's.
[46] Ibid, p. GL-9.

combat the radio nets of a line unit. The FII is dependent on the force's identity, needs, and ends. Tactical radios are indispensable for some types of forces, but not required by other types, for example.

MEII: The MEII is a concept developed by RAND analysts. They describe the MEII as a process, and not a hardened, isolated communications architecture. This study adopts the RAND position that the MEII is not an infrastructure subset secured against all conceivable attacks. Instead, what is "essential" depends on a case-by-case analysis, and also depends on identity of actor, means, methods, and ends. As the RAND analysts point out the concept begs the question of "essential for what?"[47] Because the nature of technology, hence the nature of information infrastructures, is continually and rapidly evolving, there can be no purely physical understanding of securing a MEII from attack. Certainly physical hardening, firewalling, encryption, and other techniques will be employed to protect the identified MEII. However, the MEII is not a static entity. Additionally, there exist any number of MEIIs within the NII at any given moment, based on the constitutive sub-actors within Blue that have identified their particular MEII. An example of one such MEII is the National Communications System's provisions for the continuity of specific governmental functions in an emergency. The MEII for this system twenty years ago looked quite different than today. Conceptually, at the paradigmatic level the concept of MEII is useful, however, as analysis transitions to a finer resolution of modeling a specific case, it is necessary to conduct analysis of what constitutes the MEII for that particular case.[48]

The above definitions emphasize technology, but do not exclude other means of communication. Any particular information infrastructure could be of many forms, including simply oral communications among individuals. Infinite permutations are possible, and each specific infrastructure will have unique characteristics.

---

[47] Anderson, et al, p. 9.

[48] See Anderson, pp. 12 – 14 for a description of a six-step methodology for determining for a particular case what constitutes the MEII.

Conceptually, the GII subsumes all other information infrastructures. In its simplest rendition the architecture of the GII is portrayed as:

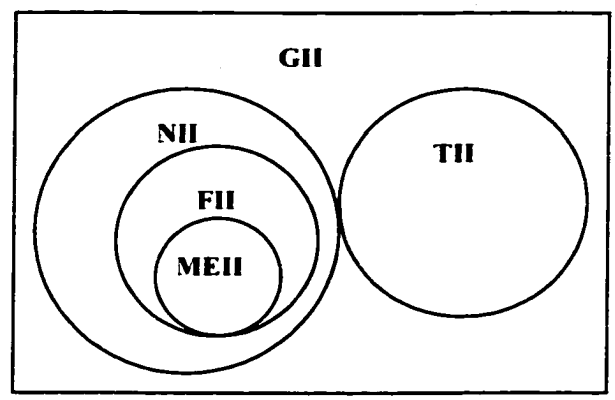


Figure 3-2: Abstract Portrayal of the GII

By definition, the GII is all encompassing; a subordinate information infrastructure cannot be outside of the GII. Argument that information infrastructures shielded from interface with the GII are outside of the GII discount the possibility that surreptitious interface has been or could be achieved by intrusion, infrastructure design flaw, or insider activity. Any conceptual representation of an information infrastructure outside of the GII contributes to a perceptual framework that implicitly denies vulnerability by conceptually denying connectivity, and ignores the physical reality that all information infrastructures co-exist in the same physical space, cyberspace, and time. Conceptually, such hardened information infrastructures are portrayed as shielded structures within the GII, hardened but not eternally invulnerable, thus more accurately portraying reality.

More complex relationships between information infrastructures are possible. One example relevant to conflict is the infiltration of an opponent's information infrastructure.

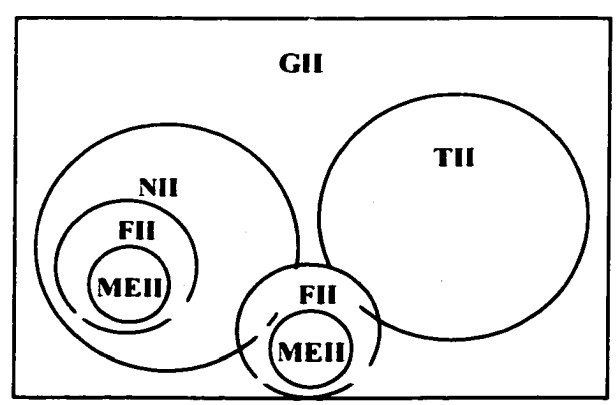


Figure 3-3: Abstract Portrayal of a Penetration Force

The above figure is a portrayal of a force that has penetrated a TII. This could be accomplished with human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), measurement and signature intelligence (MASINT), open-source intelligence (OSINT), technical intelligence (TECHINT), or counterintelligence (CI) assets. The penetration, however, should not be viewed as necessarily a unidirectional flow as the broken lines of the circles symbolize. Agents can be turned into double-agents, and computer or telephone taps can be discovered by the threat and exploited to transmit disinformation. Any interface is a two-edged sword. Firewalls, Intrusion Detection Systems, and other devices can be employed to mitigate potential blowback, but some risk, even if only that of discovery, is inherent in any penetration.

Within a NII, TII, and FII typically exists at least one MEII. Where penetration of other information infrastructures occurs, however, the potential exists that the MEII could be compromised. The MEII, as noted above, is not necessarily a specific hardened information infrastructure, although that may be a component of it. The MEII, again, is a process of ensuring information security of an infrastructure. If that information infrastructure is used to penetrate a TII it is possible during operations that the MEII may itself be penetrated. For this reason, a FII employed to penetrate a TII should be itself isolated from the NII. This is analogous to the standard operating procedure that a specific computer used to hack into a threat network should itself be "air-gapped" from the Blue agency's computer networks. Safeguard measures are not certain, and there will always exist in a complex information system unknown pathways or vulnerabilities that could contaminate the information infrastructure being used to penetrate the TII, and then itself used by the threat to penetrate the NII.

The penetration of the TII also potentially serves to change the nature of the TII. If compromised, the penetration will warn the threat of a vulnerability, causing a response to the stimulus of penetration of its information infrastructure. This potential threat response demonstrates the interdependent and dynamic nature of the security environment.

Interaction does not occur exclusively through direct contact between Red and Blue. Gray, or the security environment, can also be a medium for transmission of information. Information obtained from an opponent is suspect. If, however, the information is obtained from the environment it is accorded higher credibility, due to the perceived difficulty in manipulating the environment to communicate a specific message.[49] In physical space, the measurement of shocks is relied upon to

[49] Jervis, *Perception and Misperception*, pp. 331-332.

determine whether a nuclear test has been conducted. This is information obtained from the environment, not the threat, and thus is accorded credibility.

Explaining the Concept of a Conductive Medium:

The word "conductive," an adjective, is defined as "having conductivity," or "having to do with conduction." This conduction is, in turn, defined as a "conveying," or a "transmission" by the passage of energy or another thing from one entity to another.[50] The trait of copper, for instance, as a conductive medium for electricity is a commonly known fact. Medium, a noun, in turn, is in this context defined as "a means of effecting or conveying something" as "a substance regarded as the means of transmission of a force or effect."[51]

Different media possess traits that allow the conduction of different things with different intensities. The physical world can conduct many sorts of things through its three dimensions; water can conduct soundwaves, and air can conduct scents, and so forth. Here the word "through" is used in the sense of *via*; or "by way of...through the medium or agency of."[52]

Regarding conflict, in a simple form violence is conducted through – *via* – the physical dimensions. Physical space is the conductive medium. Kinetic (or chemical, heat, light, sound, etc.) energy is translated through the physical world against a target, resulting in its injury. At its most primitive level, the conduct of conflict and its effects exist in the realm of the first three dimensions of physical space at an instant of time. Physical space is the fundamental conductive medium of violence. However, it is not the only conductive medium through which means can be employed, nor do some means operate in only one conductive medium.

The conduct and effects of conflict can also exist in the fourth dimension. A slow-acting pathogen does not immediately injury the target; over time, however, the pathogen's effects are transmitted into the first three dimensions in the form of disease. The conduct of conflict through the fourth dimension, or the use of time in conflict, can be of variable duration. In the case of a slow-acting pathogen, the duration could be measured in weeks. This has the potential disadvantage of allowing the target to discover the attack and take countermeasures to defeat it. It, however, has the potential advantage, seen from the attacker's perspective, if not discovered of allowing the pathogen to

[50] Webster's New World Dictionary, 2nd ed. (New York: Simon and Schuster, 1984).
[51] *Merriam-Webster's Collegiate Dictionary*, 10th ed. (Springfield, MA: Merriam-Webster, 1998), p. 722.
[52] Ibid, p. 1314.

be spread through multiple vectors infecting an entire population, thus yielding a more devastating effect on the target.

Other means require much less time, perhaps only the time-of-flight of a ballistic missile, which reduces the use of time, the fourth dimension of conflict, as a conductive medium. This has potential advantages, again from the attacker's perspective, because the target's reaction time is less, and the probability of surprising the target is increased. As the duration of conflict is diminished, it more closely approximates conflict in the three dimensions of physical space at a particular instant in time, with the corresponding reduction in the time available to the target for countermeasures. From this, the efficiency of a specific means in terms of its use of the fourth dimension as a conductive medium can be ascertained. A ballistic missile is more efficient in its use of the fourth dimension than a slow-acting pathogen, given equal effects. However, both still must be transmitted in physical space. Scope of use of a conductive medium also does not equate to effectiveness of the means employed.

Cyberspace as a conductive medium, however, is unique in a few aspects. Cyberweapons can be transmitted and act at, literally, near lightspeed. This is potentially hyper-efficient in its use of the fourth dimension, approaching a point at which time, because so little is required, is not a significant constraining factor in their employment, and thus not a robust conductive medium to counter a cyberstrike and engage a threat. During a cyberstrike, time to respond is usually limited. However, cyberweapons can also be programmed to remain dormant until a specific point in time, triggered by either the passage of time, or by an event taken by either Self or Other, or both. Additionally, cyberweapons can be designed to attain effects in the physical world, cyberspace, or both. When cyberweapons are employed in a delayed mode, time becomes a conductive medium for countering them to the degree that there is a delay in activation. A dormant computer virus can be found, if Self is allowed time before it activates.

The effects of cyberweapons can also be viewed as *almost* a one-way street for the conduct of offensive conflict and its effects. An Other (here a threat) in conflict with Self that operates in cyberspace may be relatively invulnerable to actions taken by Self in the physical world. For example, an information warfare team based abroad cannot be effectively engaged by a conventional military force. However, the information warfare team can effectively engage the conventional military force in both physical and cyberspace. This renders the conduct of conflict and the transmission of its effects almost a one-way street from cyberspace into the physical world. It is not a perfectly one-way vector, as the potential exists for Self to discover the location of the Other's information warfare team in physical space and kill it. However, this countermeasure must operate in six dimensions, or

conductive media: a killer team must be assembled by Self and move through physical space, time must be available for Self to take this action, the information warfare team must be sensed by Self in cyberspace, and the true identity and location of the Other must be perceived by Self. Other can easily deny any of the six required conductive media to Self by: either striking in real time, and then disengaging before Self can counter, or, employing a time-delayed cyberweapon; moving in physical space following the attack; cloaking its presence in cyberspace through stealth; or, altering Self's perception of what has happened, for instance, portraying the cyberstrike as a hardware failure or software glitch.

Other can design a *modus operandi* that, in effect, makes it a stealth actor. By avoiding activity in the physical world, Other renders itself invisible to Self's Hegelian simple sensuous Consciousness. Self's traditional intelligence collection methods fail, including signals and human intelligence, if Other exercises discipline in the physical world. There are no uniforms, organizations, buildings, symbols, or other physical evidence of the existence of the Other. By using the fourth dimension intelligently, Other denies Self the time to counter an attack or to learn over time during a brief engagement. By limiting its presence in cyberspace to the minimum required in both cyberspace and time to accomplish its operation, Other minimizes its signature and the ability of Self to sense it in cyberspace, hence Other denies Self the sixth dimension. In the dimension of perception, Other's precautions in the first five dimensions of conflict lessen the ability of Self to perceive even the existence of Other. Additionally, Other may also employ deceptive techniques as an *a fortiori* precaution to confuse Self's ability to accurately perceive Other's true identity should Self become aware of Other's existence. To the degree that Other remains stealthy, it possesses all initiative of action, thus offensive capability. Self can only defend against intelligent stealthy actors, and is denied preemptive courses of action. Preventive courses of action, to some degree, may still be possible.[53]

One preventive course of action is to cause no offense without good cause. In a security environment where Blue (i.e., the United States) is a fixed, visible target pursuing global interests, inevitably there will be some actors provoked into attacking Blue. A criterion for deciding on courses of action should consider implications resulting from implementation, specifically the provocation of

[53] The Department of Defense Dictionary defines a preemptive attack as "an attack initiated on the basis of incontrovertible evidence that an enemy attack is imminent." The concept of prevention (vice preemption) is based in the belief that "conflict, while not imminent, is inevitable, and that to delay would involve greater risk." Thus, prevention as a possible option, when feasible, temporally precedes preemption, because the development of a threat capability logically transitions through a "not imminent" phase before reaching an "imminent" phase. Whether a preventive option is exercised depends partially, among other factors, on whether a threat capability or activity is perceived. Document available at http://www.dtic.mil/doctrine/jel/doddict/.

other actors, either known or by pure-type typology. Implementing, for example, a heavy-handed policy of overt, military confrontation in a volatile region may have costs to Blue beyond the scope of known actors in the region. If the policy is based along a metaphysical divide, like religion in the Middle East, a policy of confrontation may provoke intelligent stealth actors to exact costs from Blue for pursuing the policy. This calculus of cost – benefit is more nuanced than simpler analysis involving only known actors. Given the difficulty of deterring and retaliating against unknown actors, the decision criterion of "make no enemies without need" may be a prudent approach. In a single Superpower world, there is a single best target for asymmetric actors dissatisfied with the status quo.

Other can choose the conductive media in which it operates, becoming a specialist, niche threat. Self, if an industrialized, developed state, must operate in all six of the dimensions of conflict or face the sucker's payoff in the game of Stalker. This is not only resource intensive, it is also difficult to craft security policies that can coordinate the diverse efforts in a holistic fashion. Other, however, is streamlined, anonymous, purposeful, and capable of employing asymmetric and asynchronous techniques of conflict. It is able to plan its operations deliberately, analyzing them in premeditated fashion for weakness and flaws. It also possesses the initiative, and can choose the conductive media for its attack. Such an Other stalks Self.

The Six Dimensions of Conflict:

Conflict is manifested in multiple dimensions. The Red, Gray, and Blue framework posits six dimensions of conflict. Examples of the conduct of conflict and its effects are readily sensed in the three dimensions of the physical world, or the Hegelian simple sensuous Consciousness that is the immediate certitude of an external object. The physical engagement of forces on a battlefield at a given instant is an example of the conduct of conflict in three dimensions. A razed city at a point in time is an example of the effects of conflict in three dimensions. However, what is sensed is, respectively, only the conduct or the effects of conflict as manifested in the three dimensions of physical space. These three dimensions constitute the first three dimensions of conflict. It is in the physical realm that the effects and conduct of conflict is made tangible.

The range of physical space within which conflict occurs and has effects is not limited to the terrestrial or intra-atmospheric. Space is a physical dimension within which conflict is pursued. Yet, the conduct and effects of conflict in space are often beyond natural human sensory capabilities. Human observation of conflict in space, for example, astronauts aboard the space shuttle peering through ports or observation using ground-based optics, is physically possible. The direct observation of the destruction of an enemy satellite is possible. But barring such exceptions, the conduct and effects of conflict in space (or beneath the sea or on land beyond the range of human senses) can only

be observed with the aid of technological sensors and other means. When not directly observed through natural human senses, the conduct and effects of conflict in space are still capable of being indirectly sensed. The abrupt cessation of an enemy satellite transmission, for instance, that corresponds in time to the employment of a weapon against it suggests the effects of conflict beyond natural human senses. The remote observation of the weapon through space-based digital video transmissions through cyberspace and its engagement of the enemy satellite provides more certitude, however, than did the abrupt cessation of transmission. As sensing moves from direct experience, or the Hegelian simple sensuous Consciousness, to indirect knowledge of effects by inference through other dimensions, certitude is diminished. As certitude is diminished, the potential for misperception and deception increases.

The conduct and effects of conflict, however, are not limited to the dimensions of physical space. Conflict also exists in the fourth dimension of time. Conventional, tactical examples familiar to most include ambushes that exist for hours before the trap is sprung, or minefields that endure over years as evidence of conflict and the effects of conflict between actors. The existence of conflict in the dimension of time is not sensed directly through the observation of time itself, but is rather indirectly sensed in the fourth dimension through observation in the first three dimensions. Time cannot be directly sensed or ascertained with natural human senses. The passage of time is indirectly observed through effects in physical space. Thus, the difference in position of the hands of a functional watch indicates a measurement of what cannot be directly observed or measured - time - much like the passage of water in an opaque pipe flowing past a functional meter. The passage of water was not directly observed, but was indirectly sensed through measurement of its flow through the meter. The observation of the conduct and effects of conflict across time by indirectly and continuously observing physical space allows great certitude concerning its (the conduct and effects of conflict's) scope in the fourth dimension. To the degree that this indirect observation is not continuous, certitude concerning the scope of the conduct and effects of conflict in the fourth dimension is diminished, and the potential for misperception and faulty inference increases. For example, the continuous observation of a functional surveillance camera transmission trained on a sensitive area affords high certainty that the area has remained undisturbed during that time it was continuously observed. However, the checking of the displayed image by a security guard once at the beginning of a shift, and then once again at the end of the shift does not provide certitude that the area has remained undisturbed during the shift between observations. Time is dynamic, not static. Intrusion can occur without leaving lasting evidence in physical space. As time is dynamic, the evidence of intrusion will dissipate unless captured on a recording medium or through a sensor.

The conduct of conflict in the fourth dimension is multifaceted. Not only is duration in time a consideration, but the timing of an attack, the amount of time required to attack, presence and patterns of activity across time, absence of activity across time, the prepositioning in space or cyberspace of time-delayed mechanisms, and other techniques of conducting conflict in the fourth dimension are important aspects. The existence of a minefield at a single instance in time is a manifestation of conflict in physical space; it becomes manifest in the dimension of time when it exists through time, as manifested by its continuing existence in physical space. Similarly, the absence of a minefield in space at one point in time can be exploited by Self to portray a temporally contingent reality to Other, which then acts based on this knowledge of reality without knowing of its temporal fragility. However, the subsequent emplacement of a minefield alters physical space at a given instant, and Other suffers the effects of operating from a conception of reality that was accurate at one point in the fourth dimension, but not accurate at all points in time. An ambush that is routinely emplaced during the hours of darkness does not exist during hours of daylight, either physically or temporally. During darkness, however, the ambush exists in both time and space. But it is only the direct observation of other dimensions that allows for the measurement of time. A single observation at a point in time does not allow one to infer how long a conflict has been in existence, or to know when it will end or undergo change, or any other temporal aspect of the conflict. The temporal aspects of conflict can only be known through direct observation of other dimensions through time.

This indirect observation of the conduct of conflict and its effects across time through other dimensions introduces an intermediate distortion of reality. Simply put, the occurrence of an event in time is measured by apprehending it in other dimensions. Even if the event is directly sensed in physical space at the instant of its occurrence, the actual position of the event in time is distorted at a minimum by the transmission time of the light waves from the event to the observer's retina, and some additional time for cognitive processing and recognition. In conflict in other dimensions, however, it is not always the lag time from event occurrence to cognition that matters; it is the lag time from event occurrence to effective reaction. Self is defeated in the fourth dimension, which ultimately is translated to other dimensions, if Other can complete its attack, despite Self's awareness of the on-going attack, before Self can effectively transition in other dimensions to counter Other's attack. For example, reinforcements that arrive too late may have been able to defeat the enemy in physical space, but the reinforcements were preempted by the enemy in the fourth dimension. Late reinforcements arrive after the battle is already decided, and their physical superiority over the enemy is moot. To the extent that intermediate distortion of time is present, certitude concerning the true reality in the fourth dimension is diminished. Within this window of temporal distortion asymmetric threats conducting conflict in dimensions other than physical space, i.e., cyberspace, can operate with impunity. A threat's effective use of the dimension of time, itself a neutral component of the environment, confers

security. An asynchronous threat operates in the interstices created by its effective use of the fourth dimension in the three dimensions of physical space.

Cyberspace – The Fifth Dimension of Conflict:

Cyberspace is not a homogenous construction that means the same thing to all actors. An individual accessing the Internet from a "smart" cell phone operates differently and with different tools and capabilities than a major Internet Service Provider (ISP). The individual's web presence also differs in both quantitative and qualitative aspects from another actor's activity. However, whether an individual or a global ISP, both actors actively participate in cyberspace; the same medium affects and shapes both actors' activities within the fifth dimension.

The elements of sameness of cyberspace that affects both actors, for example standard communication protocols that govern electronic interaction, could be understood to constitute a "deep structure," or undergirding element of the medium. Surrounding each of the two illustrative actors, however, the aspects of the medium are very different. Quantitatively, perhaps measured in bandwidth or other factors, there is an immense difference between an individual's single access point, or point of presence, and an ISP's potentially thousands of access points into cyberspace. Qualitatively, the content, purpose, identity mask, and potential methods of interacting with other actors between the two actors' aspects are very different. This difference is not necessarily due to a difference in standards that constitute cyberspace as a viable medium, but to factors unassociated with how the medium functions. This portion of cyberspace can be understood as the "shallow structure" of cyberspace. A metaphor is a limited tool, but here one may illustrate the point. An ocean is basically comprised of seawater, and in the middle of an ocean it may be the only constitutive element present. This is the "deep structure" of the ocean. But as one approaches an island, one discovers that a specific island has surrounding it reefs and a much shallower, variable depth of water. Additionally, it has a beach, a port, and a few passage points from the ocean through the reef to the beach. This is the "shallow structure" of the ocean at this location.

Any metaphor if over-extended will break, however, this limited use illustrates a point. Cyberspace is not a homogenous construction. Only the "deep structure" of cyberspace approaches homogeneity; the shallow structure of cyberspace is radically differentiated across different actors, as our example of the difference between an individual and a major ISP demonstrated. Actors in cyberspace interact with other actors in the shallows of cyberspace, not in the deep structure. An individual browsing through cyberspace encounters a web page, and recognizes the web page as belonging to a friend. The specific aspects of the shallow structure of cyberspace surrounding this

friend's web page have been translated from the fifth dimension to the sixth dimension – perception. Leaving his friend's web presence, the actor browses to the web site of a major international corporation. The shallow structure of cyberspace and the specific aspects of this specific shallow structure are translated into the actor's perception that this is a different actor, with a different appearance, opportunities to interact, different content, and other quantitative and qualitative factors.

Many texts on Internet architecture typically have a "Figure 1-1." This figure generally shows two computers connected by a line through a "cloud." Figure 3-2, below, is a stereotyped depiction of this classic figure.[54]

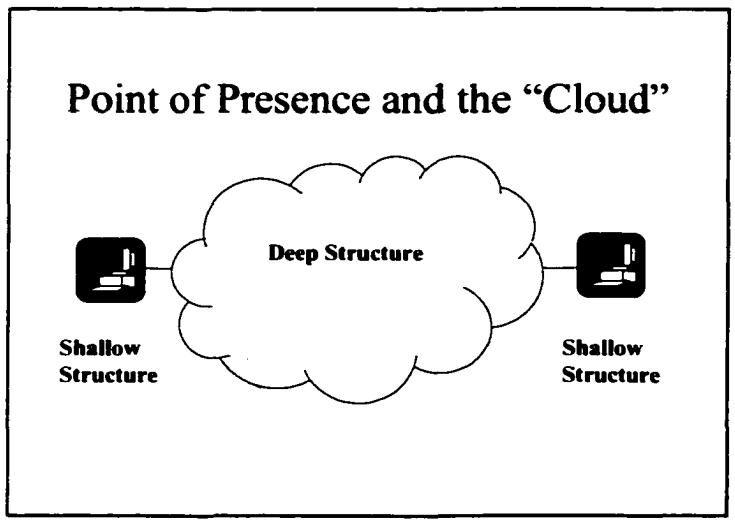


Figure 3 – 4: Point of Presence and the "Cloud" of Cyberspace's Deep Structure

The deep structure is the constitutive materials of cyberspace: the hardware, firmware, software, standards, and protocols that maintain an all-encompassing virtual environment of all electronic communication infrastructures. It is more than "the net." Shallow cyberspace is where interaction takes place, chat rooms, web pages, and even on phones. Shallow cyberspace is "noisy" and deep cyberspace is "quiet" and in the background, or underneath the surface of activity. Monitoring shallow cyberspace entails monitoring communications, but monitoring deep cyberspace entails monitoring the shape of cyberspace itself. The inclusion of a new constellation of communications satellites into cyberspace alters the shape and scale of deep cyberspace. This has profound meaning if analyzed from a national security framework. Both deep and shallow cyberspace grow, shrink, and change shape. Very importantly, if an actor can control deep cyberspace, it can then

control shallow cyberspace, in so far that it can monitor, disrupt, or deny interaction and communication. But this does not mean that all communications transiting the deep structure will be understood if monitored. Encryption and other techniques of cryptography can render a communication's substance opaque, as well as steganography and digital watermarking. But in the deep structure of cyberspace, the communications can still be "seen."

In terms of the figure shallow cyberspace exists from the "point of presence," or "edge," to the actor. Here is found the differences in configuration and other aspects that differentiate one actor in cyberspace from another. Within the "cloud" is the deep structure of cyberspace. This is not a clear demarcation or hard boundary between the shallow and deep structure of cyberspace. Standards exist in shallow cyberspace, for example coding, that is uniformly applied in the shallows surrounding many actors. Nor is deep cyberspace devoid of all evidence of presence. But there is a boundary, and cyberspace is not homogenous.

The Sixth Dimension of Conflict – Perception:

The sixth dimension of conflict is partially constituted by the influences of the first five dimensions. In turn, the sixth dimension of conflict influences the first five dimensions. The activity of Self and Other in the first five dimensions influences how Self and Other define each other's role, respective to each other. These practices constitute the interaction between Self and Other, which defines their roles and perceptions. Hegel's Master and Slave were both men, but the difference between them was their interaction in physical space and time. This pattern of interaction informed, then reinforced, their perspectives of Other and defined their roles as Master and Slave. Perceiving himself to be a Slave, the Slave acted towards the Other as his Master, and the feedback from the sixth dimension thus influenced the dimensions of physical space, time, and the actors' actions.[55]

Identity and role played by an Other can be inferred from action. Where these actions are objectively quantifiable, they can be used as parameters in modeling. The parameters of a specific interaction can be monitored, and based on their values, an assessment of identity or role made. A simple example is a log-in routine protecting an actor's computer network. Various activities, e.g., logging in, can be monitored, and the parameters measured, for instance password values. If the parameters in the model correspond to an actor identified as a legitimate user, then the identity is assessed by the model as a friendly user, and access to the network is granted. If the activity's measurement does not correspond to a value designated as "friendly," the model could flag the activity

[54] The concept and figure applies to networks other than the Internet, as well. See Ray Horak, *Communications Systems & Networks* (Chicago, IT: M&T Books, 2000), figure 1-1, p. 2.

for further, perhaps human, analysis. In this simple example the activity in the first five dimensions determined an assessment in the sixth dimension.

Jervis states "If he is to decide intelligently how to act, a person must predict how others will behave."[56] This prediction is based on Self's perception of Other's identity. If seen as a threat, Self will infer that Other will act counter to Self's interests. If perceived as an ally, then Self will infer Other's actions will not be counter to Self's interests. It is this dynamic within the sixth dimension that drives the activities of the first five dimensions. This dynamic is recognized by both Self and Other. If experiencing hostile activity in the first five dimensions, Self infers that Other views Self as a threat, and is acting accordingly. This dynamic can be altered by either actor through complex learning. Wendt explains "On the "we are what we do" theory of social interaction...by acting as if it had a new identity and teaching the Other what it must do to help sustain that identity, each actor erodes his previous identity and learns to see himself in the mirror of the Other, changing his conception of who he is."[57]

Perception is both simultaneously cause and effect. Sophisticated actors recognize this dynamic, and adjust their actions and identity masks accordingly. Skillful exploitation of perception formation can create surprise and operational advantage. To the degree that factors can be modeled and objectively measured, automated analysis can discern, at least tentatively and superficially, the identity and role of an Other. This is an important contribution of models, especially in the fifth dimension where physical reality cannot be apprehended with human senses and communication is limited to digital transmissions, excluding other forms of communication like direct observation of the actor and actor's actions that would provide a richer context for understanding.

Indications and Warning

How might one conceptualize the six dimensions of conflict in a way that would allow an observer to apprehend indications and warnings of threat? A visual representation of the six dimensions would be based on a foundation of the three dimensions of physical space. One example would be a high-resolution depiction of a city which an intelligence source or analysis suggests could serve as a base for a known or potential threat. The fourth dimension runs in real time within the city's depiction, with changes in landscape and the positions of sub-elements (cars, buses, people, etc.) shown. So far, this simply corresponds to the real time transmission of video images from traffic and surveillance cameras into an operations center – a common and ubiquitous system in many world

---

[55] Wendt, *Social Theory of International Politics*, p. 335.
[56] Jervis, *Perception and Misperception*, p. 32.

cities. Alternatively, it could correspond to a high-resolution satellite image feed in real time, or a hologram. Overlaying this image would be an integrated sensor-fed depiction of cyberactivity within the area under surveillance. This could be as simple as a graphic representation based on a binary variable, showing nothing overlaying the image in the absence of cyberactivity, with the presence of cyberactivity shown as a colored zone superimposed over the image at the physical space were the cyberactivity is emanating. Alternatively, greater detail is conceivable, with the absence of a superimposed image denoting no cyberactivity, and various colored zones superimposed over locations of cyberactivity to signify whether the activity is attributable to a military, commercial, organizational, individual, other, or unknown entity. Further discrimination is possible, based on type of device used to access cyberspace, e.g., web-enabled phones, desktop computers, or an entire information technology complex. This image as described so far accommodates the first five dimensions of conflict. The sixth dimension, perception, could be modeled based on defined parameters of activity observed. If an activity's parameters (cell phone number, satellite phone transmission signature, etc.) corresponds to a known or suspected threat actor, an alert symbol would be projected onto the image at the location where the transmission emanated, sensing occurred, or the best approximation of location was calculated, and automated resources engaged to capture data. Advances in GPS technology, and the embedding of GPS in many systems including cell phones, personal computers, and automobiles makes this technically possible today. Other types of transmissions could be located using triangulation informed by ground, air, subterranean, or space-based sensors. Additionally, sensors positioned within the information infrastructure could feed data regarding communication details to the operations center in either a push or pull capacity.

At the next level of empirical analysis, this data could be captured and archived. Analysis of patterns by both human analysts and artificial intelligence may suggest possible futures. This is, in effect, what meteorologists do with their models when forecasting future weather patterns. Using historic data, integrated with current knowledge of on-going weather effects, they forecast whether it will rain or not. City planners, similarly, use historic traffic flow data, supplemented with current knowledge of street and other conditions, to project future traffic patterns. An analogous use of past data reflecting the six dimensions of conflict, supplemented with real time surveillance, may indicate potential locations for the employment of additional sensors to more intensely monitor trends across type, location, timing, and other traits, and thus provide indications and warnings of future attack.

Inductive approaches are useful and necessary. However, when used without a deductively derived theory or model, they pose the danger of mistaking spurious association for meaning. A familiar example is the association between height and mathematics achievement test scores. Both are

---

[57] Wendt, *Social Theory*, p. 346.

dependent until a plateau is reached upon other factors such as age and continuation of educational progress. Brute force computational approaches to indications and warning are theoretical cul-de-sacs and, again, demonstrate that bad theory results in bad policy.

The Levels of Conflict – Strategic, Operational, and Tactical:

Not all conflicts are equal in scope or effects. Because of this, when weighing security policy options decisionmakers either formally or informally assess the stakes involved. This assessment of the stakes involved extends in the fourth dimension to include expectations of future behavior.[58] Crafting a national security policy to counter a threat capable of only minor effects at a local level is neither an appropriate response nor a wise use of resources. Similarly, placing a strategically important relationship in jeopardy of future diplomatic tension over a present, minor gain is also imprudent. The judgement of the decisionmaker is informed by, at the minimum, a rudimentary, intuitive understanding of the scale and type of an appropriate policy response to a specific threat. This judgement is based on both a quantitative and qualitative analysis, however primitive or sophisticated, conscious or subconscious, of the threat's capability and intent to cause effects. Addressing the need of a decisionmaker to exercise this judgement, Clausewitz stated that:

> "*First*, therefore, it is clear that war should never be thought of as *something autonomous* but always as an *instrument of policy...Second*, this way of looking at it will show us how wars must vary with the nature of their motives and of the situations which give rise to them. The first, the supreme, the most far-reaching act of judgement that the statesman and commander have to make is to establish by that test the kind of war on which they are embarking; neither mistaking it for, nor trying to turn it into, something that is alien to its nature. This is the first of all strategic questions and the most comprehensive."[59]

Clausewitz's first point is that conflict should not be prosecuted mindlessly for the sake of conflict itself, but rather to accomplish an end. The wise design and management of violence is not found in blind action, but in deliberate calculation. Conflict is a means to an end, and in designing wise security policy the ends dictate the quantitative and qualitative traits of the means – conflict – employed. Clausewitz's second point instructs that the quantitative and qualitative aspects of conflict are dependent variables, with the ends ("nature of their motives") desired and the security environment ("situations which give rise to them") acting as independent variables.

---

[58] Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976), p. 103. See also Robert Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 1984), pp. 126-127.

[59] Carl von Clausewitz, *On War*, Michael Howard and Peter Paret, eds. (Princeton, New Jersey: Princeton University Press, 1976), pp. 88-89.

The quantitative and qualitative aspects of a potential conflict interact and overlap to some degree. A large-scale conflict, for example an historic struggle between empires or a world war, is of a certain qualitative character, regardless of whether it was prosecuted with swords or modern weaponry. In this case, a quantitative difference of degree translates into a qualitative difference of type. Similarly, a conflict involving the most modern and lethal weapons (excepting for the moment WME, which will be addressed separately), but which is only of a few minutes in duration, strictly limited in geographic scope, and resulting in limited effects is more aptly termed a firefight or an engagement, but not a war.

The assessment of the quantitative and qualitative nature of conflict is an empirical conclusion, however, it is not easily calculated in hard, discrete terms. An ordinal ranking outlining the scope of a conflict is useful as a cognitive tool for decisionmakers. Assessing a conflict as tactical, operational, or strategic has served decisionmakers over time and across cultures to better understand the stakes involved in a specific conflict. The divisions between the ordinal categories, however, are not distinct, because conflict exists along a continuum, not in discrete categories of precisely quantifiable, interval data.

Past examples of ordinal ranking of conflict have been advanced and, ultimately, discarded. One categorization ordered conflict as Low-Intensity, Mid-Intensity, and High-Intensity.[60] However, this ordinal ranking was based on the means, including force size, composition, organization, methods, and weapon types employed in the conflict and not the effects or ends of the conflict. Clearly, this conflates the traits and employment techniques of the means with "the kind of war upon which they are embarking," exactly counter to Clausewitz's caution against such reasoning. This mistaken reasoning of the conduct and effects of conflict *a priori* categorizes guerrilla warfare as Low Intensity Conflict, although the end, and ultimate effect, of such conflict may be the complete overthrow of a legitimate, sovereign government.

State-centric, conventional means based ordinal categorizations of the conduct, effects, and ends of conflict are irrelevant for describing, explaining, and predicting the actions of asymmetric actors. However, using the ordinal categories tactical, operational, and strategic has utility for understanding the ends of such actors.

---

[60] For example, mid-intensity conflict was characterized by large-scale, conventional warfare, and high-intensity conflict by crossing the nuclear threshold. Low Intensity Conflict (LIC) as a term has survived in US military doctrine, however. See Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms* (Washington, DC: Office of the Joint Chief of Staff); and US Army field manual FM 100-23, *Peace Operations* (Washington, DC: Department of the Army, 30 December 1994), p. 84.

Strategic targets are vital to an actor's political, military, economic, or social-psychological elements of power. Strategic conflict has the end of significantly degrading these elements of power. The effect of a successful strategic attack is to severely impede the actor's capability or intent to carry on with a conflict, perhaps by targeting a critical system composed of multiple critical infrastructures (e.g., energy).

Operational targets are essential to an actor's capability or intent to conduct coordinated, distributed, and often large-scale operations. These targets could be critical infrastructures without which activity supporting a conflict's prosecution cannot continue effectively. An example would be the electrical power critical infrastructure, itself a component of the energy infrastructure.

Tactical targets affect an actor's capability or intent to conduct engagements of relatively limited scope. An example of a tactical target would be a local telephone exchange, or an electric power distribution sub-station.

The levels of conflict when used to describe the conduct and effects of conflict by conventional forces frequently coincide with the geographic scope of effects. A tactical target is a localized target with a local effect, while an operational target could be a major sea, air, and rail port facility supporting an entire region's logistical network, while a strategic target could be the actor's capitol city.

However, the levels of conflict when used to describe the conduct, effects, and desired ends of conflict by asymmetric actors will frequently not correspond to geography, but to systems, critical infrastructures, and population. A threat employing an asymmetric means can achieve strategic results. A computer virus can disable vast networks, achieving an operational and perhaps even strategic effect, although the threat employing the virus may be an individual, or First Image actor. This renders state-centric understandings of the levels of conflict obsolete.

Targeting Critical Infrastructure and Population:

The Red, Gray, and Blue framework posits Blue's vulnerabilities not in terms of conventional military forces in the field or any other past measures, but in terms of critical infrastructures and population. This is because asymmetric actors, the focus of this study, neither are required nor desire to confront strength to attain their desired ends. Where targeting is required, asymmetric threats will attack weakness that supports attaining their ends, and proceed from this as a point of departure in

conducting their mission analysis, and not from some *a priori* defined target set traditionally held as important.

This is not to say that military assets will not be targeted. Numerous examples of asymmetric actors attacking military targets exist. But these attacks, whether bombings or assassinations, attacked military targets in asymmetric fashion, and not conventionally. Frequently the military target was not directly relevant to the conflict, but was a symbolic target representing American power. The attack of the USS Cole on 12 October 2000 by two men in a boat carrying explosives was an asymmetric attack targeting a symbolic target during a moment of weakness – a refueling stop in a small port in Yemen. The USS Cole itself, an Aegis cruiser, is not a means directly relevant in a conflict with global terrorist organizations. The value of the USS Cole as a target was symbolic, and not an operational necessity of the terrorists in their conflict with America.

Random targeting is not the *modus operandi* of most threats. Those who would argue, for example, that terrorists are indiscriminate in killing innocents mistake the victim for the target. In such cases, the victim actually is a conductive medium for transmission of the message to the true target: the population at large and the institutions of government. Bruce Hoffman points out that "The wrath of the terrorist is rarely uncontrolled. Contrary to both popular belief and media depiction, most terrorism is neither crazed nor capricious. Rather, terrorist attacks are generally both premeditated and carefully planned."[61] In this classic view of terrorism, the victim is the conductive medium.

Random targeting and completely irrational activity is, of course, possible. Limitations of weapons and technology have in the past limited the scope of effects, thus the level of conflict, resulting from actors targeting in a random, chance fashion. A delusional madman with a pistol undeniably has an impact when he inexplicably shoots an innocent bystander, but objectively it is confined to a short-term, tactical effect that does not threaten the population at large, critical infrastructures, or the institutions of government.

Technology, however, has increased the potential scope of effects that can be achieved by an irrational First Image actor. Employing a toxin will potentially inflict more casualties than a pistol, and threaten a much larger portion of the population. Currently, obtaining and using WME is more complex than the employment of conventional weapons. WME acquisition and employment is not a simple matter, and this serves to increase the difficulty of an irrational actor achieving a large-scale

[61] Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), p. 157.

effect. The advance of technology and the proliferation of knowledge concerning WME building will work to lessen the challenge of WME acquisition.

By definition, an irrational actor acts in a fashion that is divorced from logic and defies prediction. It is likely futile to attempt a study of how completely irrational actors choose targets if explanation and prediction is desired. In the case of a completely irrational actor, warning of a specific attack is confined to scenarios of accidental discovery. Precautionary defensive measures are the best actions to counter a truly irrational actor. Given the increasing proliferation of WME, whether cyber or CBRN, adequate defensive measures must be designed and implemented. Because of the effects of WME this presents a massive challenge and results in a far different world than implementing defensive measures to counter the still present conventional dangers such as a deranged individual with a handgun.

Thankfully, WME employment is not necessarily easy. Effective use of many WME requires rigorous employment techniques, specialized targeting, and thorough knowledge of technical aspects of the WME characteristics, as well as environmental conditions. This is not always the case, especially with cyber weaponry. Assuming a deranged individual acquires a WME, employing it effectively may itself present a challenge orders of magnitude more difficult than the indiscriminate use of a pistol or a bomb. A hypothetical scenario of an irrational actor using WME requires several prerequisites be accomplished before an effective attack. The actor must first acquire, build, or cultivate a WME, a task that requires premeditated and knowledgeable effort, again, excepting cyberweaponry which can be downloaded from the Internet on demand. The actor must then select a target capable of being engaged by that WME. Not every target lends itself to effective attack by some categories of WME, and even weather and wind patterns can negate the effects from some types of WME. Finally, the actor must employ the WME using appropriate technical protocols. This, also, demands specialized knowledge and efforts. This is not, of course, an exhaustive listing of tasks involved in WME employment; rather only the most general stages of effort. Specialized tools and machinery to assist in building or cultivating some WME are often also required, which presents further challenges. The difficulties illustrate that the scenario of a deranged individual employing a WME effectively is, although possible, not necessarily easy.

It would be a significant mistake to infer, however, that WME will not be employed by actors whose concept of rationality differs from a "mainstream" perspective. This is a different actor type than a deranged individual. For example, suicide attacks are, from the perspective of a Shi'ah Islam

martyr, completely rational acts.[62] Inflicting mass casualties against non-combatants is a rational option for a terrorist. These and other actors operate from different perspectives of rationality. Culture counts in defining an actor's perspective of rationality. These perspectives are, however, internally consistent belief systems that can be understood, explained and potentially anticipated, unlike the capricious, impromptu activity of a wholly deranged individual. In modeling Red, the social-psychological aspects are important.

WME use by actors with different concepts of rationality is not only possible, but has occurred. It is probable that it will become more common. Limited in the past by the technological characteristics of available weaponry, actors who previously possessed intent to inflict significant harm, but lacked the capability, can now possess both. President Clinton assessed the future use of WME within the continental United States as "highly likely to happen sometime in the next few years."[63] President Bush has also expressed this position.[64] Other senior national security officials have expressed similar views of the probability of terrorist WME employment. Threats operating from different belief systems nevertheless possess faculties of reason, and are capable of premeditated, purposeful activity to gain and use WME.

A thorough understanding of Red is essential, because a threat will target for reasons based within its belief system, and will not act in a haphazard, random fashion. The nature of the threat dictates to some extent its *modus operandi*. By knowing the threat's capabilities and "operational code" a *modus operandi*, in broad terms, can be to some extent mapped. Prediction, of course, is not a certain science and there are always exceptions. But the adage "know you enemy" remains indisputably good advice, and more important in the current security environment than ever.

The worst-case scenario is such an actor armed with a WME, capable of and intending to employ it in optimal fashion to inflict maximum casualties and damage. This threat actor understands that small-scale, tactical attacks are most simply and effectively accomplished using conventional weapons or bombs. If only a tactical effect was the objective, it is less probable that an actor would pursue an expensive, time-consuming, complicated, and dangerous-to-self course of action involving WME. Instead, this Other will target for strategic effects, and critical infrastructures and population

---

[62] Several passages from the Qur'an, the Sunnah, and ahadith detail the rewards of a martyr. See the Qur'an (3:169-172), and the hadith *Sahih Bukhari* (Vol. 2, Book 23, Number 329; Vol. 9, Book 93, Number 555).
[63] William J. Clinton, *Oval Office Interview of the President by the New York Times on January 21, 1999* (Washington, D.C.: Office of the Press Secretary, 23 January 1999), p. 3.
[64] *Remarks by the President to the Troops and Personnel of US Joint Forces Command*, USJFCOM press release, 13 February, 2001 (Norfolk, VA: US Joint Forces Command), p. 2.

are the best targets for such purpose. Understanding how to target critical infrastructures is the first step to understanding how to protect them from attack.

Although as old as war, targeting critical infrastructures is an approach in targeting methodology that made significant strides in sophistication during World War II. Allied planners studied the Nazi war machine and targeted railyards, ports, factories, and other systems in an effort to shorten the war. Perhaps the most elaborate example of infrastructure targeting, however, is the Single Integrated Operation Plan (SIOP) first drafted during the height of the Cold War. The SIOP details the nuclear attack options available to the President of the United States, and the Cold War version was based on extensive analysis of the Soviet Union's forces, systems, and infrastructures.

An actor sophisticated enough to possess a WME is capable of understanding how to target for strategic effect. It is unlikely that it will target an unpopulated section of arid desert in Nevada, having gone to the expense, effort, and danger to obtain a WME. The targeting will likely be against a critical infrastructure or a population concentration, such as a large city.

In selecting a system to target, the identity of the threat will influence, but not necessarily determine, the choice. A threat actor interested in immediate, dramatic media footage of casualties would have a targeting preference against the population, while an actor motivated by anti-capitalist ideology would perhaps target the banking and finance system. The type of actor only suggests targeting preferences; ultimately, a significant, successful attack against any of the critical infrastructures cascades effects into other systems.

The cascading effect from one infrastructure into others is the result of several related factors. Historically, many of these systems were independent of and isolated from each other. As technology progressed, a search for increased efficiency in asset allocation led to increased interconnectivity of systems. Shared resources, such as phone lines to transmit data, were too expensive to build as redundant, single system-dedicated mechanisms, and their sharing by different infrastructures further tightened the couplings between systems. The current interlinked and automated nature of critical infrastructures has created vulnerabilities and the potential for a failure in one system to proliferate through linkages into other systems.

A critical system may contain multiple critical infrastructures. For example, the national energy system (energy is a critical system) is comprised of at least four critical infrastructures: the transportation infrastructure, including pipelines for oil, railroads for coal, and both marine and over-

land oil tankers; the oil and gas production and storage infrastructure; the electrical power infrastructure; and the telecommunications infrastructure, which controls data transmissions among all the infrastructures. All of the infrastructures detailed above are complex systems distributed across vast geographic areas. Targeting such complex, distributed systems demands rigorous analysis to achieve optimal results from the employment of finite means. Within a critical system, multiple targets are present. Target analysis of critical systems focuses on the interaction between its multiple, constitutive target systems, with an objective of determining the most effective way to affect the critical system in the desired manner.[65] For example, an attack against an oil storage facility would encounter numerous physical security systems including armed guards. Assuming these protective systems could be defeated, the question remains how to damage the oil stockpiles, which in the case of the national Strategic Oil Reserves is located thousands of feet underground in huge caverns created in the salt domes of the Texas and Louisiana Gulf Coast regions.[66] Critical system analysis may reveal that the key vulnerability to the oil reserves is its data transmission facilities controlling critical sensor and valve mechanisms.

A target system within a critical system is a category of targets based either on geographic proximity, effects-based results of disruption, or a system-based category. Defining a target system based on geographic proximity is self-explanatory. Effects-based target system definition means that the disruption or damage to the group will produce a specific effect desired by the attacker. This desired effect may be to cross the threshold of the strategic level of conflict by a First Image actor. An example could be the interruption of the distribution of electricity to a specific world-city, which would entail targets from different electric power sub-systems in different geographic locations. What groups these targets together is the desired effect: disruption of power to a specific world-city. A system-based category is constituted by all targets within a given system. An example would be bulk electric power supply facilities.

A target subsystem is a fundamental constitutive element of a target system. Generation, transmission, and distribution subsystems comprise an electric power supply system, for example. The failure of any target subsystem results in degradation, perhaps even failure, of the purpose of the target system. Inability to distribute electricity due to the destruction of electrical lines and substations negates the purpose of the larger electric power supply system. Some subsystems are more fragile or

---

[65] This discussion of target analysis is a modification of, but adapted from *Joint Special Operations Targeting and Mission Planning Procedures*, Joint Pub 3-05.5 (Washington, D.C.: Chairman of the Joint Chiefs of Staff, 10 August 1993), pp. II-5 thru II-12.

[66] US Department of Energy Fact Sheet, *DoE: Fossil Energy* (Washington, DC: 29 April 1997), p. 1. Document at http://www.fe.doe.gov/techline/tl_sprfr.html.

vulnerable than others, and thus may lie on a critical path to designing attacks against the larger target system.

A target complex is defined geographically or in other dimensions, and is an integrated concentration of related facilities or activities. An electric generating plant facility is a physical target complex, on which may exist components of the generation, transmission, and distribution subsystems. An example of a target complex in cyberspace is a collective, virtual workspace where interaction occurs. Modern stock exchanges are no longer exclusively located in physical space, like the physical Wall Street, but actually now exist in the fourth and fifth dimensions of time and cyberspace. Participants in stock exchanges may physically occupy office space and work on Wall Street, but they could as easily, perhaps even more efficiently, participate in the stock market through telecommuting in cyberspace from another physical space. Disruption of a stock exchange need not involve physical attack against a building anymore than disruption of the electric supply necessitates a physical attack against a power plant. The increased anchoring of the first three dimensions of physical space aspects, like wealth or control of an infrastructure's processes, in the fifth dimension of cyberspace increases vulnerability.

Target components are smaller elements within a target subsystem that are necessary to the operation of the subsystem. A turbine-generator hall is a target component within the generation subsystem of the electric power supply system. Attacking this component can occur in either physical space or cyberspace.

Target components can be further subdivided by criticality and vulnerability. A critical node is that part of a target component that is vital to the functioning of the target component. The cooling system for a turbine-generator hall is vital to the operation of the machinery. Failure of the cooling system will result in overheating of the turbines, which will destroy the machinery. A vulnerable node is the most vulnerable component of a critical node. A key sensor array that regulates coolant levels and temperatures within the cooling system is an example of a vulnerable component.

Target Analysis Hierarchy and Examples	
Critical System	**Energy Supply**
Target System	**Electric Power Supply System**
Target Subsystem	**Generation subsystem**
Target Component	**Turbine-generator hall**
Critical Node	**Cooling System for Turbines**
Vulnerable Node	**Key sensor array monitoring coolant levels**

Table 3 – 2: Target Analysis Hierarchy and Examples

This defined hierarchy is contingent on several factors. Not every Other will possess infrastructures that can be strictly modeled with the above definitions. Some Others may be relatively independent of technological systems; the water supply for guerrillas may be simply rivers. Additionally, an Other may exist embedded within Self's infrastructures, dependent on Self's electrical and other systems for its own support. Urban-based terrorists use and benefit from the same electrical, transportation, and other infrastructures as the government they attack. Highly-advanced Others may have no significant dependence, hence vulnerability, on physical infrastructures to act in the role of threat. A threat actor operating in cyberspace is only reliant, and that at miniscule levels, on electric power and telecommunications infrastructures, both of which may be based abroad in any event. A First Image actor has limited need for physical infrastructure, and if existing within Self's physical space and population in parasitic fashion may be immune to an attack on physical infrastructure unless very precisely targeted.

Targeting emerging threats entails determining the conductive medium (media) within which they can be engaged. The Other, however, can conduct analysis of Self's infrastructures at will. Critical infrastructures within the United States are completely vulnerable to attack. The distributed nature of the infrastructures simply is too vast to shield anything but the most vulnerable, highest-value, geographically integrated sites. Not every vulnerability, however, is significant. Cutting power lines in a remote area yields only nuisance value; the electric grid is designed with redundancy and has alternate paths to distribute electricity; the repair of damage is measured, at most, in days. Disruption of electricity is difficult through a tactical-level, wire-cutting campaign.

Other will choose targets within its capabilities to affect, which yield results supportive of its ends, in accordance with its *modus operandi*. Other will do so using a target analysis methodology that indicates which of Self's vulnerabilities meets its targeting criteria. If strategic effect is desired, a tactical attack on wire lines is not effective unless on a huge scale and simultaneously executed.

A methodology for targeting within security policy and military planning circles is CARVER.[67] The acronym CARVER stands for Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability.

Criticality, or importance, is determined by both Blue and Red perspectives. A target viewed as unimportant by both Blue and Red is not critical, although its status may change over time. From a

[67] Joint Pub 3-05.5, pp. II-8 through II-10.

Red perspective, a target is critical if it is key to accomplishing an objective, or of overriding symbolic value. A target is critical from a Blue perspective if it is essential to the operations and interests of Self. Where both Red and Blue view a target as critical, it will be a probable location of conflict. Analysis of possible targets must be conducted by Self and Other from both a Blue and a Red perspective. Where Red's *modus operandi* is to select targets based on perceived value from a Blue perspective, Blue, assuming it recognizes this target selection criteria of Red, will be able to anticipate potential targets and take action to protect them. However, an unknown Other may have a Red perspective that is unfamiliar to Self. Because of this, targets assessed as unimportant by Self from both a Blue and Red perspective may nevertheless be attacked by an unknown Other.

Criticality is always assessed from the perspective of a desired end. From Blue's perspective, the criticality of a policy or system may be to ensure the uninterrupted provision of electrical power or another critical infrastructure. Criticality is not assessed from a perspective that is isolated from an end.

Both Blue and Red determine how accessible is a target. In order to attack a target, Other must have the means of reaching it either directly or indirectly. Self can increase the difficulty of accessibility by hardening targets it identifies as critical from either a Red or Blue perspective. Accessibility can also be reduced through preventive measures taken to deny Other the means to effectively engage the target. Finally, Blue may choose to preempt Red's capability of accessing a target. The three methods of denying access are defending against, preventing, and preempting Red's capability.

Blue determines how recuperable is a target. The targeting criterion of recuperability is a constitutive element of the criterion of criticality. If a target can be easily repaired, replaced, or bypassed in a short time with modest expense, it is highly recuperable and therefore a poor target choice. A critical target can, in actual effect, be made non-critical by investing in capabilities to repair, replace, or bypass the target. Targets that otherwise would be critical if not supplemented with redundant backups can be made relatively unattractive as targets through intelligent design and resourcing that prevents a single-point failure, or single critical node, in a system. Although highly necessary for the operation of a system, if a target is also highly recuperable, it is not, in effect, truly critical.

Both Blue and Red determine how vulnerable is a target. The capabilities and intent of Red determine a target's vulnerability, while Blue's precautionary measures (defensive, preventive, and

preemptive) also influence the degree of vulnerability to Red's capabilities and intent. A target that Red does not have the means to attack is not vulnerable. Additionally, should Red possess no intent to attack a target, perhaps due to cultural considerations, its irrelevance to objectives sought, or Red's own dependence, future or current, on the operational status of the target, it is not vulnerable.

The effect of attacking a target is determined by Red, Blue, and potentially Gray. Considerations of effects include political, economic, legal, social-psychological, and military ramifications. A target that would have significant ramifications for Gray actors, such as a major stock exchange, must be considered from many perspectives before targeting. Likewise, targets that would adversely affect population health and welfare may support subsequent information operations that ultimately negate any advantage gained by Red attacking them. Target effects must be calculated and weighed beyond the immediate scope of attack. This calculation must extend beyond the initial effects to include potential second- and third-order effects. In analysis of complex systems this is a challenge, but necessary to preclude negative effects that can be identified.

Blue determines the recognizability of a target. Camouflage, deception, and operations security measures can render a target incapable of being identified, hence targeted. A detailed treatment of recognizability is treated in the Cyberspace Personas and Identity Masks section below.

The timing of targeting of critical infrastructures is an important consideration. A detailed analysis of timing of attack is addressed later, but an initial treatment is appropriate here. Targeting systems entails analysis of when to attack. Some systems may be (in)vulnerable based on windows of time, with attacks mounted outside the window having no or little effect. Additionally, some systems are optimally targeted at specific times, such as an electric power supply system at peak load. This factor is a time-variable payoff, which operates in the fourth dimension of conflict. High demand placed on a time-variable payoff system, like the electric power supply, may tighten intersystemic couplings, open parallel pathways through which effects can cascade, and increase the velocity of effects throughout the system. High demand also may reduce system robustness, redundancy, recuperability, reparability, and resiliency as well as make the targeting criteria contained in CARVER more favorable for attacking. Detailed analysis of effects through the fourth dimension is critical to understanding the scope of an attack's impact.

Targets may be further delineated in time by designating some as initial targets. Initial targets are targets that must be struck at the outset of an attack to enable subsequent targeting of higher-payoff targets, or because failure to target them immediately will result in the loss of ability to target them, or

they may serve a preemptive purpose which if not exercised early results in a lost opportunity. Also, staggering of attacks in time may allow the effects of subsequent targeting to become more effective, due to intrasystemic processes that increase the value or effect of attacking a specific target subsequent to an initial array of targets. There are many other considerations of the timing of attack, but these serve to illustrate how targeting critical infrastructure extends beyond the three dimensions of physical space.

Cyberspace Personas and Identity Masks:

Deception is as old as war. A technique of deception is concealing true identity. The techniques of concealing identity have changed, but principles have proven more durable. For example, the Trojan Horse employed by Ulysses to penetrate the walls of Troy has been replaced by trojan horse viruses designed to penetrate computer networks. The techniques and means differ according to situational context, but the principles are the same.

Concealing identity is accomplished by masking.[68] One purpose of masking can be to deny any perception by another actor of one's identity. This forestalls other actors' knowledge of one's existence, and allows covert operations through anonymity. A second purpose of masking is to create the appearance of being what one is actually not. The Trojan Horse appeared to be a gift, yet it was actually a weapon.

A relatively new aspect of creating "masks" is translating past principles of deception into the fifth dimension of cyberspace as techniques. Increasingly an actor, whether individual or collective, will have a presence in cyberspace. This presence is a representation of the actor – a mask or persona – that communicates to other actors the identity of the owner. In the case of a corporation, this mask communicates the capability to conduct business in all of its aspects from marketing to sales to logistics. In the case of an individual or group, this presence in cyberspace may consist of transactions regarding one's credit history, phone numbers and usage patterns, financial transactions, on-line purchases or other matters.

This presence is to some degree influenced by culture, socio-economic factors, and even geographic location. At the time of this writing, a citizen of an advanced industrialized society is more likely to have a cyber-presence than a citizen of a non-industrialized, nomadic society. This is, however, not a hard and fast law of nature, as advances in wireless communications and satellites have made technologically feasible the access of cyberspace from the most remote locations on earth. In the

[68] Peter Andrews, *Electronic Identities: Secure Masks*, IBM Executive Tek Report, 14 August 2000. Document at http://www.ibm.com/services/innovation/ltrelectronic_ids.pdf.

near future continued diffusion of technology may result in the proliferation and establishment of cyberspace as a "dense" medium globally, with ubiquitous personal, cyberspace access devices possessed by individuals. The proliferation of wireless telephones capable of accessing cyberspace suggests the continued proliferation of individual cyberspace access globally. As this proliferation of access advances techniques of creating "masks" in the fifth dimension likely will also grow and evidence cultural, economic, geographic, even fashion and other varieties.

An actor without a presence in cyberspace could be an aberration showing a high-degree of isolation from the fifth dimension, or an actor that has taken active measures to erase its presence and so protect itself from detection. In the first case, an actor completely isolated from the fifth dimension cannot – directly – engage or be engaged through this dimension's conductive medium. The second case is interesting, however, because a stealth actor can engage an adversary through the conductive medium of cyberspace, but may not be vulnerable to retaliation.

An anonymous actor employing a secure digital mask enjoys freedom of the fifth dimension, but is virtually invisible to others within the medium because of its active efforts to cloak its existence. This case is roughly analogous to a submarine's ability to move in the sea, without being apparent to vacationing observers on a cruise ship. Without specialized sensors and techniques, the submarine is unnoticed.

The case of impersonating another actor is different. Here the efforts are not to erase the digital signature of one's activity and presence in the fifth dimension and operate as a stealth actor, but to portray a different actor. Extending the analogy, this would correspond to pirates flying a false flag to come alongside the cruise ship.

Creating a mask depends on the purpose desired of the mask. In the case where stealth is desired, the purpose of the mask is to confer "invisibility" and it will be created using tools, techniques, and tests to ensure the actor remains covert. Means to accomplish this purpose are dynamic, constantly evolving objects, dependent on the deep and shallow structure of the fifth dimension. As used in this study deep structure includes the fundamental architecture, systems, and constitutive "wares" (hardware, firmware, protocol standards) of the conductive medium - cyberspace - itself. Shallow structure resides near other actors, with firewalls and password protected intranets being examples of shallow structures that do not pervade the entire fifth dimension. Interaction between actors in cyberspace occurs in the shallow structure. Deep structure constitutes cyberspace itself as a dimension, and masks can be transmitted through the deep structure, but it is in the shallow structure of cyberspace that masks are created, maintained, sensed by other actors, and work effects into the sixth dimension.

To remain completely covert in cyberspace an actor must take measures to remain undetectable in both the shallow and the deep structure of cyberspace. The architecture of the hardware infrastructure must not provide evidence of an access portal, digital traces of activity must be destroyed or caused to "evaporate," and the operations of a stealth actor must be undetectable and unrecognizable to similar actors passively surveilling the deep structure of cyberspace. A stealth actor requires a mask that serves as a shield deflecting observation. Even more challenging, this mask must not be able to be "sensed" by its effects on the structure of cyberspace itself. Much as the existence of an unknown celestial body, for instance a black hole, can be inferred from its gravitational pull on known aspects of the heavens, a stealth actor can be sensed indirectly by its use of bandwidth or through other metrics. This suggests that the stealthiness of a mask is not a dichotomous variable, but a matter of degree.

Creation of masks involves creating objects both in cyberspace and other dimensions. A credit history may have been created in three-dimensional space, and as it displays a pattern over time includes a component of the fourth dimension, time, in its substantive content. When it is posted on a computer network, however, it gains "presence" in cyberspace, and by extension the individual subject of the credit report now has a cyberspace component to his identity. But it is also anchored in other dimensions, which increases its credibility. This multi-dimensional presence of persona, in turn, translates into the sixth dimension of perception. Continuing with the First Image example, the credit history is explicitly designed as a tool or metric to affect another's perception of a specific actor. In this case the perception influenced regards the trustworthiness of the individual. Trust and belief exists in the sixth dimension of perception.

The tools for creating a mask are varied.[69] Currently, the tools to create an individual's mask include telephone numbers in directories, a personal web page, a "my site" personalization of news organization web pages, membership on issue-specific e-lists, records of financial transactions with retailers and stockbrokers, and many other tools. The techniques involved are closely related to the tools employed, but there is a difference. It is the technique that actually populates the identity with substantive information. The generic tool of purchasing goods in cyberspace, for example, contributes to the establishment of an individual's mask. The technique of buying books from a major retailer in cyberspace, and the actual books purchased, informs other actors to some degree of the substantive nature of the individual, or what the mask "looks" like. In other words, the tool of purchasing establishes the cyber presence of an individual, but the technique employed establishes the type of individual mask or persona created.

---

[69] Andrews, *Electronic Identities: Secure Masks*, p. 2.

The above example has dealt with the individual as the object of study. However, the tools and techniques of establishing a mask apply *a fortiori* to higher-level actors, not just in scale but also in depth and complexity. For example, should an intelligence organization need to establish the web persona of a global corporation, it involves a much more complex array of tools and techniques that must be employed to fabricate that cyber presence, or the mask. The cyber presence increasingly also must have anchors in the other dimensions to be credible to Others. For example, at the individual level even a teenager can establish a mask of an alternative identity in little time with few resources. This mask is not necessarily unsophisticated; even intelligent individuals can never be sure with whom they are interfacing in cyberspace. But the demands of crafting a higher actor's mask in cyberspace are more extensive. A corporate presence in cyberspace is reinforced by a myriad of other interlaced objects in other dimensions, including the (working) phone numbers and (real) addresses of home offices, the names of employees, even formal corporate filings with official government institutions. At this level of sophistication, however, the constructed mask of an actor in cyberspace easily enters the sixth dimension of perception as a believed construct and this crossing of the threshold of belief enables a scale of activities denied to an individual, or First Image, mask. One example of a complex mask constituting a national security threat is the global laundering of terrorist and drug cartel finances through fictious off-shore banking entities.[70]

Testing is the third component active in establishing a mask's validity. In the individual case, details are confirmed by those actors with an interest in establishing the validity of the mask. Research is conducted that corroborates or denies what the mask presents to them. At the individual level, these tests can take the form of confirming type and length of previous employment, after first evaluating a credit history. In the corporate example, the tests could include preliminary exchange of correspondence by investigative departments within government agencies.

The testing involved in establishing a mask's validity is contributed by both the actor whom the mask represents as it ensures its viability during construction, as well as unwittingly by the actors who take measures to assess its validity. For example, in forming a database of organizations, a government agency creates an object that corresponds to an actor within that database. This act alone potentially further reinforces the mask of the actor being investigated, by using the data it initially has

[70] The US Department of Justice has published a strategic plan to combat money laundering as a national security issue. These illicit financial markets are extensive. One of the most important from a national security perspective is the Black Market Peso Exchange (BMPE). The BMPE is the "primary money laundering system used by Colombian narcotics traffickers." It channels approximately $ 5 billion dollars annually out of the United States into the drug cartels' leaders hands annually. Quote from *The National Money Laundering Strategy for 2000* (Washington, DC: US Department of Justice, March 2000), p. 24.

gathered as a starting point for understanding the actor. Until a reason exists to suspect the mask as false, the very existence of an entry corresponding to the actor's mask in an official government database serves to corroborate the actor's existence to that and other agencies. Each test the actor's mask withstands increases the validity of the mask for both those conducting and later observing the testing results, and decreases the likelihood that the mask will be perceived as incongruent with the actor's actual identity. This becomes a self-reinforcing cycle, and in the case of a First Image mask requires little anchoring in physical space.

An example serves to illustrate how a false mask can become viewed as a truthful representation of the first five dimensions in the sixth dimension. Increasingly scholars participate in highly specialized discussion forums based in cyberspace. Some of these discussions involve exchanging thoughts, even papers, on critical scientific topics. This type of community, especially when involved in critical sectors of technology, is a rich, inviting target for intelligence collection. In this case, either type of mask can serve to gain information on a critical technology from a select group of research scientists communicating in cyberspace. The stealth actor mask can monitor the digital correspondence of all the participants. This minimizes vulnerability to discovery or suspicion, but surrenders any chance of influencing the direction of the correspondence by asking questions or making contributions.

Alternatively, a false overt mask can be created to infiltrate the community. Participation will require contribution. However, this can be useful not only for establishing credibility and building rapport, but also for subtly steering the group into discussion of relevant intelligence collection priorities. Most intelligence agencies can easily support a false mask with the level of expertise to gain and maintain credible standing in a community, even to the extent of publishing under the false mask's *nom de plume* in some minor publications. Using this technique, it would not be desirable to portray the mask as a leading figure in the discipline. Disciplines know their leading scholars personally. But portraying a motivated graduate student interested in a research science topic may be sufficient. This technique may not capture cutting edge research from a targeted academic circle, but just gaining access to a draft "gray literature" article concerning critical technology six months before it appears in a professional journal constitutes an intelligence victory, especially when it concerns sensitive technologies. Even the knowledge of who and which institutions are conducting different types of research is itself useful.

The concept of creating deceptive images is not new. What is new is the extent to which establishment of a mask has been made easier, the scale of deception the mask can exert, and the cyberspace dimension within which the mask can be wielded as a weapon. Before the Internet, an

actor engaged in corporate deception and economic espionage had to possess a significant presence in physical space. This was not only a resource requirement, but also increased the vulnerability of the actor. This requirement of presence in physical space has been lessened by the Internet's support for cyberspace presence as a physical space substitute. This ersatz nature of cyberspace confers advantages of lower resource requirements, expanded capability to assume different personas, ease of transnational communications and operations, mounting large-scale operations from a central, controlling operational base, employing multiple, distributed "front" masks, and reduced vulnerability. Phones, mailing addresses, and other anchors of the mask in other dimensions must still exist, but the facilities in physical space need not be as represented in cyberspace. Beautiful photos of a corporate campus gracing a purported multinational business' home page need have no corresponding physical reality; because they exist in the fifth dimension, they potentially exist as "reality" in the sixth dimension. A candid, dorm room photo of a smiling graduate student "interested in superconductors" as his dissertation's topic need have no corresponding physical reality; but as it exists in the fifth dimension, it potentially exists in the sixth dimension.

Masks can be created to either cloak a covert actor's existence, or to overtly deceive as to one's true identity. Tools, techniques and testing create masks. Credible masks are anchored in the four dimensions of physical space and time, exist in the fifth dimension of cyberspace, but conduct their activity and seek their effects in the sixth dimension of perception. Creating masks requires few resources, allows large-scale operations employing multiple masks, transcends political boundaries, facilitates centralized control, and reduces vulnerability and risk. Masks are potent tools for non-state actors, because states do not necessarily possess an inherent advantage despite their material and other sources of power. Non-state actors adept at employing masks can challenge states asymmetrically, asynchronously, and even anonymously.

A Typology of Self:

Defining Blue as "Self" is a useful convention for communicating the conceptual topography of the Red, Gray, and Blue framework. At the strategic level it is a useful anthropomorphism. As discussion leaves the realm of theory and enters the realm of a specific security policy field, however, it is necessary to more specifically define what constitutes Blue. The task is no longer to communicate a general, overarching framework, but to describe and explain with some degree of specificity a type of Self at the lower level of abstraction that typifies a model.

A typology of Self, to be useful, must serve as a guide for policymakers to order the forces, tools, vulnerabilities, and interests of relevant stakeholders within the Blue camp. At the framework level the state or a systemic-level non-state actor is "Blue." At the level of model, Blue loses this

coarse-grained resolution, and multiplies into a community of endogenous, constitutive sub-actors. Ordering these constitutive elements of the larger systemic-level actor explicates relationships, capabilities, interests, and other traits that suggest policy-relevant solutions to the challenges posited by emerging threats. As a depiction of reality, Blue in a model of the policy process becomes an "issue network" or a "policy system." Without critical self-assessment of this issue network, a coherent strategy cannot be crafted. Analysis of Blue is as necessary as understanding the environment in which one operates (Gray), and the threat one faces (Red). For example, for policy purposes it is functionally inadequate to refer to Blue's electrical sector. Instead, the constitutive sub-actors that actually comprise both the public and private portions of the electrical sector's issue network must be identified at a finer level of resolution.

This flexibility in the concept of Blue is based on the levels of conflict, the levels of analysis, and the use to which the framework is employed. At the strategic level Blue is paradigmatic, at the operational level Blue symbolizes the Self as an element of a specific model, and at the tactical level Blue may be a First Image actor, small group, or a single corporation involved in conflict with a particular Red in a specific case. Viewed introspectively, Self may be comprised of multiple actors. However, when viewed from an exogenous point of view, Blue is a unitary actor in its interactions with Red and Gray. The below table details the approximate correspondence. Of course, the relationship is only roughly illustrative. Nothing militates against even a very small, but intelligently targeted, strike against a single critical node in an infrastructure from having catastrophic, strategic consequences. In fact, it is this easy translation across all levels that allows employment of the Red, Gray, and Blue framework to usefully describe, explain, and potentially provide weak prediction across all levels.

Strategic	State or systemic-level non-state actor	Paradigm
Operational	Issue Network	Model
Tactical	Individual / Agency / Corporation	Case

Table 3-3: Meanings of Blue

A typology of Self is detailed in Table 3-4. Like the typology of threat, it is not exhaustive and can be expanded and refined to model a particular case. For the purpose of this study, Self is the issue network of actors concerned with protecting US critical infrastructures and population.[71] This issue network contains within it many actors, both government agencies and private organizations.

The actors interested in critical infrastructure protection bring a diverse set of concerns, means and ends to the issue. What unites them into a policy community is a common interest in a

[71] True, Jones, and Baumgartner, p. 99.

reliable critical infrastructure. The critical infrastructure protection policy system includes what could be termed a "legacy" policy subsystem rooted in the Cold War – the traditional US defense and national security community and its ancillary actors. However, the CIP policy system incorporates new actors, and relies on private entities to a degree not seen during the past security era.

Unlike the legacy Defense community, which was founded on a federal infrastructure and provided a common pool service – national security understood as the pursuit of policy overseas through the instrument of military power – the CIP community is radically different. The overwhelming majority of US critical infrastructures are privately owned and managed. Recalling the arrow-diagrammed construction of the theory, emerging threats now possess WME capable of striking US critical infrastructure and population within the United States. This effectively removes any advantage conferred by America's traditional geographic sources of homeland security from attack, its oceans and absence of threat neighbors, and simultaneously reduces the risks to threats inherent in attacking the United States. Additionally, the threat means and methods employed in attacking necessarily involve US private industry, especially in critical infrastructure sectors, to an unprecedented degree. The frontlines of America's defenses are its private corporations that manage critical infrastructures. In a figurative sense, the Fulda Gap has been replaced by Indiantown Gap as the first battlefield of a future war.

This has resulted in the recent formation, in accordance with PDD 63, of Information Sharing and Analysis Centers (ISAC).[72] ISACs are information clearinghouses, aligned with critical infrastructures, which provide both private and public actors the means to share information on threats, vulnerabilities, incidents, and solutions.[73] An ISAC accomplishes this through a secure database that includes analytic tools, information gathering and distribution facilities, as well as personnel with expert knowledge of the infrastructure and the threats. This results in early notification of participants of relevant information concerning the infrastructure's protection. ISACs also compile trending, metrics, and benchmark data which are then analyzed and distributed to members.

The voluntary participation of private corporations in an ISAC serves to partially define Blue as an issue network. Other members include US government agencies with stakes involved in the infrastructure, as well as interest groups and even concerned individuals capable of gaining access based on national security credentials. However, due to the national security charter of the ISACs,

---

[72] The first ISAC was the Financial Services ISAC (FS/ISAC) placed into operation on 1 October 1999. See *Statement by Treasury Secretary Lawrence H. Summers on Financial Services Information Sharing and Analysis Center*, US Treasury Department Press Release LS-135 (Washington, DC: US Department of the Treasury Office of Public Affairs, 1 October 1999).

private interest groups are constrained in gaining access by the legitimacy and credibility they can claim in a national security policy arena. Private actors outside of the infrastructure are not viewed as stakeholders until they meet a higher level test than they may be customarily subjected to in gaining access to venues not associated with national security. For example, an environmental movement actor may be able to gain access to a congressional committee hearing on a particular industry by exercising the right of public access. However, when the issue concerns the same industry, but in the ISAC venue of national security, the environmental actor may be excluded.

Because of this the resulting issue network is a hybrid mixture of the legacy national security network's emphasis on secrecy and the exclusion of actors not directly involved in the policy formulation and decision making process, and the openness and accountability to shareholders and other groups inherent in a publicly-traded corporation. The ISACs make explicit an institutional venue within which collaboration in the issue network occurs. As Baumgartner and Jones note the "institutional venue is home to a different image of the same [policy] question."[74] Private corporations answering only to shareholders concerning profitability will view the same question differently when it becomes a national security concern, they are participants in a closed policy community, and are receiving and sharing information concerning threats. Inevitably, this unprecedented combination of both public and private actors in an issue network concerning national security has resulted in government and industry both operating out of familiar comfort zones. The ISAC's middle ground is where industry recognizes the need for sharing sometimes proprietary, sensitive information and government recognizes the need to safeguard it from further dissemination that would harm a corporation's interests in profitability and competitiveness. The inability to reconcile this tension contributed to the blocking of access and exclusion of government actors from the sensitive financial services ISAC. The director of security for Fidelity Investments has stated that "In our early efforts to structure information sharing venues, many of us have agreed to share anonymously among ourselves but have elected to withhold from government," and "We simply do not know what politically motivated interests might do with the information."[75]

The unique aspects of the hybrid issue network and the novelty of the venue significantly defines Self in a given model. The electrical sector Self will be different from the financial services Self. The issue network shares a communication network that is also unique, and which serves as

---

[73] The Financial Services ISAC (FS/ISAC) does not include a US government agency as a member, nor can any USG agency access the FS/ISAC.
[74] Baumgartner and Jones, p. 31.
[75] George K. Campbell, "Security Expectations for Transnational Corporations," in Max G. Manwaring, ed., *...to insure domestic Tranquility, provide for the common defence...* (Carlisle, PA: Strategic Studies Institute, October 2000), pp. 75-84. Quotes from page 81.

another constitutive element. The National Information Infrastructure (NII) can be understood to be the communications network of Blue at the paradigmatic level. However, as the discussion of the ISACs illustrates, the Force Information Infrastructure (FII), or the communications network of a particular issue network concerned with protecting a specific infrastructure, is unique to that policy community. The recipients and contributors of information to the FII are in part included in the issue network because they communicate with the issue network members through this shared FII.

Identity	Means	Vulnerabilities	Interests
Private Corporation (Infrastructure)	Rules, Regulations, Laws, Orders	Complex Systems	National Security Advantage
Private Corporation (Non-infrastructure)	Force	Critical Infrastructures	Financial Gain
Law Enforcement Community	Research & Development Programs	Population	Political Influence
Military	Public Infrastructure Protection System	Cross-Actor Reporting and Interstices	Political Change
Intelligence Community	Private Infrastructure Protection System	Knowledge Warehouses	Safeguard WME
Academia	Expert Skills & Knowledge		Survival
Consultants	Consequence Management Teams		Deter
Critical Infrastructure Regulatory Agents	Education & Training		Neutralize a Threat
Emergency Services	Intelligence Assets		Economic Advantage
Executive Branch	Encryption		Retaliation
Judicial Branch	Products		Altruism
Legislative Branch	Services		Maintain Civil Order
			Limit Exposure & Liability

Table 3-4: A Typology of Self

Defining Threat:

In a classic article on threat perception written early in the Cold War, J. David Singer defined a threat as a capability coupled with intent to harm.[76] He explicitly defined a term he thought was used too loosely in vital security debates at that critical time. His definition remains a basic point of instruction for participants in the national security policy field.

Arguably, other components also constitute the identity of threat. For instance, opportunity and vulnerability may be prerequisites to the constitution of a threat. This begs the question of whether these are aspects of the actor viewed as a threat, however. Environmental conditions can confer

[76] J. David Singer, "Threat-perception and the armament-tension dilemma," *Journal of Conflict Resolution*, Vol. II, No. I (March 1958), p. 94.

opportuntity, as can Blue actions. Vulnerability is rooted in Blue's aspects and Red's capabilities. For example, opportunity to cause harm may be dependent on proximity in physical space. Either Red, Blue, or Gray's aspects can influence the proximity of two actors in space, however. Vulnerability itself begs the question "vulnerable to what means?" This necessarily incorporates aspects of Blue juxtaposed to Red's capabilities.

The criteria of intent and capability, where capability is understood as a command of means, are both exclusively rooted in Red's aspects. Singer's definition reduces complexity by anchoring the constitution of threat firmly in Red's aspects.

This does not mean that Blue or Gray aspects are unimportant. The analysis of capabilities and intent, difficult as it is, would be made more complex and challenging if weighing in changing aspects of Blue and Gray across time would be necessary to constitute a threat identity. In pragmatic terms, Singer's definition is functionally adequate, and although consideration of both Gray and Blue aspects are necessary to comprehend the potential effects resulting from a threat actor's possible activity, they are neither necessary nor sufficient to constitute a threat identity. The coupling of capability and intent are sufficient conditions to constitute a threat identity; whether that identity acts or, if acting, succeeds, is due to many variables. However, these exogenous variables differ from case to case, and are not constitutive elements of threat, but of a specific case's conditions.

The Metaphor of the Realm of Cerberus:

Metaphors, like other images, can be loaded with implicit meanings. The meaning packed into a metaphor depends on several factors. One factor is cultural perspective. For example, the battle of Dien Bien Phu if used as a metaphor to characterize a potential, future struggle could connote for a Vietnamese an ultimate triumph over a technologically superior foe, achieved through cunning, discipline, and perseverance. The same metaphor interpreted through a French or an American cultural lens could connote a disastrous, humiliating end to a failed strategy supporting a lost cause.[77] Metaphors suggest to an audience a situation's nature, and can be used to define the situation, specify roles and strategies, and justify action.[78] But metaphors can be misleading or misunderstood, and when rigorously examined may fail to prove valid beyond a superficial level. Neustadt and May caution that analogies, like metaphors and similes, are potentially dangerous cognitive tools for

[77] Vertzberger, pp. 302-303; Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton: Princeton University Press, 1992), p. 63.
[78] Vertzberger, *The World in Their Minds*, p. 298.

policymakers to employ, stating that "invoking them often substitutes for thinking hard about things as they are."[79]

Nevertheless, it can be useful to employ metaphor to illustrate a point. A security environment approach to National Security Policy Decisionmaking (NSPD) portrays the security policy decisionmaker as Cerberus, the three-headed beast that guards the gates of Hades in Greek mythology and prevents the escape of terrors from the underworld. The metaphor is fitting for the Red, Gray, and Blue model, where policymakers and strategists must be informed of not only Other, but also the environment and Self. Applying the metaphor to the Red, Gray, and Blue framework, a policymaker must study the three components of the security environment, Self, Threat, and the environment, to prevent harm to security interests. Without adequate analysis of the three components, security policy is possibly flawed in its design, and unable to protect or further interests.

Within the Realm of Cerberus leadership, deterrence, and other activities take place. Even absent any interaction or communication between Blue and Red other than conflict, that language of conflict is understood by the decisionmaker(s) operating in the Realm of Cerberus. Their understanding of Self, Other, and environment constitutes the case-specific context within which security policy is planned and implemented. National security elites must emulate Cerberus and regard three different entities simultaneously.

Stalker:

As modeled, the Red, Gray and Blue framework is an abstract depiction of reality. This model can be made to more accurately describe the relationships that potentially exist between actors within an environment. The Stalker model, comprised of seven possible worlds of relationships or variants, is a finer-grained resolution of the more abstract Red, Gray, and Blue framework. The seven variants represent the possible permutations of relationships between Blue, Red, Green, Yellow, and Gray actors. In the variants, Blue and Red represent Self and Threat, respectively. Green represents a neutral actor, Yellow represents a threat actor other than Red, and Gray represents either an unknown actor or actor of unknown intentions.

The Stalker models have seven plateaus. The first plateau is defined as the Status Quo. In this plateau Red does begin to prepare an attack against Blue, and the existing status quo is maintained. In the second plateau, Hold Reconnaissance and Continue Preparation, Red initiates a preparatory

---

[79] Richard E. Neustadt, and Ernest R. May, *Thinking in Time: The Uses of History for Decision Makers* (New York: Free Press, 1986), p. 89.

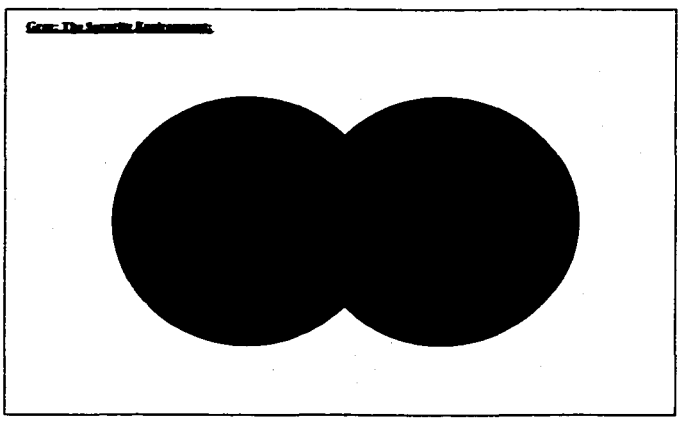
stage for attack, but does not begin reconnaissance. In the third plateau, Hold Strike and Continue Preparation and Reconnaissance, Red is conducting preparatory and reconnaissance tasks but has not yet launched a strike. In the fourth plateau, Undetected Strike, Red's strike is not perceived in the sixth dimension by Blue. In the fifth plateau, Unresponsive Target, Blue has perceived Red's strike, but has elected to not respond. In the sixth plateau, Defensive Target, Blue limits its response to Red's strike to strictly defensive measures. In the seventh plateau, Ineffective Retaliation, Blue has conducted offensive retaliatory operations unsuccessfully. The plateaus are addressed in detail in chapter four.

The Stalker variants serve as the foundation for the development of conflict decision trees in the form of graphical networks, examined in chapter four. These decision trees model a game theoretical design of an anonymous, asymmetric, and asynchronous threat actor's attack of a state actor's population and critical infrastructure. From Stalker's variants strategists and policymakers can design even finer-grained, case-specific models to describe, explain, and provide weak prediction of a particular conflict.

The seven variants of Stalker are:

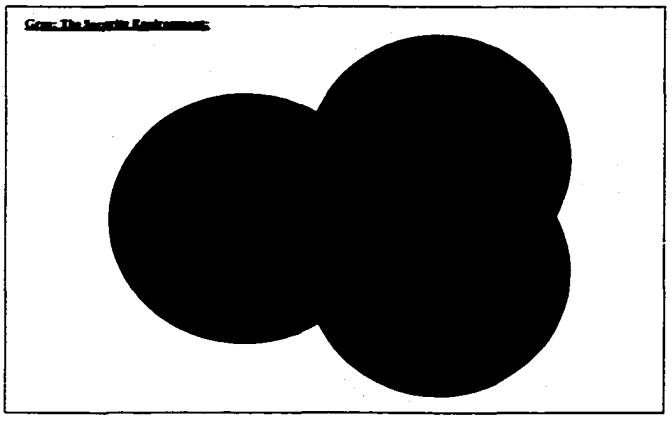
1. Simple Conflict: The simple conflict model consists of exactly two actors, Blue and Red.

Stalker: Simple Conflict
Variant I



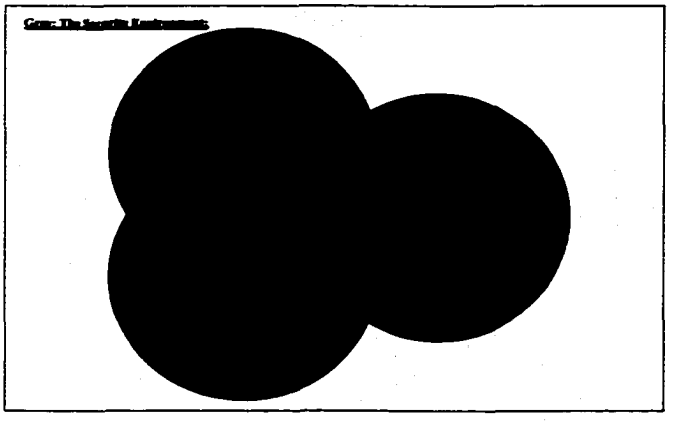
2. Ganging Up on Blue: This model consists of at least three actors. Red actors have a unified purpose in attacking Blue.

Stalker: Ganging Up on Blue
Variant 2



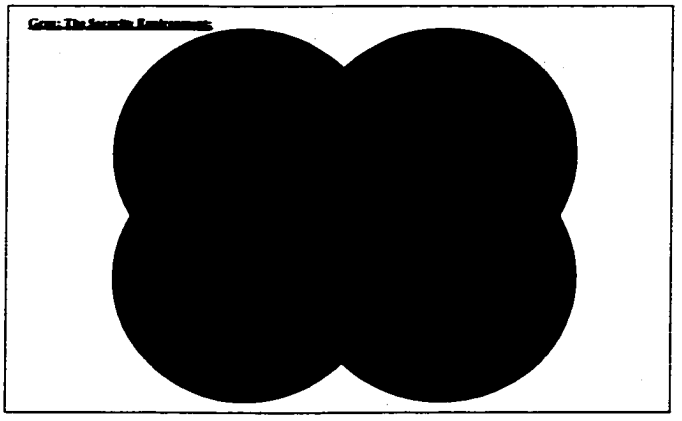
3. Ganging Up on Red: This model also consists of at least three actors. The Blue actors are attacking Red with a unified purpose.

Stalker: Ganging Up on Red
Variant 3



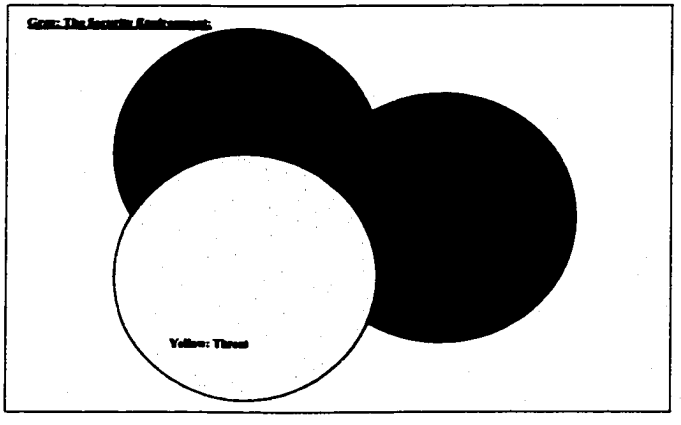
4. Alliances: In this variant, there exist at least four actors involved in conflict, with two alliances. Both alliances consist of members acting with a common purpose.

Stalker: Alliances
Variant 4



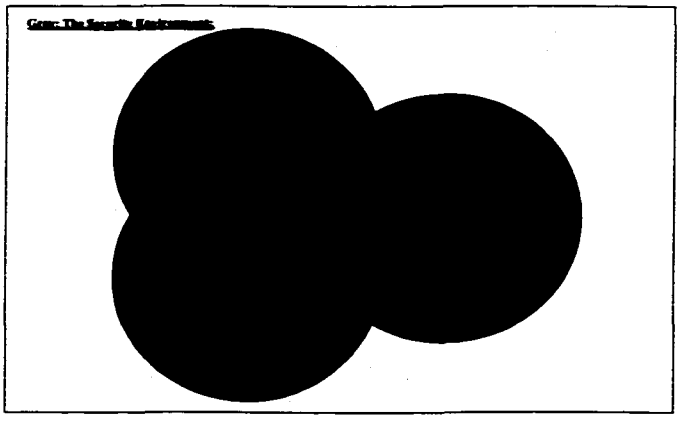
5. Factions: This variant is constituted of at least three actors, none of whom have a common purpose. Given a world typified by Factions, Blue has a hierarchical order of preference for its actions. This order of preference is: a. Ally with Yellow, resulting in the variant world "Gang Up on Red"; b. Negotiate Yellow to Gray, resulting in the variant world of fighting Red in "Simple Conflict"; c. Negotiate Yellow to Green, yielding a "Mixed Game" world; and, lastly, d. Factions, with at least three actors locked in conflict without common ends. Within the Factions variant, there is a sub-hierarchy of desired worlds from Blue's perspective: a. Two Against Red, with simultaneous efforts by Blue to negotiate Yellow to move to a Ganging Up on Red world; b. All Against All, with Blue employing Third Actor Escalation (TAE) to attempt movement of either actor to negotiate peace with Blue; and, c. Two Against Blue (but not allied against Blue), with Blue again employing TAE to incite conflict between Yellow and Red, or move to a world of All Against All. Failing these efforts, Blue will be engaged in two simultaneous games of "Simple Conflict" absent a Yellow – Red dyad.

Stalker: Factions
Variant 5



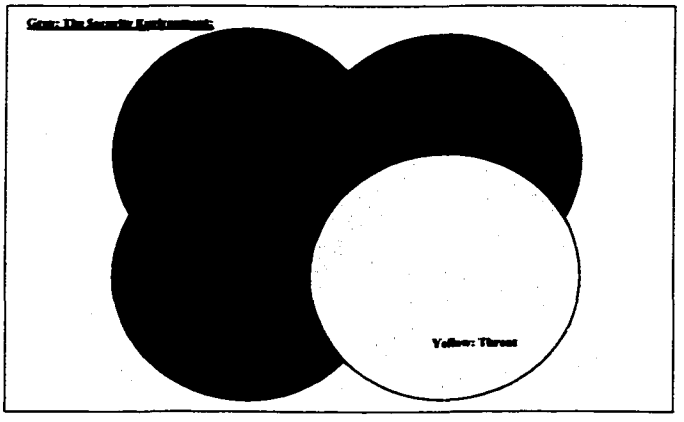
6. Mixed Game: This variant has at least three actors, Blue, Red, and Green (neutral) in the model's design. Green's involvement is as an active observer of Red and Blue, while continuously weighing strategic decisions concerning its neutrality and options for active involvement in the conflict.

Stalker: Mixed Game
Variant 6



7. N-Actor: This model involves at least four actors: Blue, Red, Green, and Yellow (a threat to Blue, but unaligned with Red).

Stalker: N-Actor
Variant 7



The Stalker models are further explicated in chapter four in discussion of their decision trees. These seven possible worlds describe the permutations of a non-state actor's anonymous, asymmetric, and asynchronous attack of a state actor's population and critical infrastructure. As such, they represent all possible permutations, with the stated numbers of actors involved in each world constituting the minimum number. For example, Ganging Up on Blue may entail more than two Red actors acting in concert, and Factions may involve more than a Red and a Yellow Actor opposing Blue.

In cases where the structure of the conflict resembles one of the seven variants, but differs in actual number of actors, the Stalker variant can be modified to account for varying numbers through the inclusion of another decision tree "branch" without changing the essential nature of the conflict modeled. It is irrelevant how many Red actors actually oppose Blue in the Ganging Up on Blue world; the model and decision tree defines the minimum number of actors in that type of world, and details the fundamental structure of the decisions taken in that type of conflict. Specific cases will modify these generic models to particular situations.

Conclusion

This chapter's epigraph asked "how do political leaders...approach the task of making calculations, of deciding what objectives to select, and how to deal with uncertainty and risk - that is, more generally, how to relate means and ends, etc.? What styles of political calculation and strategies are developed for this purpose by different leaders?"[80] The question deals with how political leaders fundamentally see their world. Before designating objectives and relating means and ends, policymakers must conceptually apprehend the security environment within which they operate. Past paradigms do not provide the US security elite with any conceptual framework for dealing with emerging threats, new US vulnerabilities, and WME employment.

This chapter has detailed a framework that policymakers can employ in formulating national security policies countering emerging threats targeting critical infrastructure and population with WME. It is applicable to all levels of conflict as well as different types of conflict and threats. It provides a paradigm that can replace the Cold War era's state-centric, bipolar framework for understanding the security environment.

The Red, Gray, and Blue framework is ontologically primitive and philosophical at its highest level of abstraction. Within this framework, seven models of more detailed resolution have been created that describe all possible permutations of actor relationships. From these models the security environment of an actor can be described and explained, and these worlds may to some extent inform weak prediction. These models "bridge the gap" George described as existing between theory and practice, and are relevant to current security challenges. The framework is internally consistent in its logic, and its models operate within its principles. The Red, Gray, and Blue framework provides a new paradigm to facilitate the ongoing transition of US national security policy formulation during the current Kuhnian paradigmatic crisis in understanding the United States' emerging security environment.

---

[80] George, "The 'Operational Code,'" p. 198.

Chapter four, A Typology of Emerging Threats and the Game of Stalker, details these models at a finer degree of resolution, developing graphical networks that characterize the seven variant's worlds of conflict. The chapter also explicates a typology of emerging threat actors in the altered security environment that can inform analysis of conflict in concretely defined terms of threat identities, means, targeting preferences, and ends.

Chapter Four: A Typology of Emerging Threats and the Game of Stalker

"Our first step must be to apprehend, and recognize for what it is, the nature of the movement with which we are dealing."[1]

Alexander George advocated that scholars and practitioners of national security policy "bridge the gap" between their worlds.[2] The concept has a long lineage, stretching back at least to Plato's Philosopher King who coupled thought with action in a single man. George's gap lies between the realm of theory and the world of practice. Bridging it requires tools that are informed by theory, but applicable to reality. Because theory is based on reality, or should be, tools applicable to reality and informed by theory can illuminate aspects of both. Often these tools, because they make explicit in their design theory's anchoring points in reality, thus illustrating their nature from two different perspectives, are more easily understood than discussion of either theory or reality alone.

The purpose of this chapter is to provide concepts, terms, and intellectual tools below the level of abstraction of paradigm, theory, and model. The intent is to continue this study's development of the security environment approach to national security policy by extending discussion of it to encompass a level of detail that can, following modification for context, be applied to specific cases. The development of these tools will further illustrate the security environment approach by showing how the discussion is coherent and integrated from paradigm to case, from the abstract to the specific, and from the strategic level to the tactical.

The chapter explicates a threat typology suitable for supporting text or data mining as an ontology, creates a game, and details seven different scenarios of threat attack. These terms, concepts, and models are not only tools, they also serve to holistically fill out and reinforce the study's structure and coherency across levels, thus enhancing the power of the security environment approach. Additionally, they also contribute to bridging George's gap by providing practitioners with tools applicable to the altered reality and informed by theory that is relevant to the new security environment.

The emerging threat typology is a radical departure from Cold War era typologies based in a state-centric approach. The typology posits several non-state actor identities, or identities a state actor

---

[1] George F. Kennan, "Telegram from the Chargé in the Soviet Union (Kennan) to the Secretary of State," transcribed from *Foreign Relations of the United States, 1946, vol. VI: Eastern Europe, The Soviet Union*, Department of State publication 8470 (Washington, DC: Government Printing Office, 1969), pp. 696-709, see Part 5, subsection (1) of conclusions.

[2] Alexander L. George, *Bridging the Gap* (Washington, DC: United States Institute for Peace Press, 1993). See also Alexander L. George, "Some Guides for Bridging the Gap," *Mershon International Studies Review*, Vol. 38 (April 1994), pp. 171-172.

can assume using an Identity Mask and whose operations it can emulate, as emerging threats. Means emerging threats may employ are detailed, and a list of targets that are particularly attractive to emerging threats are outlined. These targets include national critical infrastructure sectors and population. Lastly, the typology identifies ends that emerging threats may pursue in the new security environment.

Following development of an emerging threat typology, the chapter introduces the game of Stalker, including seven variants of scenarios. These different scenarios were briefly introduced as a segue at the end of chapter three at the level of generic models of actors and their social – political relationships. In this chapter they are further explicated into attack model networks, or decision trees, that serve to model the variants in a form that can "bridge the gap" by providing policymakers and strategists with a graphical representation of Self – Threat interaction under the seven variants of Stalker. These attack model networks can be applied, with adjustment for specific context, to particular cases of conflict.

In this role, the chapter serves as a toolkit for strategists and policymakers concerned with formulating national security policy countering emerging threats. When analyzing a particular case, they can take from it intellectual tools, terms, concepts, elements of an emerging threat typology, and applicable attack model networks and, after some modification for context, apply these tools to their specific challenges. The threat typology developed is further explicated in terms of operationalized coding definitions in Appendix A: Coding Definitions. For those involved in data and text mining research concerning emerging threats and their means, targeting preferences, and ends, Appendix A provides a point of departure compatible with the Red, Gray, and Blue framework and this chapter's threat typology.

A Typology of Emerging Threats:

The classification and analysis of threat based on category type serves useful purposes. First, imposition of categories results in ordering data, and order aids understanding. Attempting to deal holistically with large amounts of data without first ordering it according to some typology is problematic. Human cognition is finite, even when assisted by computers, and without an ordering typology decisionmakers may suffer information overload when confronting a large amount of raw, unstructured data. A typology orders and filters information which, in turn, increases efficiency of information processing by culling irrelevant data and noise and structuring relevant information in categories that are understood by decisionmakers.

Second, ordering by a threat typology suggests characteristics of the threat and other aspects to decisionmakers. This reduces *de novo* analysis of all information gathered to determine its significance. A typology of emerging threats also suggests potential counters, time available, threat ends pursued, threat means available, threat targeting preferences, both friendly and threat vulnerabilities, and other information to the decisionmaker.

Third, a threat typology provides for warning decisionmakers of "high-priority" threats based on standing criteria and predefined parameters. The discovery of a threat capable of employing WME may signal to the decisionmaker a priority threat, for example. Based on positional responsibility, a threat typology can cue a decisionmaker that his organization's involvement is required.[3] Unless information is ordered and then analyzed to provide a specific cue to a decisionmaker, e.g., possession by an actor of WME, the identification of such a specific threat is made problematic.

The above purposes are not exhaustive. There are other advantages to employing a typology. However, there exist potential risks in employing a typology to categorize threats, as well.

First, viewing information through preconceived notions of what constitutes a threat risks not identifying threats that are novel or unique. A threat not anticipated by or encompassed within the typology may evade identification or be misidentified. Emerging threats in the current security environment may not be included in existing threat typologies, either implicitly or explicitly. The advance of technology has enabled the emergence of new threats based on new means. For example, past typologies formulated before the proliferation of the computer do not recognize a threat based on an actor employing cyberstrikes targeting a computer-controlled infrastructure.

Second, employing a typology risks misclassification of threats. Any abstract construct, including even broad typologies, cannot perfectly describe the infinite complexity of reality. There exists the risk of classifying a threat as something it is not, and this error is influenced by the traits of the typology employed. A highly abstract typology of few categories necessarily lumps diverse actors together based on a reduced number of variables; a highly stratified and differentiated typology of many categories avoids the risk of extreme aggregation at the cost of increased complexity. A desired characteristic of a typology is to balance these two extremes, with a design based on its subject matter that is useful and accurate, while not becoming complex and unwieldy.

---

[3] Vertzberger, pp. 70-74.

The challenge above concerns the risk that exists in failing to identify a threat and failing to properly identify a threat. Given the difficulty in understanding an environment without some ordering typology, however, this challenge must be met. Risk can be mitigated through intelligent design and judicious use of a typology, but it cannot be totally eliminated.

The identity of a threat is a nominal variable. As a qualitative classification, it captures inherent traits that describe, explain, and predict capabilities, intent, and activities. Means, Targets, and Ends are also nominal variables. The variables Means and Targets are roughly quantifiable, in so far as they can be measured in systemic impacts and potential casualties. However, they are also qualitative variables that describe the means and targets most probably associated with particular threats.

Threats:

Precise use of terms aids clarity. This study has explicitly adopted Singer's definition of threat to avoid the confusion of using the term in varying ways. As the Red, Gray, and Blue framework is "drilled down" from the paradigm to the generic case level, the term threat must itself be disaggregated into specific Red-types, and these types formally defined. Such precision and discipline in the use of terms provides a solid base for subsequent employment of the terms as tools capable of application to specific cases in particular contexts by policymakers and strategists. As crafted in this chapter, and explicitly defined in Appendix A: Coding Definitions, the terms and concepts can be adopted wholesale as existing tools into a coding effort, for example, that saves a researcher time and effort, and remains within the Red, Gray, and Blue framework.

Additionally, identifying types of Red explicitly defines the boundary between past conceptions of threat rooted in a state-centric perspective, and what is increasingly known in this new policy field as emerging threats. Frequent employment of the term "emerging threats" is made, yet almost as frequently not defined in any meaningful way. This is not helpful in providing in concrete fashion the requisite intellectual tools and concepts that materially contribute to the development of a perspective, from paradigm through case, that can inform policy. The foundation of policy is theory, and the crafting of theory requires precision and detail if it is to bridge the gap between thought and practice.

Identity	Means	Targets	Ends
Autonomous Terrorist Organization	Assassination	Banking and Finance †	Obtain WME
Cult	Biological Agent	Biological and Genetic Research /Production / Storage Installations	Contain the United States
Economic Warfare Team	Bomb	Business	Economic Advantage
Fringe Group	Chemical Agent	Chemical Research / Production / Storage Installations	Expand Power
Hacker	Cyberstrike	Continuity of Government †	Financial Gain
Information Warfare Team	Direct Action	Diplomatic/Political Target	Hate
Insider	Nuclear Weapon	Law Enforcement	Political Influence
Lone Wolf	Espionage	Electric Power System †	Ideology
Paramilitary Group	Extortion	Emergency Services System †	Metaphysical
Spy	Deception	Water System †	National Security Advantage
State	Economic Attack	Nuclear Research / Production / Storage Installations	Survival
State Sponsored Terrorist Organization	Information Operation	Government Installations	Political Change
Transnational Actor	Genetic Agent	Oil and Gas System †	Vandalism
Transnational Criminal Organization	Radiological Agent	Military Installations	Retaliation
		Public Health System †	
		Telecommunications / Information System †	
		Transportation System †	
	Crime	Population	
		Food System	

Table 4 - 1: A Typology of Threat by Identity, Means, Targets, and Ends[4]

[4] This table is organized by columns to portray that an actor may employ one, or many, means against various targets for diverse ends. For example a cult may employ a bomb against a military installation for the purpose of vandalism. The

The provision of terms defining types of emerging threats, or specific Reds, does not mean that modification will not be required. The employment of concepts at the generic case level may not be suitable for employment in specific cases and contexts without some modification. However, the generic case must provide a start point for such modification, or there will persist a gap between theory and practice that requires each new, specific case to bridge it. This bridging of the gap without the direction provided for by a generic case ensures a wide variety of terms and concepts being invented by a series of analysts that may not conform to the higher, more abstract levels' shared tenets, or hard core. Failure to develop the Red, Gray, and Blue framework below the level of theory would be to, in Lakatosian terms, not provide the positive heuristic of the research program, as explained in chapter one.

To this end, the terms introduced here are defined in Appendix A: Coding Definitions in four components: definition, usage, non-usage, and example. The definition of the term is its formal explanation. The usage component explains under which circumstances the term can be correctly employed, and non-usage sets the parameters of when the term cannot be correctly used. Finally, the example provides an illustration of the term in reality.

Operationalizing Emerging Threats:

A common vocabulary is a hallmark of a profession or field. This is as true for national security studies as it is for any other discipline. Many articles have been published in the past few years concerning emerging threats. Ironically sometimes a state actor, perhaps a resurgent Russia or advanced China, is identified as an emerging threat. The net effect of such use is to make the term little more than a cliché for *potential* threats. Emerging threats are distinct and different from conventional or potential threats. Until the terms in this newly established field of critical infrastructure protection countering emerging threats are codified in policy, vague reference to emerging threats to mean any threat will contribute to confusion and not progress. The typology introduced in this chapter is intended to serve as an intellectual tool to clarify discussion.

Means:

The use of a specific means to conduct an attack has implicit meaning. This meaning provides some degree of insight into the nature of the threat, its capabilities, resources available at its command, technological sophistication, targeting preferences, countermeasures available to Blue, and many other

---

table's organization does not support reading across a specific row to connect an actor with fixed, specific means, targets, and ends. See Bill Flynt, "Threat Kingdom," *Military Review* (July – August 2000), pp. 12-21. † These targets, collectively, comprise the US Critical Infrastructure, as defined by Presidential Decision Directive 63, May 22, 1998.

details. However, to begin to exercise this degree of analysis concerning pure-type threat actors armed with specific means, one must first use a nomenclature of means that has rigor and meaning. Broad-brushed assertions that "emerging threats will use WME" are not helpful in designing national security policies to protect critical infrastructures and population. What is required is a typology that provides a shared understanding of the means as a foundation upon which more detailed analysis can be established. Without the shared understanding of terms describing means that are novel, there can be no analysis by policymakers and strategists that proceeds from the same start point. Some terms are not controversial in their meanings, and lay usage corresponds to the defined usage. However, some terms are unique, and without explicit, standard definitions confusion can result and hamper policy formulation and implementation.

Targets:

Targeting is an information-rich process, if analyzed. The selection of a target is rarely haphazard or random. Targets, even if at the subconscious level, are chosen by attackers for characteristics that are anchored in the attacker's own identity. Willie Sutton's famous remark of why he robbed banks is a profound statement regarding how targets point to the identity of their attackers.

Not only do characteristics of the attacker's identity influence target selection, characteristics of the target influence their selection as well. This is especially relevant for emerging threats seeking system-level effects. The characteristics of targets that influence their selection include difficulty in striking due to security measures, preeminence as a symbol, level of expertise in a field, potential for cascading effects resulting from a successful strike, unique or known vulnerabilities, requirements for attack resources, perceived or actual first-order relevance to the attacker, and other factors.

Gleaning information from targeting preferences of a threat actor entails understanding aspects of the target beyond the superficial. Considerations include location in space and time, the cyberspace topography or shallow cyberspace of the target, the target's image, and the secondary and tertiary effects achieved by striking. The target attacked is not necessarily the actual target. For example, should an emerging threat wish to target a large population concentration, one method would be to attack an industrial plant manufacturing toxic pesticides located in physical space such that prevailing winds would carry the gas plume to the population center. The physical location of the plant is relevant, but so is the timing. Wind patterns vary according to the time of day, weather patterns, and

other factors. This introduces timing into the calculus of the attacker. And the existence of known vulnerabilities in a particular plant's computer SCADA network makes it a particularly attractive target.

The ability to gain insight into the attacker through the targeting preferences exercised depends on Blue's framework, perspective, and intellectual tools and concepts. Approaching the incident at the pesticide plant from the traits inherent in an insurance fraud investigator's perspective, one consideration for information gathering will be the financial soundness of the plant, believing that there exists the possibility of deliberate sabotage by company management to cover financial weakness with insurance compensation for loss. The traits inherent in a systems engineer perspective will be to look for flawed equipment and outdated procedures that contributed to the accident. One perspective of the corporate security director will be to review the possibility of a disgruntled employee seeking revenge. Management will be concerned with confirming maintenance processes were properly documented, standard operating procedures were followed by employees, and with limiting corporate liability to litigation. All of these perspectives serve to hide the identity of the true attacker, and in the case of fear of litigation even limit information to investigators, because they are all founded on an insufficient appreciation of the plant's own traits when viewed not as an accident site, but as a target. The ability to discern information from targeting is thus partially dependent on Blue's own traits. The perspective most likely to approach the incident from a functionally adequate perspective is that of a counterterrorist analyst. This is not a perspective likely present at the site of a routine industrial failure until casualties reach a high threshold value.

The result is the perspective most likely to determine the true intent of targeting is only involved after a significant, successful strike. Attempted strikes that fail likely escape analysis from perspectives that could better inform indications and warning.

To discern information regarding threat from the nature of the target necessitates a rigorous definition and explanation of the target's aspects. Referring in sweeping terms to the national electrical grid as a target for emerging threats is at the paradigmatic level of abstraction. To serve as an intellectual tool at the case level, however, the electrical grid must be disaggregated into its component subsystems and the characteristics of the subsystems themselves analyzed. This approach would then inform specific case analysis involving attacks on such targets.

The detailed analysis of a particular target category would itself constitute a separate, major study, and is not necessary for the purpose of this section. It suffices here to state in this typology at

the generic case level the types of targets that emerging threats will engage. This provides the necessary start point from which a specific case analysis must depart.

Ends:

Among the most informative items of knowledge that Blue can possess enabling effective countermeasures to a Red strike is to know the specific ends that the threat is attempting to achieve. If the end is known, then some means and targeting options can be eliminated as viable courses of action for the threat to employ based on the known end. The analogy is that if the destination is known, then only particular routes will get one to the desired destination. Of course, knowledge of the end does not necessarily make the analysis of threat an easy study. Many means and targeting options can still accomplish the same end. However, to the extent that a threat's end is known, some analysis is made under less uncertainty.

Knowing a threat's end also simplifies Blue's defensive planning. For example, given that a threat is identified that has the known end of obtaining WME research, Blue can allocate additional resources to protecting the repositories of such research. Identification of end allows a quasi-reverse engineering process of security policy creation that uses as a start point the denial of what the threat wishes to achieve. The category of ends may communicate information to Blue that neither the category of means or targets imparts. Similarly, the means and targeting preferences of a threat communicate some information that is not inherent in the end pursued. By combining knowledge of means, targets, and end a threat can be largely defined, and perhaps even precisely identified in some cases. The category of end, however, as the terminal category for Red's constitution as a threat is a key indicator of future activity.

The Game of Stalker and Seven Attack Model Networks:

Shelling noted that failure to anticipate threats is a characteristic of an inappropriate national security framework: "...the danger is in a poverty of expectations – a routine obsession with a few dangers that may be familiar rather than likely..."[5] Like the failure of Pearl Harbor the failure national security elites commit in the current security environment, this study argues, is that the threats and the threats' operations are not understood due to the employment of a functionally inadequate framework; it cannot "bridge the gap." Policymakers' vague references to "emerging threats" and "asymmetric strategies" may communicate their conviction that the current paradigm is inadequate, but the

references do not suffice to provide the detailed, explicit theory upon which policy must be established. Stalker is a game that describes and explains the emerging threats and their actions, and additionally provides seven attack model networks that capture the dynamics of conflict with these actors.

As above with the threat typology and Appendix A's explicit definitions of emerging threats, until new concepts are placed into a sufficiently detailed form that at least allows criticism there can be little progress. Bacon's dictum, again, calls for clarity and not confusion as the best route of progress. Even flawed notions, provided they are made explicit and thus vulnerable to critical thinking and scholarly debate, can promote the cause of progress in understanding. To this end seven attack model networks that describe variants of the game of Stalker are explicated. An attack model network is a graphical form of knowledge that has formal probabilistic semantics, rendering it suitable for statistical calculations. Such networks incorporate expert knowledge of a process, here in the game of Stalker the attack of Blue by an anonymous, asymmetric, asynchronous Red. Attack model networks are similar to neural networks, with two important advantages: first, the capability to easily encode expert knowledge into the network allows better subsequent discovery of additional knowledge, and, second, the nodes and arcs in such networks describe processes in terms of causal chains.[6]

Conventional, traditional approaches to modeling threat are of limited utility in modeling anonymous, asymmetric, and asynchronous threats targeting critical infrastructure. State-centric approaches fail to capture the means, methods, and ends of non-state actors. Approaches suitable to state-on-state conflict, and emphasizing the conventional military instrument of power are unwieldy intellectual tools when countering emerging threats. For example, the Joint Intelligence Preparation of the Battlespace (JIPB) methodology described in the US Joint Chiefs of Staff doctrine is not suitable for application to emerging threats, because the explicit, overarching paradigm of JIPB is predicated on protecting a US military force deployed away from the Continental United States (CONUS).[7] Yet, despite the US military's significant role in homeland defense, the JIPB and its service-specific

---

[5] Thomas Schelling, foreword to Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Palo Alto, CA: Stanford University Press, 1962), p. xiii.

[6] David Heckerman, "Bayesian Networks for Knowledge Discovery," in Usama M. Fayyad, Gregory Piatetsky-Shapiro, Padhraic Smyth, and Ramasamy Uthurusamy, *Advances in Knowledge Discovery and Data Mining* (Cambridge: MIT Press, 1996), pp. 273-274.

[7] A representative quote from newly written doctrine for US Joint Forces makes the point: "National interests require the United States to act in concert with other nations. In many situations, Armed Forces of the United States will join with foreign military forces to defeat common adversaries..." This doctrine still applies within its narrow world, however, it is increasingly irrelevant to the emerging challenges faced by the United States. Quote from *Doctrine for Intelligence Support to Joint Operations*, Joint Publication 2-0 (Washington, DC: Chairman of the Joint Chiefs of Staff, 9 March 2000), p. A-1.

counterpart methodologies are the only existing doctrinal models for assessing threat. These, literally, Cold War era models have limited applicability for assessing emerging threats targeting US critical infrastructure and population. Such models founded in state-centric approaches, focusing exclusively on the military instrument of power, and in the context of policy implementation in locations overseas are fundamentally flawed as an approach to the emerging threats in the altered security environment.

Reliance on past models and approaches may not only be ineffective, but dangerous. National analysts trained and tasked to monitor and assess military strikes against a state actor by another state actor may be unable to perceive the patterns and activity of a non-state actor. In the United States analysts from national intelligence agencies are significantly constrained from examining many types of activities occurring within CONUS.[8] This is an institutional constraint that denies intelligence analysts the experiential base required to gain analytical expertise and knowledge of emerging threats. Vertzberger points out that perception, hence cognition, is filtered through a societal-cultural prism, and this "impacts on information processing."[9] National analysts are trained and tasked to think in terms of regions and countries, the military instrument of power, and state actors. Their education, training, and performance measures are predicated on a cultural community that itself is founded on a state-centric perspective that is institutionalized through resourcing, tasking, and other factors. It is a classic Kuhnian community paradigm. This societal-cultural prism can cause analysts to fail to see emerging threats that differ in identity, means, *modus operandi*, targeting preferences, and ends from threats with which they are familiar, responsible for, and resourced to identify because of societal conditioning and an established community paradigm.

A case in point is the failure of the Japanese Government to initially perceive the religious cult Aum Shinrikyo as a threat to the Japanese state and people. Although known to authorities as a problematic religious cult with numerous complaints against it of kidnappings and physical assaults, Aum Shinrikyo was not perceived by authorities as a threat actor, or Red.[10] It thus enjoyed *de facto* anonymity as a threat actor, because authorities' perception of it "masked" its true nature. Aum Shinrikyo exploited the authorities' preconceptions by conducting quasi-religious activities to maintain this Identity Mask. Of course, Aum Shinrikyo proved to be more than a cult that simply abused its

---

[8] Multiple legal authorities exist governing the collection of intelligence within the United States by various agencies. See as examples *Executive Order 12333: United States Intelligence Activities* (Washington, DC: Executive Office of the President, 4 December 1981), and *Department of Defense Regulation 5240.1-R: DoD Intelligence Activities* (Washington, DC: Department of Defense, 25 April 1988).

[9] Vertzberger, pp. 260-261.

members. They produced and employed both chemical and biological agents, and at their height of power had approximately 60,000 members in six countries, possessed over one billion dollars in assets, and mounted multiple attacks using WME against the government and people of Japan designed to inflict tens of thousands of casualties.[11]

What are needed are new, relevant intellectual tools that are made explicit to a level that enables criticism to assist in understanding the nature of the emerging threats in the new security environment. As detailed in chapter one, Jervis' Law of the Instrument applies. Until policymakers and strategists possess new intellectual tools with which to understand the environment, they will continue to employ the "hammer" of past concepts to pound every problem as if it were a nail. The game of Stalker and the seven attack model networks of its variants, when coupled with the threat typology above, serve as the intellectual tools required to understand the altered security environment, and enable the construction of a foundation of theory to support the creation of intelligent national security policies.

Below, the study continues extending the security environment approach from paradigm through model to decision trees. It presents Stalker's seven variants that are capable of showing the logic and decision calculations of multiple actors. These networks are "probabilistic graphical models [that] are a unified qualitative and quantitative framework for representing and reasoning with probabilities and independencies."[12]

There has been some research on identifying the process emerging threats exercise in attacking Blue. For example, Scambray, McClure, and Kurtz have delineated an attack template for computer intrusions. This template proceeds through the steps: footprinting, scanning, enumeration, gaining access, escalating privilege, pilfering, covering tracks, creating back doors, and then conducting a denial of service attack as a branch option after gaining access.[13] This flowchart of attack methodology, like others, misses the mark. First, the flowchart suggests that a threat just "is" and is not created by intrinsic traits of Blue or Red. This fails to examine motivations, which dictate ends pursued, and as such relegates the process advanced to at best a tactical level analysis of a small portion

---

[10] *Global Proliferation of Weapons of Mass Destruction: A Case Study on the Aum Shinrikyo*, Senate Government Affairs Permanent Subcommittee on Investigations Report (Washington, DC: US Senate, 31 October 1995) section III. A. 2.

[11] Ibid.

[12] Wray Buntine, "Graphical Models for Discovering Knowledge," in Usama M. Fayyad, Gregory Piattetsky-Shapiro, Padhraic Smyth, and Ramasamy Uthurusamy, eds., *Advances in Knowledge Discovery and Data Mining* (Cambridge: MIT Press, 1996), p. 59.

[13] Joel Scambray, Stuart McClure, and George Kurtz, *Hacking Exposed*, 2nd ed. (Berkeley: Osborne / McGraw Hill, 2001), back cover.

of a threat's method of operation. Second, this specific methodology is not logically consistent internally, as activity (creating back doors) occurs subsequent to the stage of "covering tracks." The point is not to denigrate a specific effort to understand emerging threats. It is that the analysis of emerging threats will not be sufficient until the security environment is itself first analyzed. Building tactical models within tightly limited arenas of inquiry that do not first examine the paradigm within which they are created simply constitutes doing things more accurately within a fundamentally failed model. It is doing the wrong thing better. Attempts to analyze emerging threats will not contribute as much as they could until the foundation of the environment is itself first examined.

Stalker is a game played by at least two actors: Red (the Stalker) and Blue (Self). The name is derived from the analogy of a person being "stalked" by another individual. A stalker observes the target's activities and behaviors, learning in great detail all aspects of the target's routine. In the current security environment, this study argues, the United States is being stalked by emerging threats targeting critical infrastructure and population. These threats do not need to overtly confront the United States to achieve their objectives; they adopt the Stalker's covert, asymmetric approach to attaining their goals.

An interesting aspect about the game of Stalker is that the victim (Blue) is required to play, even if the threat (Red) is not playing. Denied knowledge of the Stalker's activities, Blue must always be vigilant, monitoring the environment for indications and warnings that signal an asymmetric actor's presence. This means that Blue is always paying the costs of vigilance, even when there is no cost for an asymmetric actor maintaining a passive status of observation.

Stalker is not a zero-sum game, in the formal sense that the sum of losses and wins equals zero. As becomes evident below, Red possesses the initiative at the start of the game, and can exercise the option to withdraw from play at any time. This makes a strategy of "raid and run" a winning strategy for Red.

Number of Actors in the Stalker Variants:

The game can involve multiple actors in seven possible permutations. The variants of the game establish a minimum foundation for different structures of actor relationships, different actors types, and different numbers of actors. The different number of actors involved is self-explanatory, with one note. The number of actors is a minimum "floor" that contributes to defining a specific "world" or

structure of conflict variant. The different actor types are signified by color as explained below. The different structures of conflict are described by the variant titles.

"Simple Conflict": In the first permutation of the game, Simple Conflict, there are exactly two actors: Red and Blue. Red is the Stalker, and is an emerging threat actor. Blue is Self, and a state actor with two Clausewitzian centers of gravity: national critical infrastructures and population. This variant is discussed in detail below. The remaining six variants have encoded within their attack model networks the core of a simple conflict decision tree. This variant is depicted in Figure 4 – 1: Simple Conflict.

"Ganging Up on Blue": In the second permutation of the game, Ganging Up on Blue, there are at least three actors: one Blue actor, and two or more Red actors. There may exist more than two Red actors, however, for the purpose of this study the minimum required number of actors is used. Consideration of additional actors is unnecessary to define the structure of conflict in a particular world, or variant. The two Red actors in this world pursue a common end, with the potential for betrayal encoded within the network. This variant is depicted in Figure 4 – 2: Ganging Up on Blue.

"Ganging Up on Red": In the third variant of the game, Ganging Up on Red, there are at least three actors: one Red actor, and multiple Blue actors. The Blue actors pursue a common end, again, with the potential for betrayal and division encoded at the decision nodes. This variant is depicted in Figure 4 –3: Ganging Up on Red.

"Alliances": In the fourth permutation of the game, Alliances, there are at least two Red actors and two Blue actors, for a minimum of four actors involved in the game. The Red actors are allied to attack at least one Blue actor, and the Blue actors are allied to defend against Red attack. This world is depicted in Figure 4 – 4: Alliances.

"Factions": In the fifth variant of the game, Factions, there are at least three actors, all of whom are independent, non-allied actors. The actors are Red, Blue, and Yellow. Yellow, a threat actor, is not allied with the other threat actor, Red. Third Actor Escalation is possible in this permutation, as it is in all variants of more than two actors. This variant is depicted in Figure 4 –5: Factions.

"Mixed Game": In the sixth permutation of the game, Mixed Game, there are a minimum of three actors. The actors are Red, Blue, and Green. Green is a neutral actor, or an actor of indeterminate intentions. Figure 4 – 6: Mixed Game illustrates this variant.

"N-Actor": In the seventh permutation of the game, N-Actor, there are at least four actors, with various combinations of independent actors and alliances possible. The actors are Red, Blue, Yellow, and Green. Should three alliances form, the game reduces either to the "Factions" or "Mixed Game" permutations. Should Yellow and Red ally, the game reduces to a "Mixed Game" variant. Should the Green actor ally with either Red or Yellow, or transition to a new threat actor unallied with either Red or Yellow, the game reduces to "Factions." The N-Actor game requires a minimum of four actors. Figure 4 – 7: N-Actor depicts this variant.

The variants do not attempt to delineate worlds where dozens of actors are involved in the conflict; the model is not reality. Instead, the variants describe the base worlds that can exist given the minimum numbers of actors. This approach allows for the explication of underlying dynamics that exist in various, base permutations of conflict, without attempting the impossible task of identifying the structure of the infinitely possible permutations of reality. Theory, even at the level of models and decision trees, must abstract from reality to achieve parsimony, elegance, power and comprehensibility. Using these base principles and relations inherent in the networks, scholars can modify these generic case models to apply to their specific cases.

Definitions of Actors by Color:

Each actor type is signified by a color, as has been the convention in the study. Blue is synonymous with Self, and Self possesses a known identity, intent, capabilities, and characteristics. Red is a subcategory of Other; an anonymous threat actor. Red is always a non-state actor, or a state emulating a non-state actor. Finally, Red is the Stalker. Green is also a subcategory of Other, and is either a neutral actor or an actor possessing indeterminate intent. Green possesses capabilities to either join Blue (J) or help Red (H). Yellow also is a subcategory of Other; a threat actor pursuing a different goal than Red. Lastly, Gray is a subcategory of Other that is either an unknown actor or actor of unknown intentions. A Gray actor may or may not possess capabilities to enter the conflict, but is unlikely to do so.

The Scenario of Stalker:

Stalker is a scalable model, applicable to the strategic, operational, and tactical levels. In the context of this study the level of conflict analyzed is the strategic level. In this context the actors are capable of system-relevant levels of violence, and the outcome is potentially relevant to other actors not involved in the conflict.

Blue is a legitimate, sovereign government and a state actor. Throughout the study Blue has referred to the United States and its efforts to protect national critical infrastructures and population. In this analysis of the game's variant one, however, Blue refers to any state actor. Although not specifically the scenario for the below analysis, the game of Stalker can model on a case-specific basis any actor or organization, e.g., a corporation.

Red is attacking Blue anonymously, asymmetrically, and asynchronously. Red combines capabilities with intent, and is not known by Blue until it acts, or is discovered. Red's targeting preferences are critical infrastructures and population, with the intent to inflict system-relevant levels of damage on Blue.

There are three ways Red can be discovered by Blue. The first is through Blue's efforts to scan the environment, which is called Discovery in the model. The second way Blue can learn of Red is through a Red mistake or activity that results in compromise of its existence and identity. This is called Unmasking. Lastly, Blue can learn of Red through identification by a third party. This is called Betrayal, and applies to Stalker variants where more than two actors are involved in the conflict, and one actor can "turn" on Red.

This study's treatment of Stalker is limited to a scenario of Simple Conflict, or variant one of the seven attack model networks. This decision tree is embedded within each of the variants as a fundamental structure; however, the different variants each possess radically different actor relationships and other dynamics. This means the analysis of Simple Conflict cannot be directly applied to the other variants, as outcomes and interactions vary too greatly across the variants.[14]

The Rules of Stalker:

[14] The detailed explication and analysis of all seven variants, including mathematical analysis, will be accomplished in a forthcoming work.

Rules provide structure and definition. Although the game boards for chess and checkers are similar, the rules dictating play of the pieces and the capabilities of the pieces serve to distinguish checkers from chess. The structure of a game is comprised by the rules, which in turn define the game. Rules can be broken, but the result is that the game is not of the type defined by the rules, but a different game. For example, two players may practice moving all pawns as if they were queens, but they are not then engaged in playing chess. In the interest of attracting criticism, the rules of Stalker are, as with the other intellectual tools, made explicit by the study. The rules that define the game of Stalker follow:

Stalker's General Rules:

1. Blue is aware of pure-type threat actors.[15]
2. Red possesses the capabilities and intent of a pure-type threat actor.
3. There must always be a Red actor opposing Blue.
4. The game of Stalker starts with Blue unaware of Red as a specific threat actor.
5. At the beginning of the game, Red has the initiative.
6. The game of Stalker ends when: 1) Blue defeats Red attack (at Node G_{12}), or, 2) Red succeeds in its attack (at Node G_{11}), or, 3) Red withdraws (W).
7. Red may elect at Node 0 to play or not to play the game.
8. Blue must continually play. In the absence of an active Red attack Blue's play is characterized by defensive operations and monitoring of the environment.
9. Multiple Yellow or Green actors are considered as one Yellow or Green actor.

Blue Rules (Target):

1. Blue will take precautionary actions to protect itself before attack, anticipating some unknown future threat.
2. Blue initially has no information of a specific Red actor planning imminent attack.
3. Blue is permitted to preempt Red if it discovers sufficient information to do so.
4. Blue is permitted to attempt TAE to split threat actors.

Red Rules (Stalker):

1. Red's means, targeting, and ends are determined by its identity, capabilities and intent.

---

[15] The pure-type threat actors are in Table 4 - 1: A Typology of Threat by Identity, Means, Targets, and Ends.

2. Red will strive to conceal the fact that an attack has taken place (undiscovered effects), if possible (means and targeting) and desired (ends). It will use asymmetric and/or asynchronous techniques to accomplish this.
3. Red will always strive to remain anonymous. It may additionally employ an Identity Mask to shield its true identity in the event of Discovery, Unmasking, or Betrayal.
4. Red will portray a different threat actor to mask its identity if its activity cannot remain covert and anonymity is not feasible.
5. In the case of Red wishing to portray a different actor for TAE, Red will adapt its means, targeting, and apparent ends, within constraints of its capabilities, to give the signature of the third actor it wishes to portray.

Third Actor Escalation (TAE):

The objective of TAE is to foment conflict between two actors for one's own purposes. By inciting two Others to conflict, Self limits the resources of Others that can be employed against Self. It also allows Self to act as Blainey's proverbial Japanese fisherman, positioned to benefit from conflict between Others acting as fighting waterbirds, and thus able to "catch fish" (benefit from the conflict) because the waterbirds are occupied with fighting and not fishing.[16] This aspect of conflict dictates that even neutral actors (Green) bear close watching.

TAE can be employed against Self. A danger is that Self will fail to recognize that it is the target of TAE by an Other. Should Self command a thorough knowledge of a specific Red, analysis of attacks may be able to confirm or deny that the true perpetrator of the attack is that specific Red.

There are two types of TAE that Self can employ: 1. Pre-strike TAE, and, 2. Post-strike TAE. Pre-strike TAE occurs prior to reaching node six on the variants' decision trees, and allows Self to engage Other(s) with TAE tools, tactics, techniques, and procedures (T + TTP) that will serve to deflect or lessen resources dedicated to subsequent strikes against Self. Pre-strike TAE is a better course of action for Self than Post-strike TAE, because it has the potential effect of preempting a strike against Self, and involving threats in conflict with each other, also serving Self's interests. Post-strike TAE occurs after having been targeted by an Other, and is designed to lessen an Other's subsequent resources that can be allocated against Self. Post-strike TAE accomplishes this by expanding the conflict to include Others, thus complicating Red's decision calculus, and forcing it to guard itself from multiple actors. Post-strike TAE may relieve pressure on Self, but it may also, but not necessarily, cost resources that could otherwise be employed against Red.

[16] Geoffrey Blainey, *The Causes of War*, 3rd ed., (New York: The Free Press, 1988), pp. 59-60.

There are four techniques that Self can employ to accomplish TAE:

1. Self can provide "damning" intelligence to Red and an Other to increase suspicion and the chances of conflict between the two actors. This can be done to conceal or disguise the source of the intelligence.
2. Self can conduct a strike, masked as an Other against Red, or masked as Red against an Other, or both. In the case of masking as an Other attacking Red, this will serve to provide a motivation and pretext for Red's retaliation against the Other portrayed as the attacker, with potential subsequent ignition of conflict and allocation of resources to conflict between the two actors, resources that cannot then be used against Self. In the case of masking as Red attacking Other, the TAE strike serves to provide Other with both motivation and pretext for attacking Red. Credibility of a TAE strike masked as Red is enhanced by Red's prior aggressor status against Blue in the case of post-strike TAE.
3. TAE can be accomplished by requesting assistance from Others, and promising rewards to them. This is not necessarily coalition building, but may simply be a promise to not attack Other while it is engaged in attacking Red, thus simplifying Other's decision calculus and increasing potential payoff to Other.
4. TAE can also be accomplished by threatening Others and demanding their assistance in fighting Red. This is the equivalent of stating that if Other is not supporting Self, then it will be viewed as a threat. This technique may not be effective if employed alone, however, if employed as a subtle, veiled threat complementing the technique of requesting assistance and promising rewards, it may prove effective in enhancing the chances of Other agreeing to bandwagon with Self.

Stalker's Plateaus:

Stalker's plateaus are characterized as patterns of behavior that can exist over time within the game's structure. There are seven plateaus.

Plateau - 0: Status Quo – This plateau is characterized by a pattern of behavior that accepts the status quo. Red takes the decision to not prepare at node 0 (See Figure 4-1: Simple Conflict), and the game is not started. The plateau is disrupted when Red takes the decision to begin preparations for attack.

Plateau - 1: Hold Reconnaissance & Continue Preparation – This pattern of behavior results from Red's decision at node 0 to begin preparations to strike Blue, but Red stops short of deciding to conduct reconnaissance operations. Blue is thus provided with the opportunity to perceive Red's preparations, and potentially to initiate preemptive operations. This plateau typifies Red as planning, gathering materials and equipment, training, and forming organizationally. Red may persist in this plateau for some time, perhaps indefinitely. The plateau can be disrupted by Red's decision to begin reconnaissance or cease operations, or if Blue preempts Red.

Plateau - 2: Hold Strike & Continue Preparation & Reconnaissance – This plateau results from Red's decision to begin reconnaissance operations. This decision provides Blue with its second opportunity to discover Red and initiate preemptive operations. In this plateau, Red is typified as both continually preparing and actively reconnoitering to ascertain Blue vulnerabilities. The plateau can be disrupted by Blue's discovery and preemption of Red, or Red's decision to strike or cease operations.

Plateau - 3: Undetected Strike – Red takes the decision to strike. Blue is not cognizant of the strike, although it has the opportunity to perceive the strike. This presents Red with the option of continuing in plateau 3 until Blue perceives the effects of Red's strike. The failure of Blue to perceive the strike may be due to the characteristics of the strike, i.e., scale, intensity, location, timing, targeting and other considerations, or the failure to perceive the strike may be due to characteristics of Blue, i.e., lack of feedback system, failure or absence of monitoring equipment or sensors, or negligence. Plateau 3 allows Red to continually strike inflicting damage to the limit of its ability and will. The plateau can be disrupted by Red's decision to stop striking or Blue perceiving the strike.

Plateau - 4: Unresponsive Target – This plateau results from Blue's perception of Red's strike, but Blue's decision not to respond or inability to respond. Blue may choose not to respond for several reasons. One reason may be that the cost of responding exceeds the costs of not responding. This case may pertain to low-level, low-cost attacks mounted by unsophisticated, low-threat actors without success. The decision to observe, but not respond may even serve as training for Blue's forces, where response would remove the opportunity to observe actual Red attacks, and result in Blue having to duplicate the scenario with simulations or self-resourced sparring partners or "red teams." An example would be Blue's decision to not respond to ineffective attempts at penetration of a corporate computer network in order to maintain the defensive force's skills and alertness, minimize the costs of legal action, gather information on developing techniques employed by attackers, and husband resources and efforts for serious threats. Blue may choose not to respond to minimize feedback provided to Red by any action Blue would take, allow the collection of forensic evidence over time to

reinforce future anticipated legal action, ascertain Red intentions and information on Red's *modus operandi*, and to feign unawareness while mounting a significant counterstrike. Alternatively, this plateau may persist if Blue possesses no means of responding. This plateau can be disrupted by Red's ceasing of operations or Blue's countering Red's attack.

Plateau - 5: Defensive Target – This plateau results from Blue's decision to pursue an exclusively defensive posture against Red's strike. This allows Red to maintain the initiative and to strike without fear of retaliation. Blue may take this decision when defensive measures are certain and offensive measures are unable to be effectively employed or are very costly, ineffective, or legally problematic. Blue can allow this plateau to persist, however, the potential exists that future T+TTP employed by Red will eventually defeat Blue defenses resulting in damage. Adopting a purely defensive posture is in the mid- to long-term a dangerous proposition. Blue conducting an offensive counterstrike or Red ceasing its operations can disrupt this plateau.

Plateau - 6: Ineffective Retaliation – This plateau results from Blue's decision to conduct offensive operations against Red, but Blue's subsequent inability to effectively engage Red. This condition allows Red to persist in this plateau until Blue can effectively engage and defeat Red. The plateau will be disrupted if Blue's counterstrike is effective or Red ceases operations.

Stalker's Seven Attack Models:

Applying the model:

The analyst must first define the problem in terms of desired ends for the players. For Blue this will entail protecting population and critical infrastructures. For Red, it means defining desired effects of its attack that are compatible with its identity. Should a player be pursuing more than one end, the analyst must rank order the ends in order of desirability from the player's perspective. Following identification of players' ends, the most probable means employed by the threat to achieve his ends must be identified. The means employed by Red dictates the active conductive medium(s) within which players will join conflict (unless Red's anonymity is compromised, in which case Blue could preempt and, thus, dictate the active conductive medium). Which conductive medium is "active," or "in play," is a function of both Blue and Red ends, means, targeting, and environmental factors (Gray). Following evaluation of the threat and conductive medium, the analyst must construct a detailed event matrix that describes Red activity upon initiation of preparation, reconnaissance, and attack, based on multiple Red courses of action. This, in turn, drives information needs to confirm or deny Red activity corresponding to a specific course of action. At this point analysis can begin.

Simple Conflict:

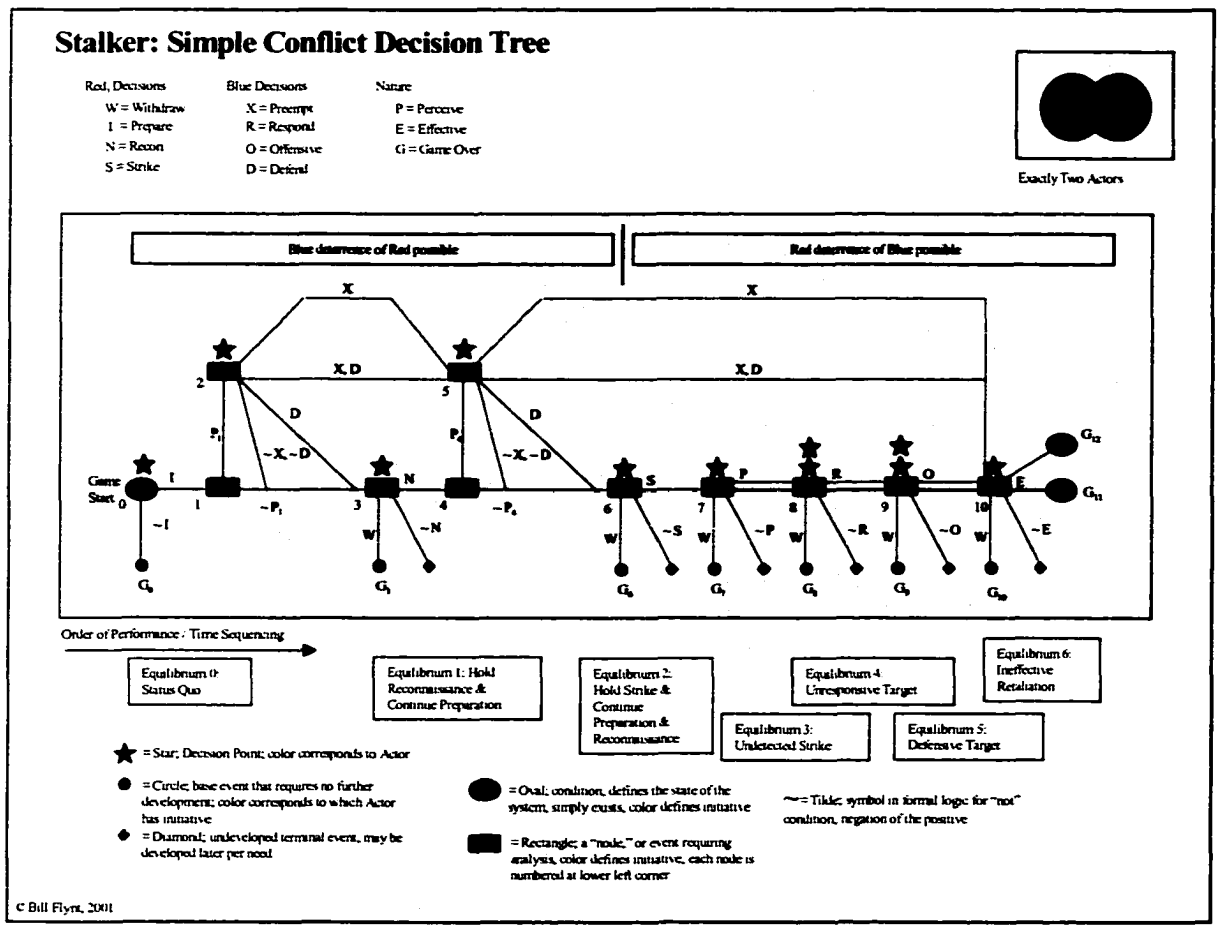


Figure 4 – 1: Simple Conflict Attack Model Network

The Stalker variant of Simple Conflict is the first level of complexity for analyzing the progression of attack of Blue by an anonymous Red. The discussion of this attack model network will proceed by node.

In Simple Conflict there are exactly two actors, Red and Blue. Unlike the more complex networks constituted by three or more actors, Simple Conflict does not allow the exercise of Third Actor Escalation, defection, betrayal, or mid-game (mid-operation) transition to different variants.

At node 0 Red has the initiative and is anonymous. Red may elect to prepare an attack against Blue, denoted by the variable "I" for initiate. If Red chooses not to prepare for an attack, "~I" meaning

"not-initiate," the game ends at terminal event G_0. At G_0 Red has not suffered losses (costs), nor has Red gained any payoffs (benefits). Likewise, Blue has not realized costs or payoffs. Red has also not moved from a passive status, which makes it difficult for Blue to become aware of Red's existence, identity, capabilities, and other attributes. This status at G_0 allows Red to remain a force in being, capable of starting the game at will later.[17] It also makes the identification of Red by Blue problematic.

Remaining at G_0 is *de facto* acceptance of the status quo. Red may not be satisfied with the status quo, but Red's dissatisfaction is not sufficient of a cost to motivate it to move to the preparation for attack stage. Red's decision to not prepare places it into Plateau 0: Status Quo.

At node 0 Red retains the ability to take the decision to prepare, signified by the red star above node 0, however, Red has not yet taken action. Singer defined a threat as an actor with both capability and intent to do harm.[18] At the time of his analysis, this was an adequate formula for threat definition given that the capabilities of concern were large maneuver forces in Eastern Europe, or ICBMs in silos that could be counted from space. In the current security environment, capability to affect significant harm is man-portable. A laptop computer can pose a significant hazard to national security when wielded by a trained hacker. Capability must be assumed in today's security environment.[19] Without Red action it is impossible for Red to transition from a "threat in being" to "a clear and present threat" to Blue. Given the assumption of Red's capability, and the inability of Blue to assess any actor as a threat based solely on possession of capability, the communication of intent by action remains as the sole indicator of threat for Blue. This is a reversal of the Cold War's assumption of the Soviet Union's intent, but uncertainty regarding some capabilities; in today's security environment, the capabilities of Red are assumed, and the effort that is required to provide indications and warning hinges on assessing intent. As evident at node 0, intent cannot be assessed without some action.

Should Red initiate any activity it will entail a risk of compromise, hence Red realizes costs. Only a perfectly passive posture is devoid of risk. This equates to Red foregoing any activity that may reveal its existence or bring suspicion on it. A Red actor that, for example, attends meetings of enemies of the state or is on mailing lists for organizations hostile to Blue runs risk of compromise, and in the

---

[17] For a complete conceptual explanation of "force" [a.k.a. "fleet"] in being, see Sir Julian S. Corbett, *Some Principles of Maritime* Strategy (Annapolis: Naval Institute Press, 1988), pp. 211-212. See also Alfred Thayer Mahan, *The Influence of Sea Power Upon History, 1660-1783* (New York: Dover, 1987).

[18] Singer, "Threat Perception and the Armament Tension Dilemma," p. 94.

[19] Bill Flynt, "Threat Convergence," *Military Review* (September – October, 1999), pp. 2-11.

game is viewed as having chosen to prepare, I, and transitioned from node 0 to node 1. Communication within a Red community is preparation, and can potentially be perceived by Blue.

Any activity by either Red or Blue potentially provides information to the Other. The conduct of conflict is a type of communication. Red preparation for a direct action attack against Blue may entail purchasing common, dual-use ingredients for field-expedient demolitions. The purchase of ammonia nitrate fertilizer, for example, communicates several items of information. First, that Red is preparing for an attack, and this attack will involve an unconventional bomb. Second, that Red possesses the knowledge to assemble a bomb from off-the-shelf ingredients, which suggests a level of training and sophistication beyond the average individual. Third, Red did not possess an adequate inventory of demolitions. Fourth, the amount of material purchased can be analyzed to estimate the size bomb Red could prepare. Fifth, essential ingredients not purchased may already be in Red's possession, or they may be purchased in the future which would provide Blue an opportunity to intercept Red later. Other items of information could be extracted from Red's activity, but the point is made. Action conveys (dis)information. In this example, following Red's action Blue has partial knowledge of Red's identity, means, and feasible targets.

The above is contingent upon Blue perceiving Red's action at node 1. In Stalker, this is one of only two opportunities (node 1 and node 4) Blue will potentially have to perceive and hence preempt Red. Without knowledge of Red, it is impossible to deliberately preempt Red. In the current security environment where intent is difficult to ascertain, and capability must be assumed, action becomes the best indicator of threat. However, action may not be perceived until too late. For this reason, Blue must be cognizant of when it may potentially perceive Red activity that will allow preemption. Failure by Blue to understand that early warning in Simple Conflict depends exclusively on perception of Red activity early in the game may mean the loss of opportunity to preempt by Blue.

Red can take measures to lessen the "signal" its activity generates.[20] By rationally timing its activity to correspond to an increase of "noise" in the environment – Gray – Red can conduct its

[20] If Red has a thorough understanding of Self, then it knows what patterns or signatures its presence or activity generates. Red can then alter its activity deliberately to avoid detection of its threat signature. Blue, anticipating Red activity, will scan the security environment for Red's signature; however, it will not in this case succeed if it only is watching for a particular signature: "To discriminate significant sounds against this background of noise, one has to be listening for something or for one of several things....one needs not only an ear, but a variety of hypotheses that guide observation." Wohlstetter, *Pearl Harbor*, p. 56.

activity below the sensing threshold of Blue.[21] This points out that Red, like Blue, must understand where its potential for being perceived by Blue exists in the game. As a thinking player, Red can outsmart Blue by manipulating or using Gray to mask its activity. Continuing the above example, purchases of ammonia nitrate fertilizer during the Christmas season is a clear signal of anomaly. Timing the purchase to coincide with the week most farmers purchase fertilizer would lessen this signal by understanding when "noise" will be strongest in Gray. Similarly, limiting the amount purchased to what is within the norm also lessens the signal strength against the noise background. Buying an amount larger or smaller than typical will attract attention. The methods of masking activity are limited only by Red's imagination. Red's awareness of its most vulnerable points in the game will enable it to minimize risk of discovery by Blue by using Gray intelligently.

Red	Blue	Yellow	Green	Nature
W = Withdraw	X = Preempt	W = Withdraw	H = Help Red	P = Perceive
I = Prepare	R = Respond	I = Prepare	J = Join Blue	E = Effective
N = Recon	O = Offensive	N = Recon	C = Committed Neutral	G = Game Over
S = Strike	D = Defensive	S = Strike	F = Fight All	

Table 4 – 2: Attack Model Network Variables for All Actors and Nature

If Blue perceives Red at node 1, then Blue reaches its first decision point at node 2 designated by a blue star. At node 2 Blue must decide among four courses of action. First, do nothing (~ X, ~ D), or not attempt to preempt or increase defenses. Second, only increase defenses (D). Third, both initiate preemptive measures and defensive measures (X, D), and, fourth, only begin preemptive operations (X). There are costs and benefits to all four courses of action.

The familiar aphorism "not to decide is to decide" is true in Stalker. Following perception of Red activity at node 1, Blue may decide to take no action, thus adopting the decision path from node 2 "~ X, ~ D." The Blue decision to take no action may be to avoid signaling Red that Blue has perceived its activity, the inability of Blue to take action, the abeyance of action due to the ambiguity of Red's action, or the failure by Blue to be aware of what its perception of Red's action actually means. Blue remaining passive lessens transmission of any signal to Red, which is an advantage. However, the cost is exacted in terms of Blue's preparation for conflict.

[21]Robert Axelrod, "The Rational Timing of Surprise," *World Politics*, Vol. 31 (January, 1979), p. 246.

In the first event where Blue takes no action to avoid signaling Red, this makes sense if Blue is confident that it will be able to intercept Red's later activity at will. Calculations of timing, reliability of surveillance, capability of rapid action from a no-notice force posture, and other considerations will be analyzed by Blue should it take this decision. The deferred payoff may be that Red is later caught in a more disadvantageous position, and Blue does not want to compromise this future opportunity by taking action it believes Red could, in turn, perceive and potentially cause it to abort its operation.

Another reason that Blue may take no action is because it is incapable of action. Resource constraints, lack of time, jurisdiction boundaries, and other factors may inhibit Blue from acting. In this event, Blue still has knowledge of Red's preparation and is thus forewarned. This may be of limited advantage, but it is still a payoff of perceiving Red's action at node 1, even if not followed by Blue action.

The third instance when Blue may not act is when Red's activity is so ambiguous that acting would be irresponsible. By holding action in abeyance, Blue does not incur costs associated with activity, but has realized a benefit of early warning, albeit ambiguous. The forewarning, as in the above two instances, also serves to increase the probability that later Red activity, specifically reconnaissance, will be perceived.

Lastly, Blue may take no action following perception of Red's action because it does not recognize or understand Red's activity. Blue may be unable to comprehend the activity of an emerging threat, whether due to conceptual limitations of the paradigm underlying policies and standard operating procedures, unfamiliarity with the threat, or due to a first-time encounter with a novel method of operation.

Blue may elect to increase its defensive posture, and nothing else. This allows Blue to achieve the benefits of early warning, as well as take action to mitigate a potential strike by Red. This course of action potentially has the advantage of less resource requirements compared to either preemption or a dual strategy of preemption and defense, because defensive activity is often less resource intensive than offensive operations. If Blue can increase its defensive posture without signaling Red, then Blue also accrues the advantage of Red possibly being unaware that it has been discovered. This could make surprise of Red later easier, and potentially a bigger payoff.

Blue may choose to both increase its defensive posture and to initiate offensive operations aimed at preempting Red. This is the most resource intensive course of action and the most likely course of action to result in signaling Red of its compromise. However, this also serves to increase the deterrence effect, which may result in Red's recalculating the costs and benefits of continuing against Blue. It also is the most likely course of action to defeat and eventually neutralize Red. As will become evident in the analysis of Stalker, only offensive action by Blue can defeat Red. This is because Red, in the absence of Blue offensive activity, retains the initiative throughout the game.

The last course of action available to Blue from node 2 is to pursue a strategy of pure preemption. This may be the preferred course of action because Red would perceive heightened security resulting from an increased defensive readiness, and thus Blue would lose the advantage of surprise. By keeping the defensive conditions that Red can observe static, Red may be convinced that it has not been discovered. This allows Blue to plan and execute a more robust preemptive strike, while maintaining the advantage of surprise. Although it accepts risk that Red may strike an unfortified sector of Blue before Blue can preempt, it does so to maximize the probability of success of the preemptive strike.

Having been forewarned by perceiving Red at node 1, Blue can increase its surveillance activity to ensure it observes Red's anticipated reconnaissance activity at node 4. Although this is not a certain proposition, as Red may conduct its reconnaissance without detection, the probability of Blue observing Red's reconnaissance is increased due to the early warning derived from node 1.

At node 3 Red faces a decision point. Red may choose to conduct reconnaissance, not conduct reconnaissance, or to withdraw from the game. Red may or may not possess better intelligence at node 3 than it had at node 0. If Blue has taken action, specifically increasing defenses or setting into motion a preemptive strike, and Red perceives Blue's activity, then Red will factor this into its decision calculations. If Red believes it remains an uncompromised, anonymous actor, it could conclude that Blue's activity may have been triggered by Red's latent operation's signature without actually compromising Red's identity, or it may be due to a coincidental endogenous Blue decision to act that was not triggered by Red's operations at all. The key factor in Red's decision calculations is the preservation of anonymity.

Red wishes to remain anonymous because an anonymous actor is immune from direct retaliation. Anonymous threats cannot be efficiently targeted offensively, because their identity and location are unknown. An actor of unknown identity and location could possess any traits or

characteristics, and Blue cannot precisely target what it cannot identify. Anonymity confers effective immunity from attack. Blind, mass retaliations against populations or classes of actor may inflict damage on Red, but it will be at Blue's significant cost of alienating large numbers of Others who until that point had been uninvolved. An example is the blind retaliation of destroying a village to target a handful of guerrillas suspected of living in the village. In any event, this study concerns the protection of US critical infrastructure, and the United States as a matter of security policy would not pursue such blind retaliation using force. Surveillance and other measures short of force can be legitimately employed against entire populations or classes of actor, however, and this would also constrain Red from complete freedom of action. For this reason, although Red will remain relatively invulnerable as long as it is anonymous, it would prefer that its activity not be perceived at all.

Should Red withdraw from the game at node 3, it will, provided it has remained anonymous, retire into a safe existence. It will have accrued the benefits of preparation for attacking Blue, and based on the traits of the means acquired, this preparation may have significant longevity. Given that Red has remained anonymous, it has only incurred the costs associated with its preparation and accrual of means. By withdrawing Red does not necessarily forego any future attacks of Blue. Should Red decide after withdrawing at node 3 that it wishes to pursue attacking Blue, it can re-start the game of Stalker at node 0, and based on its previous preparations may not require a significant preparatory effort, with a consequent lessening of vulnerability to discovery at node 1 during the second iteration of play.

Red may also choose the "not reconnaissance," or "~ N," course of action. This course of action places Red into Plateau 1: Hold Reconnaissance & Continue Preparation. Red can remain in this plateau indefinitely, preparing for subsequent reconnaissance at a later time. This has the net effect of being a planning, recruitment, training, and logistical support and acquisition plateau for Red. Plateau 1 is subject to Blue perception at node 1.

Should Red choose to begin reconnaissance operations, or the "N" course of action, it will move through node 4, thus giving Blue its second and last chance to perceive Red as a threat before Red has the opportunity to strike. It is important to note that preparation and reconnaissance, although sequential in start points, are not mutually exclusive. Both preparation and reconnaissance can occur simultaneously. Should Red continue preparation during the reconnaissance stage, Blue will have two nodes active and potentially capable of providing early warning, nodes 1 and 4. If Blue fails to perceive Red's reconnaissance at node 1 and node 4, then Red is potentially capable of mounting a strike against Blue without risking preemptive action by Blue, dependent on timing.

If Blue perceives Red's reconnaissance at node 4, then at node 5 Blue confronts the same menu of courses of action as it did at node 2: do nothing (~X, ~ D), defend (D), preempt and defend (X, D), or simply preempt (X). However, if Blue perceived Red's preparatory efforts at node 1, then at node 5 Blue may have increased its readiness, hence probability of success in either defensive or preemptive efforts due to the time afforded by early warning for planning, deployment of sensors, movement of forces, reinforcement of systems, and other efforts. Any action by Blue at node 5 can be improved by prior activity initiated at node 2, assuming Red did not detect it and take countermeasures or radically alter its operational techniques.

Under this scenario, Blue may have prepositioned a preemptive strike that is triggered by the sensing of reconnaissance by Red at node 4. Successful preemption, either from node 2 or node 5, shortcuts all intervening nodes and transitions the game directly to node 10. Node 10 is a "nature's turn" event that determines the success or failure ("E" or "~ E") of a Blue preemptive strike. Should the preemptive strike be effective, then Blue "wins the game," the game terminates at node G_{12}, and Red is defeated, and perhaps neutralized, as a threat. Should Blue's preemptive strike be ineffective, then Red retains the initiative of action, and could transition into mounting its own strike at node 6, exist in Plateau 6: Ineffective Retaliation, or simply withdraw from the game.

A disadvantage of Blue pursuing the strictly offensive course of action of a preemptive strike is that if Blue incorporated a defensive course of action, then Red may have been deterred from striking. Deterrence of Red is a factor in play in the game of Stalker until node 6, after which Red strikes and, by definition, is not deterred. By mounting a pure preemptive strike course of action from either node 2 or node 5, Blue abandons the possibility of a defensive course of action deterring Red from attacking. However, this is a very limited disadvantage. Red as an anonymous actor deliberately conducting first preparation, then reconnaissance is a malicious actor "stalking" Blue, hence the name of the game "Stalker." Even if deterred, there is no guarantee that Red will not continue to stalk Blue in the future. Only neutralizing Red removes it from future iterations of the game. Defensive courses of action that deter Red are only deferring conflict into the future. Deterring Red only defers conflict to a future iteration of the game; it does not eliminate the possibility of conflict with the same Red actor. Deterrence through defensive measures may serve to not only warn Red, but allow it to attack more intelligently in the future, perhaps with greater strength.

The advantages of preempting Red are several. Red is neutralized as a threat, which can only be accomplished through offensive means. Red is denied the opportunity from node 6 through node 9

of accruing payoffs at Blue's cost. Blue possesses at node 5 the best chance of success for a premeditated offensive operation, because Blue's defenses, systems, and forces have not yet been attacked and potentially degraded. The game of Stalker strongly shows that Blue, if capable, should always preempt Red. Red does not gain any additional absolute capabilities should Blue's preemptive strike fail, and the payoff is large for a successful Blue preemptive strike. The only exception would be if a preemptive strike would deplete Blue's resources for defensive measures in the event of failure of the preemptive strike. This would serve to make a preemptive strike a high-risk course of action.

At node 6 Red has three courses of action available. First, Red can withdraw before it launches an attack, thus securing all payoffs accrued from preparation and reconnaissance. Second, it can choose not to strike, or "~ S," and so place itself into Plateau 2: Hold Strike & Continue Preparation & Reconnaissance. This has the effect of maintaining the capability to strike Blue at will and perhaps with little or no delay, while continuing to increase the strike's potential effectiveness by both additional preparation and reconnaissance. The possibility of Blue discovery of Red at node 1 and node 4 persists in Plateau 2.

At this point, Red may even possess the capability to deter Blue. Chapter two's example of Chechen separatists targeting Izmailovski Park in Moscow using Cesium-137 is one such attempt at deterrence using WME.[22] Similarly, a Red actor could emplace throughout the United States devices designed to disperse radioactive agents on remote command. Such devices would not require the destructive effect of a large bomb. Their design is intended to make consequence management and clean-up a very expensive operation, potentially render unusable the area in which they are employed, and panic a population. If shielded, they would be difficult for Blue to locate until they were activated and actually dispersing their contents.

Further developing this hypothetical scenario, three devices constitute the minimum capability for Red to possess as a functionally adequate deterrent option. For Red to develop a deterrent capability over Blue, the first device would be emplaced, but its location made known to Blue. Following Blue discovery and analysis of the first device, the second device would be detonated to demonstrate Red's will to employ the capability. Following this strike, Red would make known to Blue in credible fashion, perhaps using a photo that has a confirmable date of creation that follows the second device's employment, the existence of at least one more device. Red could then make demands.

---

[22] Jessica Stern, *The Ultimate Terrorists* (Cambridge, MA: Harvard University Press, 1999), p. 67.

This scenario represents a plausible deterrence of Blue by Red's development from node 0 to node 6 of a course of action.

The third course of action available to Red at node 6 is to strike Blue, or "S." Exercising this option, should the above hypothetical scenario of Red developing a deterrent capability be in play, Red will ensure through signaling that Blue recognizes it is the actual Red actor conducting and responsible for the operation. This action will ensure that Blue "perceives" the existence of the first device and the employment of the second device at node 7. The desire of Red to achieve a deterrent capability over Blue thus negates the possibility of Plateau 3: Undetected Strike, as well as surrenders to Blue knowledge of Red's existence, although not necessarily Red's identity.

Should deterrence of Blue not be the objective, Red will strike and Blue will have the opportunity at node 7 to perceive ("P") or not perceive the strike ("~ P"). If Blue fails to perceive that Red has attacked, this allows Red to continue its strike as a series of attacks in Plateau 3: Undetected Strike. An example would be the hacking of a bank's account databases. If undetected, Red can continue to "strike," in this case transfer funds, until Blue recognizes it is under attack. Dependent on the type of attack, Blue may have little time to perceive Red's strike. In the case of cyberstrikes, Blue's window for perception may be only seconds, literally. Should Red be successful and withdraw from the game, Blue's later discovery will be typified by an *ex post facto* analysis and forensic examination of its computer network. Should the strike's effects be below Blue's threshold of sensing or Red's signature erased or concealed, it may never be discovered. At node 7 Red has a decision point whether to persist in attacking, or to cease operations and, in effect, "quit while ahead."

At node 8 both Blue and Red face decisions. Given that Blue perceived Red's strike at node 7, at node 8 it must take a decision to respond ("R") or not respond ("~ R"). The decision to not respond would result in Plateau 4: Unresponsive Target. Blue may choose to not respond based on a number of factors. The threat posed by Red's strike may be negligible, and may even serve to provide Blue with cost-free systems testing and training opportunities. This level of threat would be analogous to automated port scans of a corporate network by unskilled hackers. In such cases, response by Blue is not cost-effective. Alternatively, Blue may lack the capability to respond. This decision by Blue allows Red's continued attack of Blue, albeit not yet effective, along the dual Red and Blue track of potential simultaneous activity that started at node 7 and continues through node 10.

Red also faces a decision at node 8. Red must evaluate whether, in light of Blue's perception at node 7, continued operations are still desirable, or if they have now become too risky.

Should Red determine that continuation of attack is not worthwhile, it will withdraw from the game. The net effect, if successful in withdrawing without continued engagement by Blue, is to have developed a capability and employed it, accruing all payoffs, without costs inflicted by Blue. At node 8 Red's withdrawal potentially constitutes a successful attack and clean escape.

At node 9 Blue and Red again face decisions along the dual track of simultaneous activity that started at node 7. Red must decide whether to continue its attack or withdraw. Blue must take the decision to either respond offensively or defensively. Should Blue decide to respond defensively, Plateau 5: Defensive Target is in play in the game. This plateau makes Blue essentially a passive actor, with Red possessing the initiative in conducting attacks. Should Blue at node 9 decide to conduct offensive operations, the game progresses to node 10.

At node 10 Blue's offensive operations will either be effective ("E") or not effective ("~ E"). If effective, Red is defeated and perhaps neutralized as a threat; this terminates the game at node G_{12}. If Blue's offensive is not effective, Red can persist in its operations within Plateau 6: Ineffective Retaliation. Until Blue mounts an effective offensive operation, Red retains the initiative along the dual track of potentially simultaneous activity. Plateau 6 affords Red the opportunity to repeat strikes, damaging Blue, while Blue attempts to recover its systems and mount an effective retaliation.

At node 10 Red again must decide whether to continue its operations. Based on the character of Blue's offensive operations, Red may have a small or large window of time to make this decision. As noted above, in the case of a cyberstrike by Blue, the window may be measured in seconds.

Importantly, although described above in a deliberate fashion, the time that elapses from node 6 to node G_{11} or G_{12} may only be a few seconds. A cyberstrike by Red against Blue at node 6 may succeed almost instantaneously, with the intervening nodes and their corresponding decisions being traversed faster than human reaction can occur. Based on this characteristic of a cyberstrike, both Red and Blue may design and employ automated processes that notify a human analyst, but have operational authority to implement courses of action and take decisions based on pre-defined parameters. In such a scenario the outcome of conflict may be determined before humans are aware that there exists a threat. If Red was to determine during its pre-strike preparation and reconnaissance what the specific Blue parameters for automated decisionmaking were, it would be able to tailor its strike at node 6 to defeat Blue without even human awareness of the strike.

The attack model network describing Simple Conflict is rich in significance for understanding emerging threats. It requires policymakers and strategists to employ a new framework – the Red, Gray, and Blue framework – as well as a typology of emerging threats that is not based on a state-centric perspective. This typology is described in the first section of this chapter in a disciplined, functional manner. For knowledge to progress and aid in the development of functionally adequate models that can be employed as intellectual tools, it is necessary to explicitly define and explain the terms and the structure of generic case models. The above discussion of the Simple Conflict model is a contribution that analysts can modify for a specific case and employ as a template for formulating intelligent policies to counter emerging threats to critical infrastructures and population.

The six remaining variants of the game of Stalker are depicted graphically with a brief explanatory passage below. The detailed explication of the remaining models, as well as further development of all seven generic models will be accomplished in a forthcoming work, as the scope of a detailed study of the Stalker game is beyond the purpose of this study. This presentation of the Simple Conflict attack model network has served to provide not only the foundation for the variants, but to extend this study's discussion of a new national security policy framework from the paradigm level to the level of generic case model, including the precise use of terms and the detailing of a typology of emerging threats. This serves as a more rigorous contribution to the efforts to understand the current security environment and the national security challenge of protecting critical infrastructures and populations from emerging threats than is typical in the literature to date.

Ganging Up on Blue:

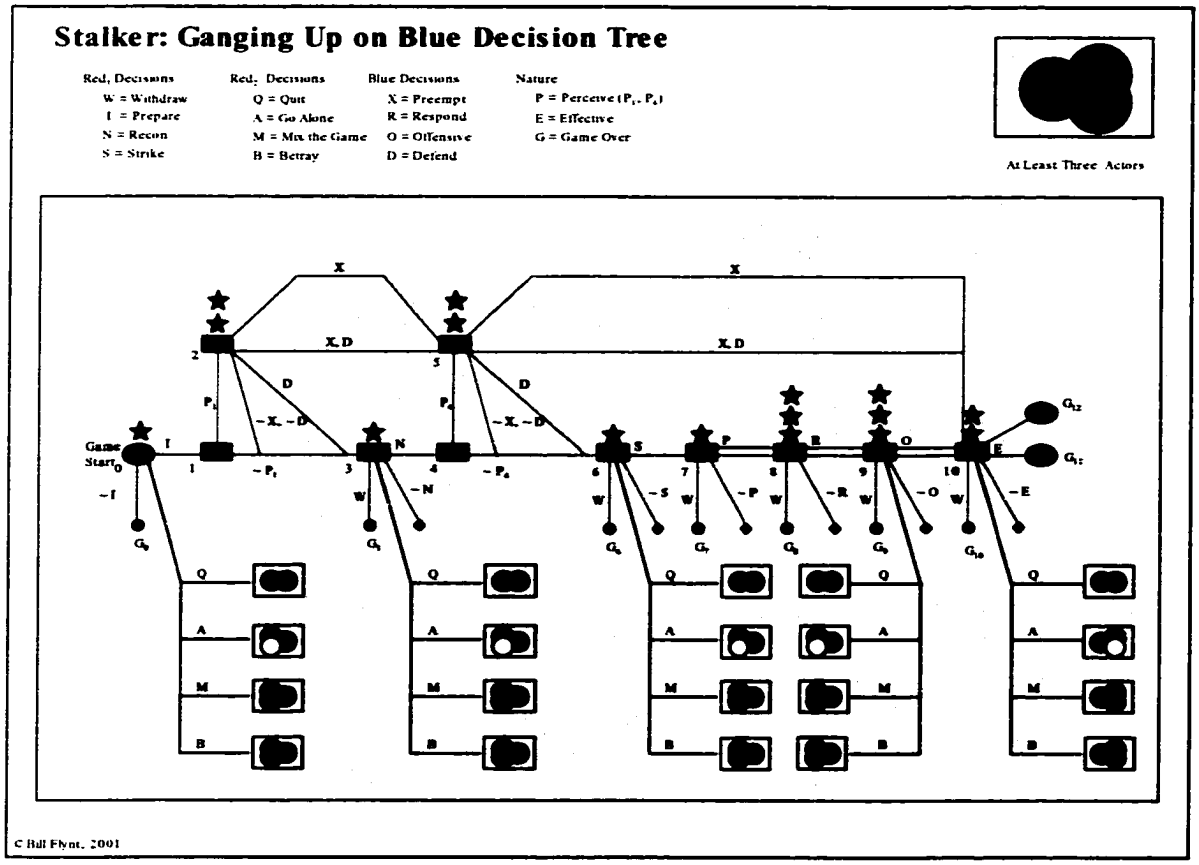


Figure 4 – 2: Ganging Up on Blue Attack Model Network

The Ganging Up on Blue decision tree requires at least three actors: two Red and a Blue. It is the first variant where transition between worlds becomes possible. For example should Red_2 exercise any of its four possible options at nodes 0, 3, 6, 9, or 10, the game will transition from a Ganging Up on Blue model to a different model.

Both Red_1 and Red_2 in this variant act in concert. Red_1 for the purpose of convention is the main threat protagonist, and Red_2 is the threat actor facing decision points that could transition the game to a different variant. These decisions are Quit, Go Alone, Mix the Game, and Betray. The resulting worlds, respectively, are Simple Conflict, Factions, Mixed Game, and Ganging Up on Red.

Behind each of the different variants' icons shown in Figure 4 – 2: Ganging Up on Blue is that variant's attack model network. The location along that underlying variant's network the conflict

transitions to depends on where the Red_2 decision to transition to that world was made on the current network. For example, if Red_2 decides to Quit at node 0 on the Ganging Up on Blue decision tree, then the corresponding location of the conflict for the next world's network will be node 0 of Simple Conflict, with Red_1 deciding whether to initiate preparation or not.

Third Actor Escalation is possible in any world consisting of more than two actors. The black stars depict opportunities to exercise TAE in an attempt to split the two Red actors.

Ganging Up on Red:

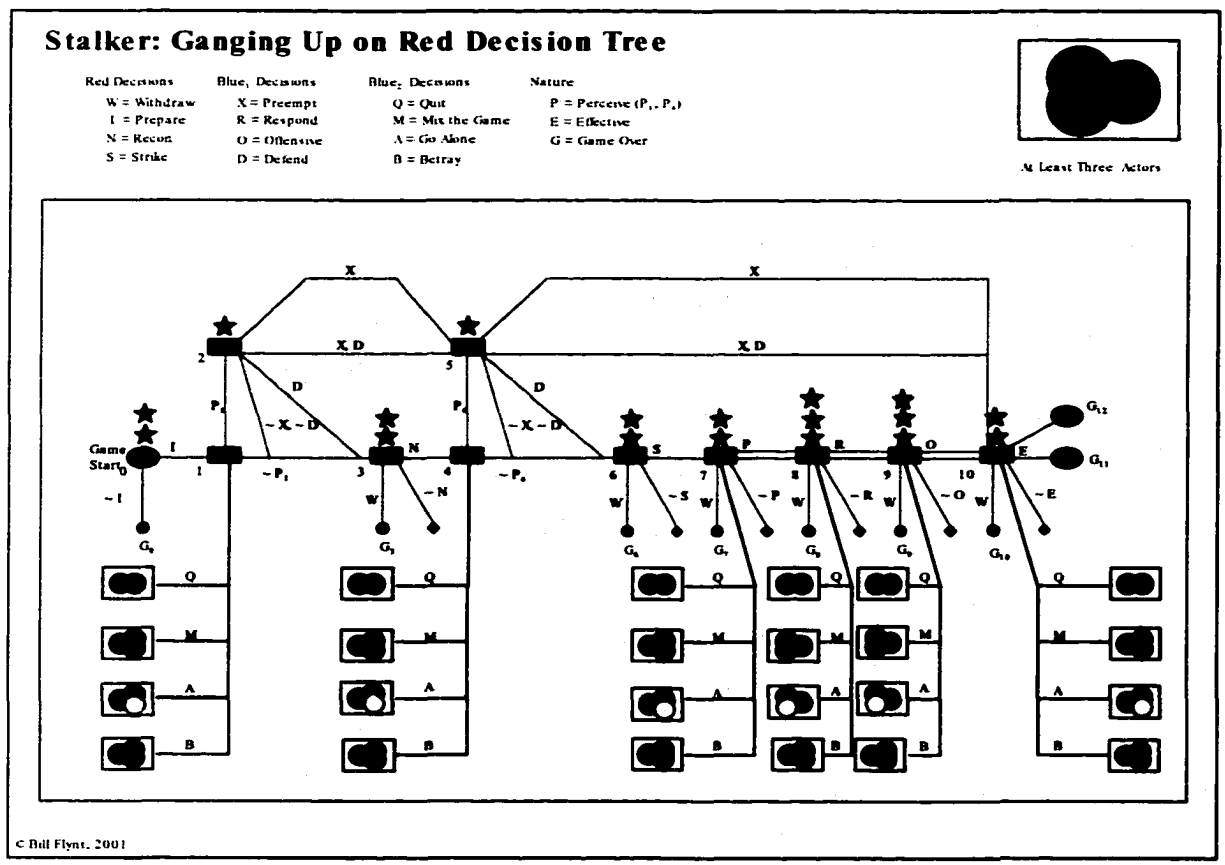


Figure 4 – 3: Ganging Up on Red Attack Model Network

The Ganging Up on Red attack model network requires at least three actors. It is similar to the Ganging Up on Blue variant, with $Blue_2$ exercising the power to transition the conflict to a different world.

The decisions that can be exercised by $Blue_2$ are Quit, Mix the Game, Go Alone, and Betray. The corresponding worlds resulting from these decisions are, respectively, Simple Conflict, Mixed Game, Factions, and Ganging Up on Blue. These decisions are similar to Red_2's decisions in the Ganging Up on Blue world, however, the second and third decisions are reversed in sequence. This connotes that Blue will transition to a Mixed World before becoming an independent threat actor in a Factions world against $Blue_1$.

As in any world with more than two actors, TAE is possible. The black stars depict where Red will attempt to split the Blue actors.

Alliances:

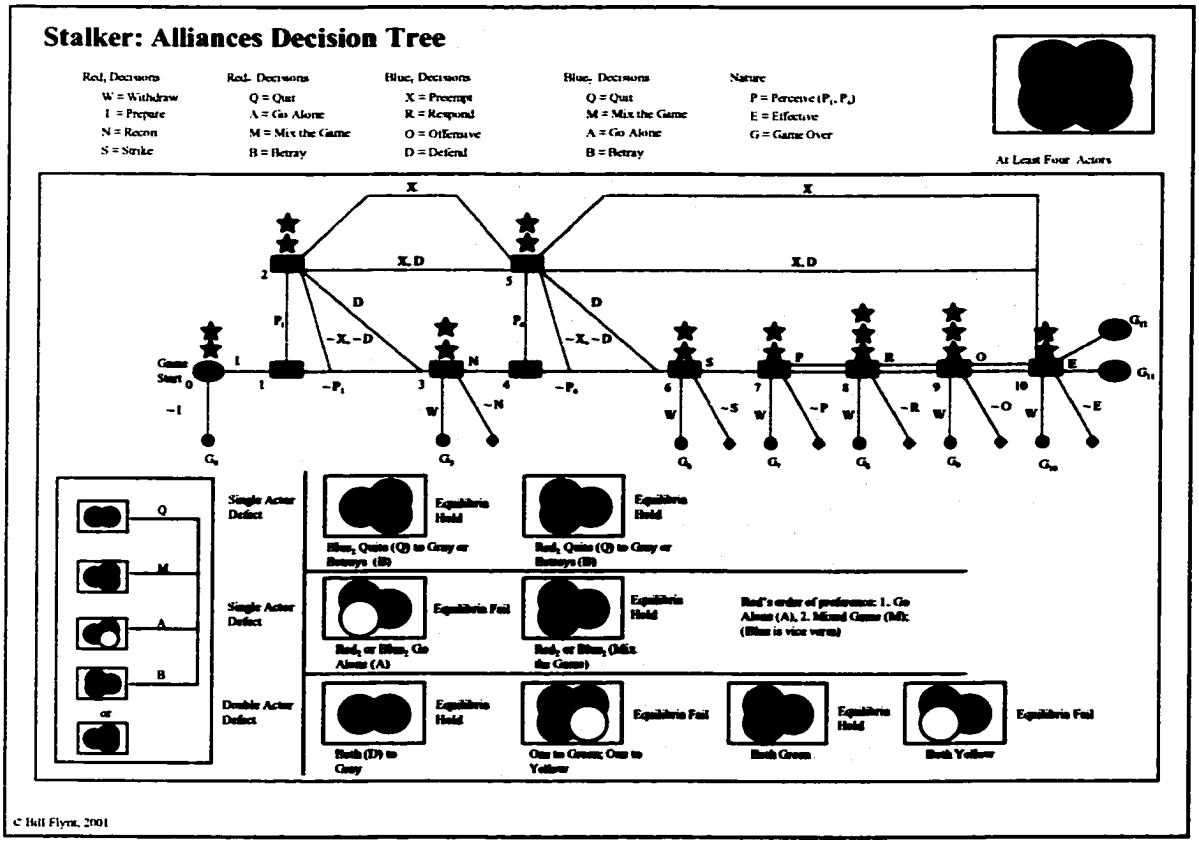


Figure 4 – 4: Alliances Attack Model Network

The Alliances variant requires at least four actors in two camps. During the conflict both Red_2 and $Blue_2$ will face decision points to Quit, Mix the Game, Go Alone, or Betray, as discussed above.

Additionally, both camps will attempt to split the opposing camp's actors through TAE. This world is more complex than the three actor worlds, because either one or both of the supporting actors may exercise an option to change the structure of the world of conflict.

Should a single actor defect, the resulting worlds will be either Ganging Up on Blue or Ganging Up on Red, with the first resulting from a Blue actor defection and the second from a Red actor defection. Here defection corresponds to the Quit decision of Red_2 and $Blue_2$.

Should a single actor defect exercising the Go Alone or Mix the Game options the resulting worlds are Factions and Mix the Game. Red_2's preference is to first Go Alone, then Mix the Game. $Blue_2$'s preference is reversed.

In the case of double actor defections, should both Red_2 and $Blue_2$ Quit, the world of conflict reduces to Simple Conflict. Should one actor declare neutrality, and the other Go Alone, the resulting world is N-Actor. Should both actors Quit or Go Alone the resulting worlds are Mixed Game and Factions, respectively.

Factions:

The variant of Factions requires at least three actors. In this world Blue is confronted with two threat actors that are unaligned. The TAE black stars correspond to efforts by each actor to foment conflict between the other two actors. This world can transition to four other world types: Simple Conflict, Ganging Up on Red, Ganging Up on Blue, or Mixed Game.

Should Yellow or Red be neutralized, the world of conflict reduces to Simple Conflict. If Yellow allies with Blue, then the world transitions to Ganging Up on Red. Should Yellow ally with Red, however, the variant becomes Ganging Up on Blue. Finally, if Yellow declares neutrality the game becomes the Mixed Game variant. Of course, either Yellow or Red could declare neutrality, but for the sake of convention the Red actor is always viewed as the primary opponent, with the secondary threat or Other being capable of change.

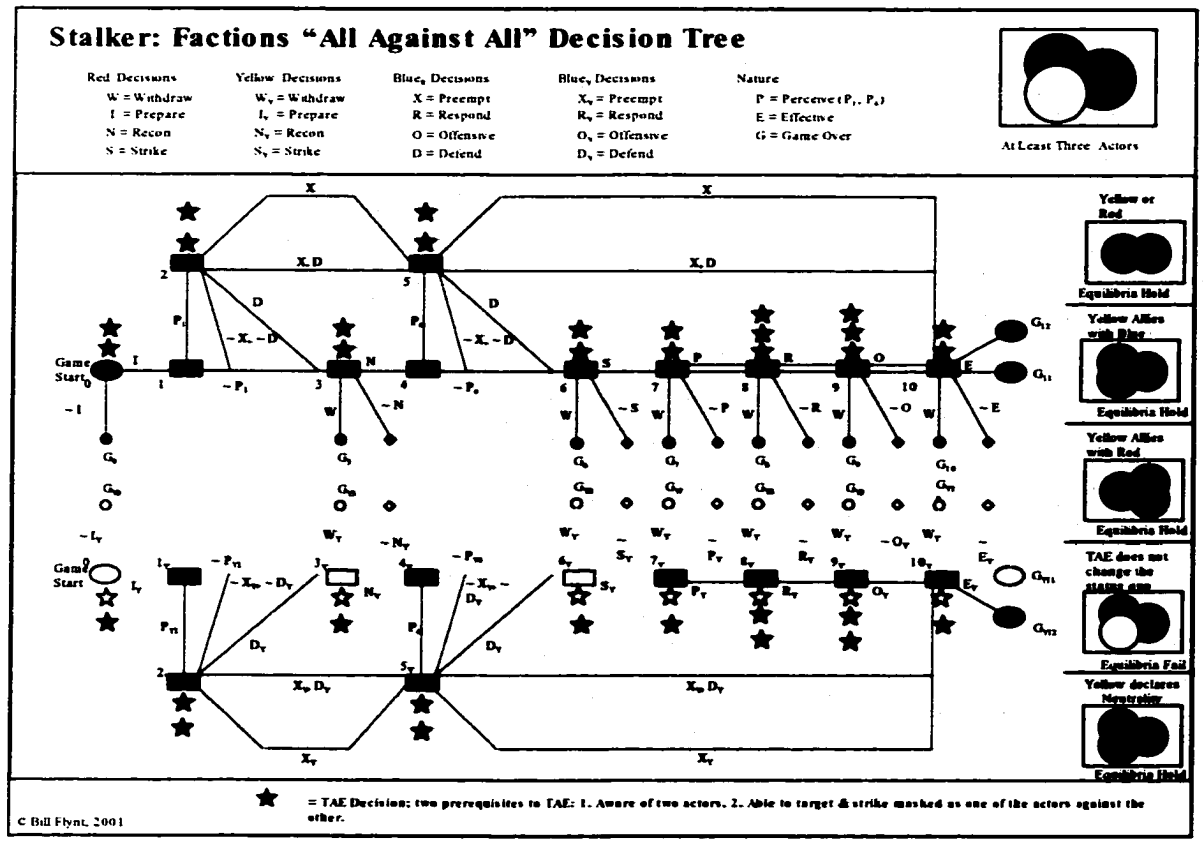


Figure 4 – 5: Factions Attack Model Network

From Blue's perspective there exist four outcomes of TAE or negotiations within the Factions model. These are: Ally with Yellow, resulting in a Gang Up on Red world; Negotiate Yellow to Gray, resulting in a Simple Conflict against Red; Negotiate Yellow to Green, with a resulting world of Mixed Game; and, finally, persisting in a Factions world.

Within this last outcome, the continuation of a Factions world, there are three variants that from Blue's perspective are in order of preference: Two Against Red, All Against All, and Two Against Blue. In each of these worlds, Blue will, respectively, take the following actions: Negotiate with Yellow to move to a Ganging Up on Red world; Employ TAE to move Yellow to negotiations; and employ TAE to incite fighting between Yellow and Red, move to All Against All, or absent a Yellow-Red dyad fight two games of Simple Conflict.

Mixed Game:

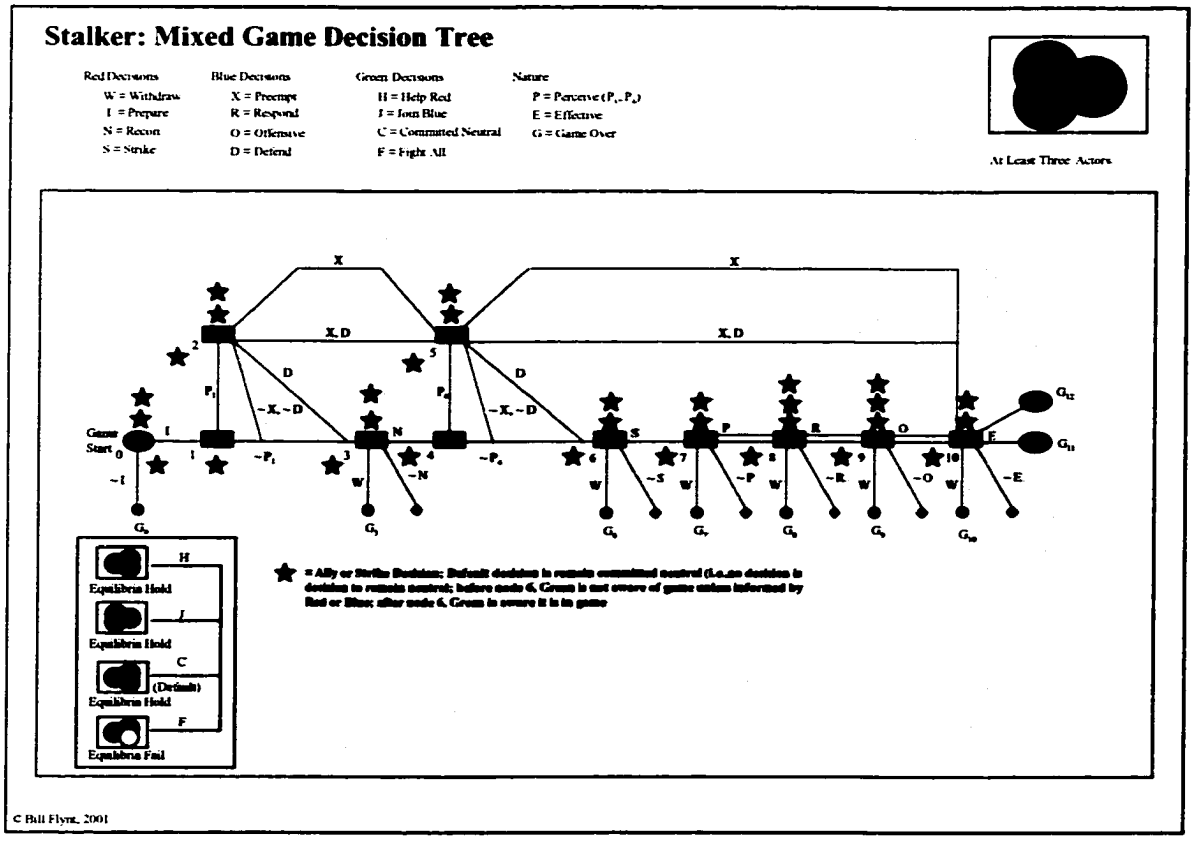


Figure 4 – 6: Mixed Game Attack Model Network

The Mixed Game variant is essentially Simple Conflict, with the addition of a neutral actor that may become involved in the conflict. Green is the neutral actor. Green faces four decisions: Help Red ("H"), Join Blue ("J"), remain Neutral ("C"), or Fight All ("F").

From these decisions three other worlds of conflict can be transitioned to: Ganging Up on Blue, Ganging Up on Red, and Factions. The Ganging Up on Blue world results from Green's decision to Help Red. The Ganging Up on Red world results from Green's decision to Join Blue. Factions results from Green's decision to fight both Red and Blue.

N-Actor:

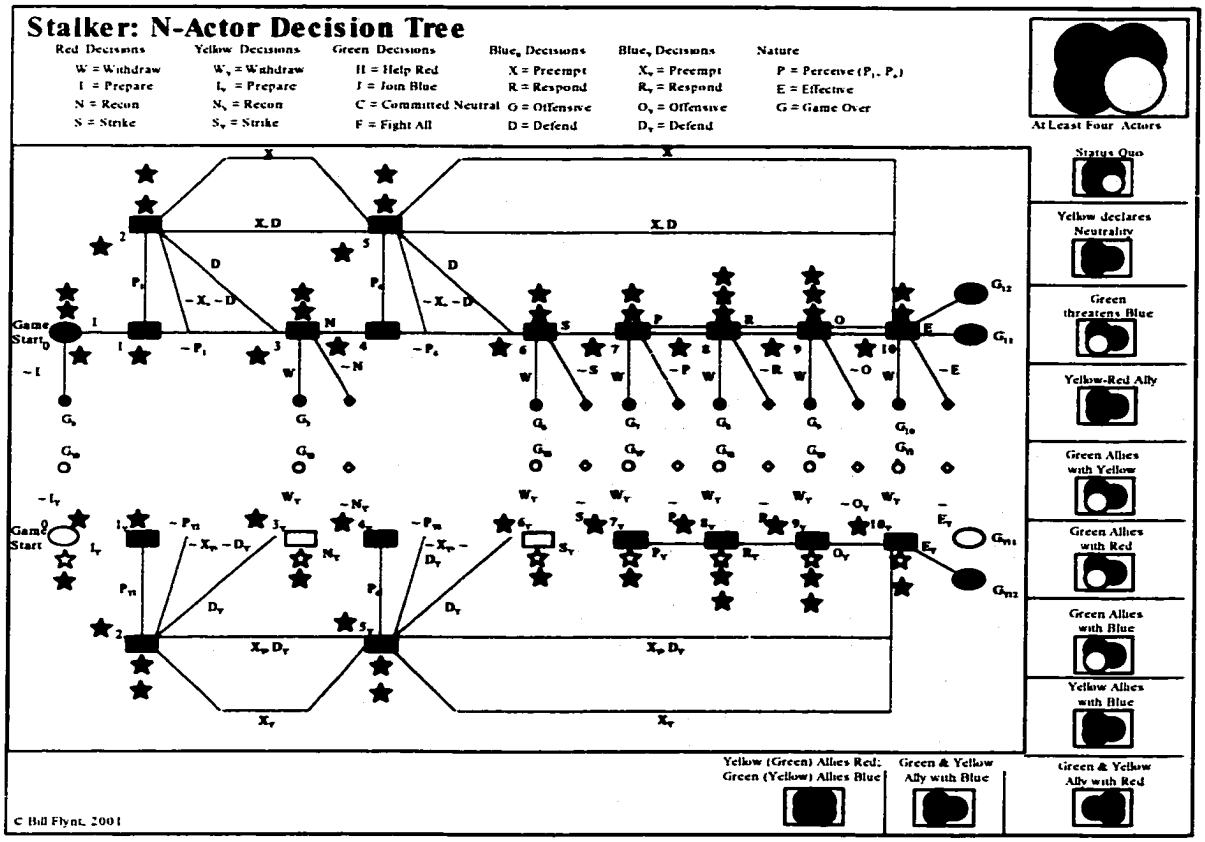


Figure 4 – 7: N - Actor Attack Model Network

The N – Actor variant requires at least four actors. This is the most complex of the worlds, with each actor potentially transforming the world of conflict into a different variant at each step in the chain. In similar fashion as the other variants, the possible resulting worlds coming from the conflict are shown as icons along the right and bottom edges of Figure 4 –7: N – Actor Attack Model Network.

In an N – Actor world, Blue must simultaneously fight two unaligned threat actors, Yellow and Red, as well as attempt to gain the support of Green, the neutral actor. There exist eleven permutations of this game resulting from various decisions by the actors.

Conclusion:

The purpose of this chapter has been to provide concepts and intellectual tools below the level of abstraction of paradigm, theory, and model. To this end it has explicitly defined terms and depicted in attack model networks varied relationships of actors involved in different worlds of conflict. It has followed Bacon's dictum that clarity is achieved through explicit contributions that are vulnerable to constructive criticism.

However, the chapter is not an exhaustive treatment of the concepts and models it has outlined and presented. That task exceeds even the scope of this study, and itself deserves a separate major study. However, to have left this study's discussion of the altered security environment at the level of abstraction of paradigm would have been to miss the opportunity of demonstrating through concrete, explicit generic case models and a threat typology how analysis of the security environment should proceed. It would have been equivalent to failing to articulate a Lakatosian positive heuristic, or an alternative in a Kuhnian sense to an existing community framework's models.

The net effect has been to drill the Red, Gray, and Blue framework down from paradigm and theory to model, generic case, typology, and terminology. This demonstrates that the Red, Gray, and Blue framework is not only a relevant strategic paradigm but is also capable of scalable application down to the tactical level. Nevertheless, this chapter remains only suggestive of how far these concepts and models can be made explicit and even modeled mathematically. Policymakers and strategists can apply the concepts of this chapter as a template to a specific context, and with modification develop a context specific model of a particular conflict that can then be coded and developed into computer simulations. The *sine qua non* for developing such models is a formally articulated typology of emerging threats and an explicit structure of attack model networks defining the conflict. Without such intellectual tools and concepts, the study of emerging threats targeting critical infrastructures and population cannot depart the realm of theory and philosophy into the world of application by practitioners. Simply put, only concrete models and typologies can bridge George's gap.

Chapter Five: Conclusion

In dim eclipse, disastrous twilight sheds
On half the nations, and with fear of change
Perplexes monarchs.
~ Milton, *Paradise Lost*

This study has argued that US national security policies designed to counter emerging threats are flawed, because they rest on an inappropriate theoretical framework. The past framework provided a perspective of the security environment through the lenses of the sole remaining Superpower; it perceived a world comprised of states largely basking in the triumph of democratic values. Exhilarated by the surprise end of the Cold War, policymakers' Blue (Self)-centric framework fueled a quixotic belief that the promise of idealism might prevail. The National Security Strategy itself was branded *A Strategy of Engagement and Enlargement*, emblematic of the proposed teaching and expansion of a progressive worldview. A shared belief in a benevolent American hegemon instructing the world in capitalism and representative government exerted a deep hold on the national security elite's collective mind. In the face of anomalies like the World Trade Center bombing, Aum Shinrikyo's sarin gas attack, the Oklahoma City bombing, and the Khobar Towers bombing they failed to realize that the conduct of conflict in the world political system had changed. Their security policy efforts became "a strenuous and devoted attempt to force" that conduct of conflict into their conceptual boxes.[1] At the end of its second term the Clinton Administration had experienced a string of national security policy failures from Somalia to Haiti to Oklahoma City.

A nascent consensus in the national security policy community is emerging, as evidenced by recent legislation, hearings, and other initiatives, that the past framework and the *ad hoc* policies and outmoded institutions crafted within its pale are no longer functionally adequate. No longer articles of faith, they are the vestiges of a past era. A Kuhnian paradigmatic crisis is in full bloom, but a new paradigm has not yet emerged as a collective belief. Nevertheless, there now exists a growing revolutionary activism within the national security elite that embraces Lakatos' view:

> The idea that we live and die in the prison of our 'conceptual frameworks' was developed primarily by Kant; pessimistic Kantians thought that the real world is for ever unknowable because of this prison, while optimistic Kantians thought that God created our conceptual framework to fit the world. But *revolutionary activists* believe that conceptual frameworks can be developed and also replaced by new,

[1] Kuhn, *The Structure of Scientific Revolutions*, pp. 4-5.

> *better* ones; it is we who create our 'prisons' and we can also, critically, demolish them.[2]

This study adopts Lakatos' revolutionary activists' view that the United States national security elite can critically demolish the old paradigm, and invent a *better* framework for the formulation of policies countering emerging threats. It agrees with Kuhn that during a paradigmatic crisis the old paradigm must be destroyed if it is to be replaced. The issue of critical infrastructure protection against emerging threats is at the national level of punctuated, macro-level politics as detailed by Baumgartner and Jones' PE theory. This study has attempted to make a contribution to the end of destroying the old paradigm and calling into question existing policies and institutions. It presents and argues "a *better* framework" – the security environment approach of the Red, Gray, and Blue framework – from the paradigmatic level of abstraction "drilled down" to decision trees of generic case models of conflict. This argument has been developed in explicit terms to attract criticism, believing Bacon's dictum that progress is furthered by clarity that allows criticism, not confusion, of concepts.

In a broad historical context the passing of eras is precedented. Following the end of World War II Kennan provided the gift of an epiphany to the US national security elite, and his vision shaped the strategic framework of the Cold War. It is not surprising that the end of the Cold War marks a similar punctuation of the paradigmatic equilibrium. Unfortunately, there has been no epiphany and ten years after the end of the Cold War the world political system is not brought into focus with any of the conceptual lenses that served to view the stark black – white of that bipolar system. The environment has faded to Gray, and the actors within it have lost the sharp distinctions of past definitions of enemy and ally. Kennan's epiphany was for a simpler time.

Paradigm is the foundation of theory, and theory is the foundation of policy. In the absence of a relevant paradigm, accurate theory cannot be developed. This chain flows from paradigm through theory to models and, ultimately, policies. In light of the catastrophic, demonstrable failures of policies to counter emerging threats, efforts to "fix" policies and institutions are wrong-headed. Such an approach has the net effect of doing the wrong thing better. Change must begin at a more elemental level with a critical examination of paradigm. From a relevant, explicit paradigm will flow the intelligent formulation of national security policies. Paradigms, theories, and models are all intellectual tools and not articles of faith. When they no longer apply to a changed reality they must be replaced. Policymakers, because they have not yet "demolished" their paradigmatic "prisons" have not escaped their "conceptual boxes," hence policies remain that are anchored in an outmoded framework.

---

[2] Lakatos, "Falsification and the Methodology of Scientific Research Programmes," p. 104.

This leads to the two questions that have driven this study: 1. How can we understand the changed security environment theoretically?, and, 2. What are the implications of the changed security environment for national security policies countering emerging threats? The Red, Gray, and Blue framework, explicated from the level of paradigm through attack model networks answers the first question. The second question has been answered throughout the study by discussion and example. Summarizing the essence of this discussion, national security policy must be tailored to the specific threats it is designed to counter, these threats have changed, past policies crafted for past threats must be abandoned, and new policies relevant to the altered security environment and emerging threats invented. This answer points us to the intrinsic process of a security environment approach within the Red, Gray, and Blue framework. To exercise this process first requires a complete paradigm shift, followed by the adoption of theories, models, and typologies that accord with the paradigm. These, in turn, will drive the design of national security institutions, processes, and policies, as well as order resources and priorities. The Red, Gray, and Blue framework with the intellectual tools of terms, typologies, and generic case models is a relevant paradigm that has the requisite components to bridge the gap from theory to practice. This study finds that a comprehensive change is required that will potentially rival the effects of both the National Security Act of 1947 and the Goldwater – Nichols Act of 1986, combined.

The first change required, however, is in the minds of the US national security elite; a change in what Kuhn identified as their disciplinary matrix.[3] Suppe notes that this comprises the *Weltanschauung*, or worldview, of the policymakers, and represents "an exceedingly complex entity, being approximately the whole of one's background, training, experience, knowledge, beliefs, and intellectual profile which is of possible relevance to working with a theory."[4] Kuhn notes that community members' "education is both rigorous and rigid"[5] and serves to account for the common vocabulary, beliefs, values, and models common to a community such as the national security elite. The Red, Gray, and Blue framework is this study's contribution to demolishing the old paradigm anchored in the state-centric, Cold War era.

This study questions the relevance of mainstream theories of international relations, specifically those theories anchored in a framework where states are the only actors capable of affecting influence within the world political system. Founded explicitly on a state-centric Lakatosian hard core where states are exclusively the actors that "matter," these theories now apply only in a

[3] Kuhn, "Second Thoughts on Paradigms," p. 460.
[4] Suppe, "The Search for Philosophic Understanding of Scientific Theories," p. 218.
[5] Kuhn, *The Structure of Scientific Revolutions*, pp. 4-5.

narrowly defined security environment where states are the actors capable of system relevant violence. However, that scenario no longer completely describes the world political system.

To the extent that an actor's security environment does not conform to its intellectual tools, there exists a need for new intellectual tools. Policymakers must avoid the trap of Jervis' Law of the Instrument that dictates when all you have is a hammer, everything looks like a nail.[6] Actor's other than states, for example Usama bin Laden's al-Qa'ida, now exercise real power in the world political system as well. Policymakers have received sufficient data to determine the inadequacy of the underlying theories they employ to craft policy. There is no further need for exhaustive study. Much as Copernicus apprehended the error of the Ptolemaic paradigm from a relatively small number of observations, policymakers have received sufficient indications of a paradigmatic crisis. Multiple trigger events have amply demonstrated that the conduct of conflict in the new environment has changed and emerging threats have more rapidly grasped the implications than the United States. The inertia of Kuhnian normal science remains to be cleared away before new force structures can be developed in accordance with a new framework.

This is not to say that states, and the theories that describe and explain state systems, have become meaningless. State-centric theory is not obsolete; it is, however, limited in relevance to a system where only states exercise systemic influence. But that is no longer the current world political system. As Wendt has pointed out "that simply means that state-centered IR theory can only be one element of a larger progressive agenda in world politics, not that it cannot be an element at all."[7] State-centric IR theory is still IR theory; it is just of finite relevance.

This study finds that Bull's assertion, implicitly held as a belief by those that champion state-centric approaches, that "states are not vulnerable to violent attack to the same degree that individuals are"[8] is outmoded. Bull caveated "it is only in the context of nuclear weapons and other recent military technology" that war can approximate a single blow.[9] Yet, non-state actors armed with WME approximate this context in ways Bull could not have foreseen. Summarizing this view, system level actors are states and not individuals, states are not vulnerable like individuals, and a system relevant level of violence does not consist of a single blow. This study, however, refutes this state-centric argument and asserts it is no longer tenable given the current security environment. What has changed is that individuals armed with WME technology, knowledge, and means can, in fact, affect system

---

[6] Jervis, *Perception and Misperception in International Politics*, p. 108.
[7] Wendt, *Social Theory of International Politics*, p. 10.
[8] Bull, pp. 46-51.
[9] Ibid.

relevant violence and influence, can injure states through targeting population and critical infrastructures, and can do so in a single blow.

New intellectual tools are demanded for a security environment where non-state actors, even individuals, potentially are capable of system relevant violence. The tools required span the hierarchy from paradigm, theory, model, concepts, terms, typologies, and decision trees. Anomalies can occur for a variety of reasons, but multiple anomalies in a pattern signal the inadequacy of the framework which views them as "novelties."

Concepts of "legitimate" employment of violence and "sovereignty of the state" increasingly appear as quaint relics of a simpler era. Non-state actors anonymously pursuing asymmetric strategies will ignore diplomatic protocols regarding means, targets, and borders. Under anarchy, those actors capable of employing violence have the self-ordained right to do so; those opposing such violence have the self-ordained right to attempt to stop them. From this conflict is spawned. Non-state actors, by definition, have little to no concern for the trappings of statehood, and states relying on traditional notions of international law will find that these state-anchored institutions prove a thin veil and not a shield against the attack of non-state actors.

Those skeptical of the need for dramatic change extending even to institutions anchored in the past paradigm need look no farther than the NSA. The agency's Director has admitted the agency is falling behind in keeping up with the global telecommunications revolution.[10] This is because technology is pushing innovation beyond understanding. The twin engines of Moore's Law, which states that over *n* years computing power increases by 2^Nth power, further compounded by Metcalf's Law, which states that computer power increases by the square of the number of nodes on the network, speaks volumes for the futility of attempting to gather and analyze information using outmoded approaches[11]. Not only are the nodes increasing in computational power exponentially, but the number of nodes comprising the Internet is also increasing resulting in net exponential increases in power. General Hayden's "trigger event"[12] convincing him of the need for fundamental change occurred on January 24th, 2000, when the NSA's systems, strained and running at near maximum capacity went offline for 72 hours.[13] National security policies, whether codified in physical institutional structures or in less tangible processes are breaking, literally and figuratively. This is a classic symptom of a

[10] CBS interview with Lieutenant General Michael V. Hayden.
[11] This does not even address the problems of the proliferation of strong encryption, steganography, fiber optic transmission lines, and other techniques of defeating analysis.
[12] Baumgartner and Jones, *Agendas and Instability in American Politics*, pp. 129-130.
[13] Hayden's remarks to the Kennedy Political Union.

Kuhnian paradigmatic crisis, and constitutes a Darwinian-like challenge to US national security institutions. Kuhn observes the reticence of community members to abandon their long-held paradigm is the practice of "normal science [that] often suppresses fundamental novelties because they are necessarily subversive of its basic commitments."[14]

It was not any single factor, for instance the Soviet Union's demise, that precipitated the current paradigmatic crisis. Rather, a confluence of factors has occurred to fundamentally alter the security environment to a point where the past framework is functionally inadequate to direct national security policies. The end of the Cold War and the demise of the Soviet Union freed the political forces of newly liberated societies. Unfortunately, it also freed control of the inventories, technologies, research and knowledge banks, cadres, equipment, and materials of multiple WME programs in the former Soviet Union, its client states, and abroad. Compounding this change in the security environment yet further, the scope and depth of technological innovation is expanding at an exponential rate. Advanced scientific research and development programs have transitioned from traditional centers in the United States and Europe to include newly emergent centers of science in South Asia and the Pacific Rim. The proliferation of computers has enabled the modeling of advanced scientific simulations, including nuclear weapon explosion simulations, without the prohibitively expensive and capital intensive infrastructure required of such research centers only ten years ago. The availability of knowledge has been increased with the Internet providing global access to the research and publications of advanced institutions of science. The result has been the achievement of near-parity in some areas of scientific knowledge concerning WME with the United States. Where a scientific research advantage remains is operationally immaterial. Sufficient knowledge has proliferated to enable the manufacture of WME by any actor serious about the task. Emerging threats do not need the state of the art research to mount effective operations. State and non-state actors formerly possessing only hostile intent towards the United States now also possess the means to strike US critical infrastructures and population by covert employment of WME at a "good enough" level. New threats with varied motives from diverse origins converge along separate axes toward America's center of gravity – critical infrastructure and population.

This enables non-state actors to exercise system relevant violence, and imbues them with the power of a systemic actor. As used, system relevant violence describes a level of violence, varied by case, which penetrates a threshold resulting in a change in another systemic actor's ability to exercise power. A strike that lessens an actor's ability to employ power affects that actor's capabilities in the world political system, and thus the strike is a system relevant level of violence.

---

[14] Kuhn, *The Structure of Scientific Revolutions*, p. 5.

Singer noted that the level of analysis chosen has implications for what the theory is able to describe, explain, and predict.[15] Selecting a lower level of analysis increases the descriptive richness and explanation of specific cases, while choosing a higher level of analysis increases comprehensiveness and abstraction. In his *Man, the State, and War* Waltz orders by images. In the current security environment, however, the First Image can now exert influence and shape the Second Image and, ultimately, the Third Image by using WME. Waltz's images, like Bull's anarchical society, did not account for a First Image actor armed with WME capable of exercising system relevant violence.

The net result of the emergence of non-state actors armed with WME and capable of striking the United States directly is that much of the United State's power, anchored in a past paradigm's force structure and policies, is unable to engage in conflict with asymmetric, anonymous actors. Two highly-credible studies have concluded that US power is waning as a trend. The USCNS / 21 phase III report, *Road Map for National Security: Imperative for Change* finds that "after more than two years of serious effort, this Commission has concluded that without significant reforms, American power and influence cannot be sustained."[16] The Central Intelligence Agency states an ominous finding in its report *Global Trends 2015* that in four different scenarios of alternative global political development out to the year 2015, or "alternative global futures," that "in all four scenarios, US global influence wanes."[17]

The study finds that there exist elements of continuity in the security environment. These elements can serve as the tenets within the Red, Gray, and Blue framework's Lakatosian hard core. They closely resemble the enduring tenets of classical Realism. These elements are:

1. The world political system is anarchic, "defined as the absence of centralized authority,"[18] with survival the ultimate end of most actors. Different anarchies are possible because agents, in part, constitute the nature of their anarchy.[19]
2. Systemic actors are those that can employ power at a system relevant level.

---

[15] Singer, "The Level-of-Analysis Problem in International Relations."
[16] *Road Map for National Security: Imperative for Change*, p. iv.
[17] *Global Trends 2015: A Dialogue About the Future with Nongovernment Experts* (Washington, DC: National Intelligence Council, 13 December 2000), p. 85.
[18] Wendt, *Social Theory of International Politics*, pp. 246-247.
[19] Ibid, p. 247.

3. The Third Image, the system, influences the First and Second Image systemic actors within it. Systemic actors, in turn, influence the Third Image. Actors (agents) and Environment (structure) are interdependent and mutually constitutive.[20]
4. Systemic actors seek power and security.
5. First Image actors are, by definition, unitary. Second Image actors intend to be unitary, rational actors.[21] Rationality may be culturally based.
6. Violence is the *ultima ratio*, but other instruments of power (diplomatic, economic, informational, psychological, and social) are also effective means. Power extends to diverse instruments, from "physical violence to the most subtle psychological ties."[22] The specific end desired by an actor seeking power and security partially dictates the means required; other influences predicating means required are the actor's identity, other actors' capabilities and intents, and the security environment.
7. Distribution of power, relative gains, and ranking or position are important among Second Image actors. First Image systemic actors will tend to focus on absolute gains.
8. Necessity and reason for existence trump morality and ethics when these values conflict.

The Lakatosian negative heuristic of the program forbids direction of *modus tollens* against this hard core. Within the protective belt are the various typologies and attack model networks explicated in chapter four. And the positive heuristic of the Red, Gray, and Blue framework invites investigation into the typologies of Self, Environment, Other, and Threat as well as the generic case models and decision trees detailing the possible worlds of conflict that exist, and the social construction of relations between the actors.

The paradigm for this research program is the Red, Gray, and Blue framework. As a disciplinary matrix for the national security elite it constitutes a proposed community paradigm. Beneath this paradigm lies a theory of how non-state actors changed the fundamental nature of the security environment. Following Van Evera's admonition that a theory that cannot be arrow diagramed is not a theory, the following arrow diagram specifies the causal chain that enabled non-state actors to achieve capabilities of system relevant violence:[23]

---

[20] Wendt, "The agent-structure problem in international relations theory," pp. 335-370.
[21] Wendt, *Social Theory of International Politics, p. 246.*
[22] Morgenthau, *Politics Among Nations*, p. 9.
[23] Van Evera, *Guide to Methods for Students of Political Science*, pp. 14-15.

$$\therefore, a \Rightarrow b \Rightarrow c \Rightarrow f$$
$$\mathbf{X}$$
$$\Rightarrow d$$
$$\mathbf{X}$$
$$\Rightarrow e$$

In the above theory, the variable "a" is the collapse of the Soviet Union, an antecedent condition for change in the international system structure and the loss of control of Soviet WME stocks, research, materials, and cadre. The variable "b" is the resulting change in the international system from a bipolar structure to a multipolar structure. The variable "c" corresponds to the number of states free of Superpower oversight and control. The variable "d" is the actual loss of control of Soviet WME stocks, and it constitutes a condition variable, and the condition variable "e" is the loss of control over client state and other states' WME programs. The variable "f" is the dependent variable that represents the attainment by emerging threats of WME strategic attack capabilities against the United States.

In narrative form, the theory explaining the attainment of WME attack capabilities against the United States by emerging threat actors is that the Soviet empire's collapse ended the global bipolar system and transitioned the system to a multipolar one. This freed many actors, both state and non-state, to pursue political agendas previously denied them. Concomitant with the demise of the Soviet Union, there was a twin loss of control over the former Soviet WME programs, and a loss of control over former client states' WME programs. A proliferation of technology and knowledge has also simultaneously reinforced the WME research efforts of actors pursuing the development of a WME capability. This series of conditions and events has lead to the current security environment's challenge to the United States. Globally active, the United States, as the "sole Superpower," inevitably has conflict with many actors. In the current security environment, even the small, non-state actors, however, potentially can conduct a strategic strike employing WME against the United States. The current security environment has transitioned from Kaplan's bipolar system to a Unit Veto system.[24]

From theory models can be crafted. According to Kuhn, models "provide the group with preferred analogies or, when deeply held, with an ontology."[25] The Stalker models advanced by this study not only serve as an ontology of the worlds of conflict, but also serve in a heuristic sense in thinking about the social relationships between actors in conflict. This describes and explains what

[24] Morton A. Kaplan, "Variants on Six Models of the International System," in *International Politics and Foreign Policy*, ed. James N. Rosenau (New York: Free Press, 1969), pp. 291-303.
[25] Kuhn, "Second Thoughts on Paradigms," pp. 464-463.

comprises the possible permutations of conflict relationships where a non-state actor is attacking anonymously and asymmetrically. However, another purpose of a model is to predict.

Hodges and Dewar argue that four prerequisites must be meet by a model in order to predict outcomes or events. The first prerequisite is that the situation being modeled must be capable of observation and measurement. The second prerequisite is that the scenario being modeled exhibit a constancy of structure in time. The third prerequisite is that the conflict being modeled exhibit a constancy across variations in conditions not specified in the model. Lastly, the fourth prerequisite states that it must be possible to collect ample data to test the model.[26] The second and third prerequisites deal with reliability, stability, and robustness of the model.

Predictions can be either specific or weak. In the social sciences, as well as in cases where chaos, chance, and complexity are involved, predictions tend to be weaker than in a hard science scenario tested under controlled conditions. The predictions possible from application of the Stalker models are weak predictions, because of the high level of complexity of critical infrastructures, the play of chance inherent in conflict between asymmetric actors, and the presence of chaos in complex, distributed systems. Only at the tactical level in well-understood systems against a known Red actor will predictions approach some degree of specificity.

Description, explanation, and prediction are not the only purposes of models. Hodges and Dewar define seven additional uses of a model. First, a model can act as a bookkeeping device, to condense or track data. Second, a model can act as an aid to selling an idea. Third, a model can be a training aid. Fourth, a model can be part of an automatic management system. Fifth, they can be used as aids to communication in organizations. Sixth, models can serve as vehicles for *a fortiori* arguments. Lastly, models can serve as aids to thinking and hypothesizing.

These seven uses of models apply to the Stalker models detailed in chapter 4. The acceptance and use of the Stalker models by the national security elite would also serve to promote the recognition of the need for change in their community paradigm. Until new tools have been discovered and promoted, old tools will not be discarded.

The observation that all policy proposals are based on theoretical assumptions leads to the expectation that during a paradigmatic crisis changing theoretical assumptions should be reflected in changing policy. This can be articulated in the three hypotheses detailed in chapter two. First, if the

[26] Hodges and Dewar, *Is It You or Your Model Talking? A Framework for Model Validation.*

paradigm in use by a policy community has become obsolete, then the policies that were formulated under that paradigm will be functionally inadequate in addressing the new reality. Second, given a paradigm shift, then there should exist evidence of changing policy attempting to keep pace with the changed paradigm. Third, if a paradigm is the foundation of a policy change and formulation process, then that process must be capable of paralleling the paradigm's pattern of change.

All three hypotheses find significant support in the study's discussion of the ten core documents of the critical infrastructure protection policy field. These ten documents, analyzed chronologically, show a trend of abandoning the old paradigm's equilibrium, and reaching for a new equilibrium. The sole exception of core policy documents trending away from the past paradigm is the 1999 version of the Federal Response Plan. This document, however, is more accurately viewed as a reissue of the 1992 version, with only minor modifications, and as such demonstrates bureaucratic inertia in practicing Kuhnian normal science as opposed to a thoughtful decision to remain locked in the past paradigm after considering the new framework. FEMA was ordered to reissue the FRP in light of PDD-63's guidance for critical infrastructure protection, and this is what was done. However, the task of coordinating a major rewrite and overhaul of a very substantial document to conform with PDD-63 and other Executive Branch documents through twenty-three federal agencies was not accomplished, and may have been too ambitious a task given the time allowed. What was reissued in 1999 is the 1992 version with changes that had been approved over the seven interim years incorporated into the main body of the plan, and some minor revisions. As evidence, the structure of the FRP's emergency support functions in table 2-2 does not conform with higher guidance issued before the FRP publication in 1999. The critical infrastructures of the CIP policy documents are not followed by the 1999 FRP, although the plan was directed to be rewritten in light of these very documents.

This failure of the 1999 FRP to support the Executive Branch's vision supports hypothesis one's assertion that policy formulated under the old paradigm will be inadequate to address emerging threats in the changed security environment. The 1999 FRP is just the 1992 FRP in new form, and as such constitutes an old paradigm policy tailored to meeting consequence management needs following natural disasters, with some limited applicability to terrorist activity, itself due to the incorporation of a change to the 1992 version into the 1999 FRP as an annex.

The numerous examples of policy documents, panel reports, legislation, and other recent efforts to change policy to meet the altered security environment support hypothesis two. The most radical yet has been the United States Commission on National Security / 21st Century (USCNS/21)

report. It makes fifty major policy recommendations, seven concerning homeland defense. The rapid growth of the CIP policy field strongly supports hypothesis two.

The PE theory is strongly supportive of hypothesis three. It incorporates strong parallel concepts to Kuhn's theory of scientific revolutions, and is capable of explaining both incremental and major policy fluctuations. As such, it is suitable for both periods of paradigmatic stability (Kuhnian normal science), as well as radical change of paradigm (Kuhnian scientific revolution). Baumgartner and Jones' PE theory is a functionally adequate model of policy change and formulation capable of serving as a macro-level guide for the pattern of CIP policy development. It nests within the Kuhnian theory of scientific revolution, and makes explicit how national security policy should be formulated during a paradigmatic crisis. The PE theory not only aids in understanding how policy parallels the underlying changing environment, it explicates the implications of the scope and scale of change on the formulation of policy. As such, it not only describes, explains, and predicts (weakly) how the formulation of policy is conducted, *it prescribes how policy should be conducted during a paradigm crisis!* The PE theory supports the study's finding that radical change in the national security elite's paradigm and the national security policies countering emerging threats is required.

The two questions that now should be occupying US national security policymakers is what theoretical framework is appropriate, and what concrete policy actions they should be taking in light of this changed security environment and paradigm. The policymakers' two questions parallel at a lower level of analysis and abstraction the study's two closely related, strategic questions: how can we understand the changed security environment theoretically, and what are the implications of the changed security environment for national security policies countering emerging threats? This nesting of questions parallels the nesting of the Kuhnian theory of scientific revolutions by Baumgartner and Jones' Punctuated Equilibrium theory of policy change and formulation.

Such a paradigmatic shift and its accompanying national security policy change is not without precedent. Following World War II, Kennan articulated a vision of a strategy of containment of the Soviet Union. This national security policy strategy stemmed from a paradigm shift of the US national security elite of what the role of the United States should be in confronting Soviet aggression. As the shape of future Soviet – American relations in the post-World War II world began to emerge, the framework in which the US national security elite operated shifted, and this shift was followed by a major shift in national security policy typified by a strategy of containment.

This change was precipitated by a "trigger" event as accounted for within the PE theory. The February 1946 speech by Stalin in which he revealed the goals of the Soviet Union's foreign policy shocked the US State Department. Operating from either one of two pure-type frameworks, a belief in the potential future of Soviet – US cooperation or a subdued Soviet Union forced to accept US dominance because of the US nuclear card, the Soviet's behavior did not accord with either of these frameworks. Baffled, the US State Department cabled their junior and almost unknown Chargé d' Affaires in Moscow for insight. George Kennan's "Long Telegram," driven by exasperation with the bureaucratic hierarchy and elation with the opportunity, forcefully sketched the animus driving Soviet conduct. His statement regarding the phenomenal impact his thoughts had on the national security elite was that Washington was "ready to receive the given message."[27]

Kuhn makes two points that apply to this historic precedent of the current security environment: first, the search for new answers does not begin until policymakers are confronted with the failure of the old rules of the game,[28] and, second, that it is usually the junior members of a community that most contribute to shattering ossified paradigms.[29] One reason old paradigms languish and die slow deaths is that the leading members of a community are committed to them, and they dictate the direction of the field through many venues. Kennan was young, junior, unknown, and isolated from the center of power in Washington. Had he not been asked to provide input, or had he responded with a watered-down opinion couched in bureaucratic caveats and evasions designed to curry favor, his strategy of containment would have not been articulated, yet alone adopted.

This relatively recent example serves to demonstrate that national security policies can be radically changed to meet the new challenges of an altered reality. It requires will and resources, both of which may be lacking when there is no clear and present danger that can be pointed to in a concrete fashion. However, it first requires that the national security elite see the world in new terms. Seeing the world in new terms is precipitated as the result of a paradigmatic crisis, in turn precipitated by "trigger events." This is the current state of the national security elite at the time of this writing; dramatic trigger events have occurred as detailed in table 2 – 4, there exists a growing consensus that the old framework is obsolete, but there has not yet emerged a new framework that has been adopted.

---

[27] Kennan, *Memoirs: 1925 – 1950*, pp. 294-295.
[28] Kuhn, *The Structure of Scientific Revolutions*, pp. 67-68.
[29] "Almost always the men who achieve these fundamental inventions of a new paradigm have been either very young or very new to the field whose paradigm they change. And perhaps that point need not have been made explicit, for obviously these are the men who, being little committed by prior practice to the traditional rules of normal science, are particularly likely to see that those rules no longer define a playable game and to conceive another set that can replace them." Ibid, pp. 89-90.

Kennan's era was confronted with the reality of nuclear weapons, which required completely new ways of thinking about security policy. Entirely new disciplines, including the rich academic study of nuclear deterrence, sprang up after the invention of the "absolute weapon."[30] Today's reality is that the United States is confronted with WME employed by small groups and even individuals, and this requires new ways of thinking about security policy. The advent of nuclear weapons was a new and fundamental development in the realm of conflict. Strategy, doctrine, research and development, force structures, institutional organizations, and policies all had to be invented *ex nihilo* to incorporate the new weapon's reality into national interests. Kingdon states that the "emergence of a new category is a signal public policy event. When people start thinking of [new policy fields] entirely new definitions of problems and conceptualizations of solutions come into play."[31] The new reality of a world where small groups and even individuals can mount strategic strikes against state actors is a radical, profound development, and requires a correspondingly radical and profound change in multiple fields, as well as the invention of new fields of inquiry.

The Federal legal landscape serves as just one specific example of such area. Although some of the legal authorities of the CIP policy field predate the 1997 report of the PCCIP, such as the Computer Security Act of 1987, the rapid pace of change in technology and the completely novel aspects of some threats employing new technologies call for a completely new legal approach to emerging threats. This concerns not only cyber-based strikes or intrusions, but also regulations and laws concerning CBRN agents, and other issues. The cultural and legal process of infrastructure assurance will require time to implement as the challenges are broadly spread across many specific issues from money laundering to the remote theft of sensitive technologies from overseas locations. Consider that for the organization of legal authorities traditional bodies of law have been assembled over time and are formally codified into coherent fields. For example, environmental protection laws have widely recognized standing as a separate and distinct field of law, with a Federal agency and numerous other organizations acting as professional authorities in the field. There exists no comparable body of law or network of organizations for critical infrastructure protection. Given the broad nature of critical infrastructures, and the interdependencies that exist across them, it is likely that CIP will be a developing field for legal authorities for decades. The PCCIP commissioners noted that efforts to invent the necessary fields to support CIP policy will be a project of significant duration. They stated such efforts are "a beginning. Our entire effort is prologue to a new era of infrastructure

[30] Bernard Brodie, ed., *The Absolute Weapon* (New York: Harcourt Brace, 1946).
[31] Kingdon, p. 113.

assurance...Our nation is in the midst of a tremendous cultural change, which will have a profound effect on our institutions."[32]

The past five years have witnessed a still modest beginning in crafting the core documents of the field. The PCCIP's report *Critical Foundations* was the first CIP core policy document to fundamentally break with the past paradigm's equilibrium to major degree. It precipitated the publication of PDD-62 and PDD-63. These twin PDDs, issued simultaneously, outlined a framework for CIP policy based on critical infrastuctures. The 1999 version of the FRP, however, represented a significant step back from progress in the field; it can only be characterized as the loss of a significant opportunity to craft a comprehensive, authoritative, and prescriptive policy document supporting the evolution of the CIP policy field. The National Plan, version 1.0, set the field back on track, a trend that has been reinforced by the Hart – Rudman's Commission phase III report.

Another area of change is institutional organization. On 24 April 2001 hearings on three House Resolutions were held before a joint meeting of the Subcommittee on National Security, Veterans Affairs, and International Relations of the House Committee on Government Reform and the Subcommittee on Economic Development, Public Buildings, and Emergency Management of the House Committee on Transportation and Infrastructure. The three resolutions were H.R. 525, H.R. 1158, and H.R. 1292, all dealing with proposed reorganizations to the Federal government and its agencies to provide for a realignment and a rationalization for Homeland Defense and counterterrorism. Several key individuals and experts appeared before the two subcommittees, and broad testimony supported a fundamental reorganization of the US government and its agencies, largely in line with the phase III report of the USCNS/21 committee's recommendations.

H.R. 1158 was introduced 21 March 2001 by Congressman Mac Thornberry (Republican, Texas). The billed is called The National Homeland Security Agency Act, and proposes renaming FEMA the National Homeland Security Agency (NHSA), and bringing under this newly redesigned agency three federal agencies: the US Coast Guard, the US Customs Service, and the US Border Patrol.[33] Also transferred to the NHSA under this bill would be the Critical Infrastructure Assurance Office (CIAO), the Institute of Information Infrastructure Protection (IIIP), the National Infrastructure Protection Center (NIPC), and the National Domestic Preparedness Office (NDPO). The goal of the

---

[32] *Critical Foundations*, p. 101.

[33] *Thornberry Introduces Legislation to Realign Federal Government*, Press Release (Washington, DC: US House of Representatives, 21 March 2001), document at http://www.house.gov/apps.list/press/tx13_thornberry/homelanddefense.htm.

legislation is to "realign and consolidate a number of key federal agencies in a way that will help the federal government better prevent and respond to homeland threats."[34]

H.R. 525, titled *Preparedness Against Domestic Terrorism Act of 2001*, calls for the amendment of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, which specifies conditions of national emergencies under which DoD assets can be employed in a civil support role. The bill was introduced on 8 February 2001, and calls for strengthening "Federal interagency emergency planning by the Federal Emergency Management Agency and other appropriate Federal, State, and local agencies for development of a capability for early detection and warning of and response to potential domestic terrorist attacks involving weapons of mass destruction; and Federal efforts to assist State and local emergency preparedness and response personnel in preparation for domestic terrorist attacks."[35]

H.R. 1292, the *Homeland Security Strategy Act of 2001* was introduced into the House of Representatives on 29 March 2001. The purpose of the bill is to require the President to develop and implement a strategy for homeland security, including antiterrorism and consequence management activities. The bill states the "United States Government does not currently have an adequate strategic sense of the unconventional threats to the United States," and directs that the President shall "develop a comprehensive strategy for homeland security under which Federal, State, and local government organizations coordinate and cooperate to meet homeland security objectives."[36]

As evident from the legislative interest described above, the CIP policy field includes initiatives designed to fundamentally alter the institutions of governance, and create a new Cabinet-level Secretary position. The proposed realignment of multiple federal agencies and offices constitutes a significant shift from past approaches to counterterrorism and consequence management. All of these initiatives conclusively support this study's finding that the US national security elite are in the midst of a paradigm crisis, and have recognized that past approaches are not functionally adequate to counter emerging threats to critical infrastructure and population. What remains to be accomplished is for the national security elite to adopt a collective framework that describes and explains the new security environment, and within which theories, models, and policies can be reconciled in a mutually supportive, coherent fashion.

---

[34] Ibid.
[35] *House Resolution 525:Preparedness Against Domestic Terrorism Act of 2001* (Washington, DC: US House of Representatives, 8 February 2001), p. 2. Document at http://thomas.loc.gov.
[36] *House Resolution 1292: Homeland Security Strategy Act of 2001* (Washington, DC: US House of Representatives, 29 March 2001), p. 2. Document at http://thomas.loc.gov.

Challenges facing the United States include terrorist groups' and even individuals' capabilities to employ asymmetric attacks and means; proliferation of knowledge, skills, and WME capabilities; the decrease in US "Cold War" civil defense programs and resources; proliferation of advanced technology; and the United States' own heavy reliance on computers to operate and maintain critical infrastructures to support the population and national economy. These challenges call for comprehensive, holistic solutions. The scope of the challenges dictate that the entire spectrum of the public and private sectors at the federal, regional, state, and local levels, across multiple sectors, be involved. The urgency of the problem requires action now to influence the shape of national security policies designed to deal with the challenges. The above resolutions would provide such a comprehensive solution; their call for profound changes, however, will energize significant opposition from institutions practicing Kuhnian "normal science" and threatened by the changes.

Assuming that the required institutional changes are implemented, there remains the task of coordinating the nation's potentially massive efforts to defend the homeland. Although fatally flawed in its current version because of its fundamentally irreconcilable present design with CIP core documents and Executive Branch guidance, the FRP is the single best document for providing a comprehensive, strategic direction for homeland defense. This study finds that following a substantial revision of the FRP to align it with the organizing concept of critical infrastructures and to reflect institutional changes implemented by the Executive and Legislative branches, the FRP should serve as the nation's overarching plan for crisis response and consequence management to emergencies, whether natural or man-made. This would serve to make every governmental response to a natural disaster, scenarios that occur multiple times each year, a full-scale dress rehearsal for response to catastrophic terrorist operations employing WME. The integration of the existing plans into a national master plan would reduce confusion, improve execution, and lessen costs and redundancies. Failure to design a prescriptive, coherent, strategic plan will result in disjointed execution and confusion in the event of either simultaneous strikes or strikes that cascade across infrastructures. Responding to a natural crisis should not make the simultaneous or subsequent response to a man-made crisis impossible, and the only way to ensure this does not happen is to have a single, overarching plan that dictates responses to both contingencies.

As far-reaching as the three resolutions are, there remain three major issues that must be addressed by any national plan to counter emerging threats to critical infrastructure and population. These issues are the role of DoD, the issue of intelligence support, and the issue of congressional

oversight.[37] The failure of the resolutions to delineate the role of the DoD is not a realistic approach. Inevitably, the massive scale of response required in any WME employment scenario dictates that DoD assets will be called upon, and the time to intelligently design that response, including responsibilities and lines of command, is before an incident occurs. Second, the issue of intelligence support is inadequately addressed. Homeland security will require the full support of the US intelligence community in producing products and estimates, as well as formal representation in the form of a National Intelligence Officer assigned a homeland security and asymmetric threats portfolio on the National Intelligence Council. Lastly, a formal venue for congressional oversight must be designed to insure the constructive involvement of the US Congress in this vital national security arena, and to protect civil liberties.[38]

This study finds that the seven USCNS/21 recommendations concerning homeland security would authoritatively address the national security challenges with a viable, effective, and comprehensive policy solution. The seven recommendations concerning securing the National Homeland are:

1. "The President should develop a comprehensive strategy to heighten America's ability to prevent and protect against all forms of attacks on the homeland, and to respond to such attacks if prevention and protection fail.
2. The President should propose, and Congress should agree, to create a National Homeland Security Agency (NHSA) with responsibility for planning, coordinating, and integrating various US government activities involved in homeland security. They should use the Federal Emergency Management Agency (FEMA) as a key building block in this effort.
3. The President should propose to Congress the transfer of the Customs Service, the Border Patrol, and Coast Guard to the National Homeland Security Agency, while preserving them as distinct entities.
4. The President should ensure that the National Intelligence Council include homeland security and asymmetric threats as an area of analysis; assign that portfolio to a National Intelligence Officer; and produce National Intelligence Estimates on these threats.
5. The President should propose to Congress the establishment of an Assistant Secretary of Defense for Homeland Security within the Office of the Secretary of Defense, reporting directly to the Secretary.

---

[37] General (R, USAF) Charles G. Boyd, *Testimony before the Joint Meeting of the Subcommittee on National Security and the Subcommittee on Economic Development*, US House of Representatives (Washington, DC: 24 April 2001), pp. 2-3.
[38] Ibid.

6. The Secretary of Defense, at the President's direction, should make homeland security a primary mission of the National Guard, and the Guard should be reorganized, properly trained, and adequately equipped to undertake that mission.
7. Congress should establish a special body to deal with homeland security issues, as has been done with intelligence oversight. Members should be chosen for their expertise in foreign policy, defense, intelligence, law enforcement, and appropriations. This body should also include members of all relevant Congressional committees as well as ex-officio members from the leadership of both Houses of Congress."[39]

A changed reality not only requires new policies, it requires new, functionally adequate institutional structures that craft security policies. The National Security Council (NSC) is the Executive Branch's "primary foreign policy co-ordinating council."[40] Under the Clinton Administration, the NSC rarely met, and did not ever convene a single formal meeting during the second term.[41] In contrast, the current Bush Administration has already held several formal NSC meetings, and more importantly, issued formal guidance regarding the organization of the NSC's structure to meet the challenges of emerging threats to US critical infrastructures and population.

Eleven Policy Coordination Committees (PCC) have been created by the Bush Administration's first National Security Presidential Directive, NSPD-1. These committees were detailed in table 2-3. The two most important PCCs for the purpose of this study are the Counter-Terrorism and National Preparedness PCC, and the Proliferation, Counterproliferation, and Homeland Defense PCC. The Clinton Administration had several different working groups dedicated to various issues that touched on the CIP policy field, but did not have a single committee or group dedicated to CIP exclusively. Various Clinton Administration entities have been consolidated into the Bush Administration's PCC on Counter-Terrorism and National Preparedness. These include the Counter-Terrorism Security Group, Critical Infrastructure Coordination Group, Weapons of Mass Destruction Preparedness Group, Consequences Management and Protection Group, and the interagency working group on Enduring Constitutional Government.

These two Bush Administration PCCs, both under the National Security Advisor Condoleezza Rice, are new policy organizations active in the CIP policy field. This is a clear indication that the

---

[39] USCNS/21 Phase III report, p. 118.
[40] Stephen Fidler, "President Places NSC Back on Top," *Financial Times* (London: 11 April 2001). Document at http://globalarchieve.ft.com/globalarchive/articles.html?id=010411001142&query=Fidler.
[41] Ibid.

Bush Administration viewed past structures as functionally inadequate to deal with the CIP policy field's challenges, and the creation of these new structures is intended to come to grips with the CIP policy field's issues. The pooling of several different Clinton-era working groups into a single, focused PCC will also serve to unite efforts toward creating a coherent policy office.

This study finds that the current security environment poses a novel security scenario. Implementing future policy crafted by these PCCs will not be accomplished by governmental agencies, but private organizations that own, operate, maintain, and secure critical infrastructures. The protection of critical infrastructures is beyond the capabilities of both the state and federal governments, and can only be accomplished by the private industries that own them. The government, however, has the necessary intelligence, law enforcement, and other organizations to inform, coordinate, and legitimize this defensive effort. The arrangement is a novel, curious joining where industry has the actual wherewithal and necessary expertise to protect the nation's critical infrastructures, but lacks the intelligence sources and legal jurisdiction to do so, and the government has the intelligence assets and legal authority, but neither the capability nor the expertise.

The presumption is that private industry will cooperate with state and federal government in protecting infrastructure. However, there is no mechanism that would ensure that protective activity would be coherently applied across the nation. Forced to balance protection with profit, many corporations may elect to isolate their infrastructures from the danger of cascading effects resulting from a cyberstrike, and thus compromise the integrity of the national power grid or other critical infrastructures. Additionally, reliance on third-party support will proliferate a wide variety of standards and protocols, which may serve to actually weaken or even introduce dangers into the systems industries are attempting to protect. If Hobbes' Leviathan is to be protected by Hobbes' Man, then government must provide private industry with information and intelligence regarding threats. Additionally, if government wishes to promote standards that are adequate and universally applied, it must provide funding to or regulation of industries. The hope that industry will voluntarily communicate, cooperate, and assume the costs of a coherent national system of protected infrastructures is not a realistic planning consideration for policymakers and strategists. This fact necessitates a radical change in how the policy process for dealing with emerging threats and WME consequence management is conducted; a policy development challenge that the Bush Administration's new PCCs must overcome.

Building a national consensus for such policy change is a significant hurdle if the above cooperation is to be achieved. Not only will the negative feedback force of normal science interfere

with alterations of the issue definition, the public must first be educated as to of what stuff the issue actually consists. Image is an important matter in the process of formulating policy. How a problem or issue is defined determines which actors can influence the policy. Defining the CIP policy issue as a national security concern ensures it falls within the purview of a specific issue network of institutions, Congressional committees, and interest groups. There exists, however, a strong movement to define CIP policy as involving significant civil rights issues, such as privacy. As a nascent policy field, CIP is still in the process of being shaped. Multiple organizations, both private and pubic, are vying for influence and access to further their political agendas in this field. "Policy images are a mixture of empirical information and emotive appeals."[42] Because of this emotional aspect to any policy image, a coordinated approach to defining the issue is important for any policy field in its formative stages. This situation will likely persist until the Bush Administration's PCCs establish codified policy in writing that sets the direction and specifies the shape of the CIP policy field, and Congress tacitly or explicitly approves of this definition of the issue. Until then, the CIP policy field's direction and future shape are very much in flux, and remain at the macro-political level of sequential processing as detailed by the PE theory.

How an issue is defined, and the image that results is influenced by the policymakers' framework. George notes a leader's operational code is comprised of two parts: the philosophical and the instrumental. The philosophical component deals with what is the essential nature of political life, and the instrumental portion deals with identifying the best approach for setting goals for political action. The Red, Gray, and Blue framework corresponds to George's philosophical component of the operational code, and the Stalker models correspond to the instrumental component. Beliefs, values, and stereotypes relevant to the security environment shape a political leader's definition of a situation and his strategic framework. The models he employs, consciously or unconsciously, are intellectual tools that are applied to specific cases confronting him. The framework of a security environment approach to national security policy countering emerging threats targeting critical infrastructure and population is the functionally adequate paradigm advanced by this study for describing and explaining the current, altered security environment.

A security environment is constituted by three elements: Self, Other(s), and the Environment. These three constitutive elements of the security environment are interdependent in shaping their individual and collective identity, each subject to the influence of the others. A simple analysis of the intersubjective relationship between Self and Other(s), however, potentially ignores the effects of Environment. At best, such an analysis of a strictly bounded Self – Other relationship is a dyadic study

[42] True, Jones, and Baumgartner, p. 101.

of a conditional, fleeting reality. It also excludes influences exogenous to the dyad that exercise influence on the relationship. A specific situation context is not a complete analysis of the social relationship between two actors. Other variables in the environment, such as interests and the conductive medium, also constitute elements of the relationship.

Self can be further disaggregated into true Self, the actual identity of the actor; proxy Selves, or other actors that ally with true Self to achieve objectives supporting Self's ends; and Identity Masks, or personas created by Self to obscure or alter aspects of true Self's nature.

Other contains four elements. The first is Threat, or Red, an actor that has both the capability and intent to harm Self. The second is a neutral actor, or Green, which is not for or against Self. The third sub-category is an actor of unknown intentions, or Gray, which may be either hostile, neutral, or friendly. Lastly, the fourth is an unknown actor, again Gray, which could also be either hostile, neutral, or friendly.

The third constitutive element of the security environment is Gray, or the Environment. Environment is comprised of three elements: known aspects, unknown aspects, and unknowable aspects. The first category are those Environmental traits of which Self is aware. The second category are aspects which could be determined and assessed if Self was aware of their existence. These aspects can be discovered through study and analysis of the Environment, in which case they then become known aspects. The two Gray actors, an actor of unknown intentions and an unknown actor, exert their influence through this category. Lastly, the third category are those Environmental influences, including chance, complexity, and chaos that are unknowable and cannot be fully comprehended, calculated, or accounted for.

The concept of the security environment is not synonymous with the world political system, except when extended to the most macro level of application. Security environments can be defined by different variables, including geography, time, and functional issues. Geographically defined security environments are regional entities. Functional security environments may be defined in terms of interests, such as control of oil reserves, or activity, such as the international arena of finance.

National security policy makers must operate from theoretical perspectives that are relevant and applicable to their security environment(s). This demands the ability to employ different theoretical frameworks as intellectual tools for differently constituted environments. Rigidity in a

specific framework introduces distortions between the intellectual tools and the apprehension of reality as reality invariably changes.

When there is no shared environment, thus conductive, tractable medium within which conflict can occur, there cannot arise a security dilemma between actors. If there is no security dilemma between actors, then conflict is improbable. Stated differently, a shared security environment is a necessary condition for a security dilemma, which, in turn, is a necessary condition for conflict. The characteristics of Self, Other, and Environment that constitute a shared security environment are the key to understanding potential causes of threat perception and interests that lead to security dilemmas, and ultimately conflict.

An actor must understand its environment. To the extent that an actor operates under a false impression of one's environment, at both the philosophical and operational level of understanding, risk increases. The Red, Gray, and Blue framework does not present the environment as a single entity with fixed attributes that mean the same thing to all actors. The security environment within which an actor operates is influenced by the actor's actions and characteristics. Whether this accrues to the actor's advantage or disadvantage is dependent on that actor's traits, decisions, and activity. At the deep structure of environment, all actors are affected by common environmental attributes, for example gravity in physical space or Internet protocols in cyberspace. But in the shallow structure of environment, the environment itself is partially constituted by the actor itself.

Gray consists of both deep structure and shallow structure traits, both influenced by and influencing the actors within it. And it is neutral; it does not inherently favor or disadvantage either Blue or Red, *a priori*. It affects different actors *impartially*, because it is unthinking. But it does not affect different actors *equally*, because different actors themselves possess traits that influence Gray's effects on them. Because Gray exists across all dimensions, it cannot be escaped; the conduct of conflict in any dimension cannot be reduced to a simple dyad of Red against Blue. Thus, in any conflict the environment itself is a factor *that favors or disadvantages an actor based on that actor's own characteristics*. Employment of the Red, Gray, and Blue framework can inform policy design of environmental factors affecting both Blue and Red, thus improving the policy.

Security environments are dynamic, and will include both elements of stability and change. The development of a model of a specific environment must account for both the factors supporting stability and those promoting change. Preoccupation with either positive or negative feedback forces as identified by Baumgartner and Jones, or elements of change or stability, is a biased analytical

methodology. What is required is an approach that accounts for both positive and negative feedback forces, and that provides a structure between the extremes of perfect continuity and unending change. The security environment approach meets these two criteria.

Security environments are interdependent, with the term interdependence as used in this study adopting Keohane's and Nye's definition referring to "situations characterized by reciprocal effects among" actors, including environment.[43] It is this dynamic of interdependence that illustrates how actors constitute their enemy and ally. In ideological terms, the United States and the Soviet Union were interdependent in constituting the other as an enemy, by definition of their own choice of identity.[44] The security environment is, likewise, interdependent for its identity with those actors that are active within it. The three constitutive elements of the security environment – Self, Other, and Environment – are mutually constitutive and politically interdependent with each other. This collective interdependence defines roles, identities, and interests. It may include economic or other components, but it is first and foremost a political and social relationship.

Intelligent analysis of a security environment is necessarily multidisciplinary, including quantitative and qualitative factors, the development of typologies, and the intuition of experienced policymakers and strategists. This analysis must include not only the known aspects, but also the unknown and unknowable aspects. The requirement is not that what is not known, or is unknowable, be somehow ascertained, but rather that the policymaker views the environment critically, understanding that such aspects exist and exert real influence. Deductive techniques offer efficiency and economy in apprehending the potential influences of significance to Self which unknown and unknowable aspects could exercise. A policymaker can examine Self critically and deduce those factors that pose a risk to Self or the attainment of its objectives. This enables Self to take preventive protective measures. Key criteria in designing operations to protect itself are robustness, redundancy, resilience, recuperability, reparability, distribution, and diversity as explained in chapter 3.

Even with the best possible analysis, the security environment cannot be perfectly known. This fact is accounted for in the unknowable aspects of the environment category. The unknowable aspects of the environment are similar to the unknown aspects of the environment. The difference is that unknown aspects may eventually transition to the known aspects category, but unknowable aspects remain incomprehensible in their causal chains and effects. However, planning can also take into account the effects of the unknowable aspects to some extent. As with the unknown aspects, this does

[43] Keohane and Nye, *Power and Interdependence*.
[44] Wendt, *Social Theory of International Politics*, p. 228.

not mean that specific counters are crafted, because specific factors to counter are obviously, again, not known. Rather it is the prudent recognition that there exist measures that will ameliorate certain future effects, regardless of their cause or origin. Countering the effects of unknowable aspects of the environment begins with a quasi reverse engineering methodology, where the desired endstate of a policy is known. A thorough assessment of Self then provides the start point, and between these two known conditions a critical path can be identified that the proposed policy must accomplish to achieve the endstate. This critical path must be safeguarded from interdiction, and its composition and traits partially determine the environmental conditions and threats that could injure Self. From analysis of the critical path, a general universe of environment aspects can be deduced that could break or damage the successful implementation of policy. Measures then can be instituted that forestall interdiction of the critical path by such environmental aspects.

Prevention of the effects of unknown and unknowable aspects also involve analysis of the conductive media in which Self is engaged. Conflict can be prosecuted in all six dimensions: the three dimensions of physical space, time, cyberspace, and perception. The structure of the dimension in which conflict occurs is the conductive medium. Cyberspace actors can engage, and be engaged, in the conductive medium of cyberspace. Some actors can engage in all dimensions against an Other confined to fewer dimensions. This may not be of significance, however, if the Other is a niche actor possessing superior expertise in a specific conductive medium The concept of conductive media of conflict is an important concept in the Red, Gray, and Blue framework. Understanding both Self and Other, as well as Other's expertise and ability to conduct operations in the various conductive media of conflict, enables the creation of a competitive advantage through superior planning and use of the best conductive media available to Self. This principle undergirds the concept of asymmetry.

Intelligent use of the dimensions of conflict can provide an operational advantage to an actor. Self's traditional intelligence collection methods fail, including signals and human intelligence, if Other exercises discipline in the physical world. There may be no uniforms, organizations, buildings, symbols, or other physical evidence of the existence of the Other. By using the fourth dimension intelligently, Other denies Self the time to react or learn. By limiting its signature and presence to minimum levels, Other denies Self the sixth dimension. Other's precautions in the first five dimensions of conflict preempt Self's capability to sense Other. Against such an Other, Self can only adopt defensive courses of action and take steps to mitigate the effects of strikes when they occur. If it desires to, Red can retain the initiative.

When Blue is a global actor it will be involved in many security environments. Inevitably there will be Reds provoked by Blue's activity. To reduce the potential for anonymous, asymmetric strikes, Blue must consider the possibility of provoking other actors, either known or unknown. A heavy-handed policy stance is not as viable a position as it was when state actors, with their inherent, inescapable accountability for their actions, were the only actors capable of striking against other actors.

Red can choose the conductive media in which it operates and become a niche actor. Blue, if an industrialized, developed state actor, must operate in all six of the dimensions of conflict. This is not only resource intensive, it is also difficult to craft security policies that work coherently across dimensions. By choosing to be a niche actor, Red is streamlined in its processes, anonymous, purposeful, and capable of employing asymmetric and asynchronous strikes.

Asynchronous operations are multifaceted in their implications. Duration of attack is one implication, but the timing of an attack, as well as patterns of operations in the fourth dimension are also considerations. A sophisticated actor skilled in use of the fourth dimension can strike when the payoff is highest, and the risk low. Blue must analyze the fourth dimension for patterns, but these patterns will only reveal the activity of those actors that are not sophisticated enough to cover their signature in time. Sophisticated actors will leave no discernable pattern, or will intentionally create a false pattern for purposes of deception. Red's effective use of time, itself a neutral component of the environment, confers security. An asynchronous threat operates in the interstices created by its effective use of the fourth dimension.

Cyberspace has different implications for operations based on actor type. The deep structure of cyberspace is constituted by the hardware, firmware, software, standards, and protocols that maintain an all-encompassing virtual environment of all electronic communication infrastructures. Cyberspace is more than the Internet. Shallow cyberspace is where interaction takes place between actors. Monitoring shallow cyberspace entails monitoring communications, but monitoring deep cyberspace entails monitoring the shape of cyberspace itself. The US Critical Infrastructure Assurance Office (CIAO) has coordinated the measurement and mapping of portions of deep cyberspace through its Project Matrix.[45] Application of measurements and signals intelligence techniques across the fourth dimension to the fifth dimension may provide insights relevant to US national security interests.

---

[45] Richard A. Clarke, "Memorandum" (Washington, DC: National Security Council, 19 July 2000). Document available at http://www.ciao.gov/Matrix/RC_Memo.htm.

Cyberspace can grow, shrink, as well as change in shape and composition. This fact has profound meaning if analyzed from a national security framework.

The sixth dimension of conflict is, in part, constituted by the influences of the first five dimensions. An actor's own characteristics also influence perception. In turn, the sixth dimension of conflict influences the first five dimensions. The activity of Self and Other in the first five dimensions influences how Self and Other view each other. They constitute their identities and roles in relation with each other.

Perception is both cause and effect. Sophisticated actors recognize this and adjust their actions and identity masks accordingly. Skillful exploitation of perception formation can create surprise and operational advantage. To the degree that factors in the first five dimensions of conflict can be modeled and objectively measured, automated analysis can discern, at least tentatively and superficially, the identity and role of an Other. This is an important contribution of models, especially in the fifth dimension where physical reality cannot be apprehended with human senses and communication is limited to digital transmissions, excluding other forms of communication like direct observation of the actor and actor's actions that would provide a richer context for understanding. Artificial Intelligence may play an important supporting role in the future, but it must be interpreted by human analysis.

Targeting in the new security environment requires heightened analysis. What is targeted provides information concerning Red (alternatively, Blue). Only in the case of irrational actors conducting random targeting is this information lacking in providing clues to the ends pursued, although even in this case there exists information concerning the means employed. It would be a mistake to infer, however, that WME will not be employed by actors whose concept of rationality differs from a so-called "mainstream" perspective. This is a different actor type than a deranged individual. For example, suicide attacks are, from the perspective of a Shi'ah Islam martyr, completely rational acts.[46] Inflicting mass casualties against non-combatants is a rational option for a terrorist. These and other actors operate from different perspectives of rationality. Culture counts in defining an actor's perspective of rationality. These perspectives are, however, internally consistent belief systems that can be understood, explained and potentially anticipated, unlike the capricious, impromptu activity of a wholly deranged individual. In modeling Red, the social-psychological aspects are important. Analysis of an actor's targeting preferences provides insights into the mind of the threat.

---

[46] See the Qur'an (3:169-172), and the hadith *Sahih Bukhari* (Vol. 2, Book 23, Number 329; Vol. 9, Book 93, Number 555).

Targeting Red is complicated in the new security environment. Unlike state actors which typically have infrastructures that can be mapped and targeted, non-state actors may possess no hard-facility infrastructures of significance, or may even exist in parasitic fashion within Blue's own infrastructures. In this case, the threat is within Self. Urban-based terrorists use and benefit from the same electrical, transportation, and other infrastructures as the government they attack. Highly-advanced Others may have no significant dependence, hence vulnerability, on physical infrastructures to act in the role of threat. A threat actor operating in cyberspace is only reliant, and that at miniscule levels, on electric power and telecommunications infrastructures, both of which may be based abroad in any event. A First Image actor has limited need for physical infrastructure, and if existing within Self's physical space and population in parasitic fashion may be immune to an attack on physical infrastructure unless very precisely targeted. When targeting Red, the acronym CARVER is a useful tool. CARVER stands for criticality, accessibility, recuperability, vulnerability, effect, and recognizability.[47] Until the Red, Gray, and Blue's framework and typologies of threat are accepted, the use of the CARVER methodology will be restricted to only known threats, and not emerging, pure-type threats.

The new security environment has new means of deceiving other actors. The principles of deception are now also implemented using cyberspace personas or identity masks.[48] Increasingly actors will have a presence in cyberspace. This presence is a representation of the actor – a mask or persona – that communicates to other actors the identity of the owner. In the case of a corporation, this mask communicates the capability to conduct business in all of its aspects from marketing to sales to logistics. In the case of an individual or group, this presence in cyberspace may consist of transactions regarding one's credit history, phone numbers and usage patterns, financial transactions, on-line purchases or other matters. This presence is influence by culture, socio-economic factors, and even geographic location. An anonymous actor employing a secure digital mask enjoys freedom of the fifth dimension, but is virtually invisible to others within the medium because of its active efforts to cloak its existence.

The type of mask employed depends on the purpose intended of the mask. Where stealth is desired, the purpose of the mask is to confer "invisibility" and it will be created in a fashion to ensure the actor remains covert. To remain covert, an actor must remain undetected in both the shallow and deep structure of cyberspace. The architecture of the hardware infrastructure must not provide

[47] Joint Pub 3-05.5, pp. II-8 through II-10.
[48] Andrews, *Electronic Identities: Secure Masks.*

evidence of an access portal, digital traces of activity must be destroyed or caused to "evaporate," and the operations of a stealth actor must be undetectable and unrecognizable to similar actors passively surveilling the deep structure of cyberspace. The ability to measure and assess the composition of the deep structure of cyberspace is the ability to monitor that deep structure. A stealth actor requires a mask that serves as a shield deflecting observation. Even more challenging, this mask must not be able to be "sensed" by its effects on the structure, shape, or size of cyberspace itself. Much as the existence of an unknown celestial body, for instance a black hole, can be inferred from its gravitational pull on known aspects of the heavens, a stealth actor can be sensed indirectly by its use of bandwidth or through other metrics. This suggests that the stealthiness of a mask is not a dichotomous variable, but a matter of degree.

Masks can be created to either cloak a covert actor's existence, or to overtly deceive as to one's true identity. Tools, techniques and testing create masks. Credible masks are anchored in the four dimensions of physical space and time, exist in the fifth dimension of cyberspace, but conduct their activity and seek their effects in the sixth dimension of perception. Creating masks requires few resources, allows large-scale operations employing multiple masks, transcends political boundaries, facilitates centralized control, and reduces vulnerability and risk to the employing actor. Masks are potent tools for non-state actors, because states do not necessarily possess an inherent advantage despite their material and other sources of power. Non-state actors adept at employing masks can challenge states asymmetrically, asynchronously, and even anonymously.

A security environment approach portrays the security policy decisionmaker as Cerberus, the three-headed beast that guards the gates of Hades in Greek mythology and prevents the escape of terrors from the underworld. The metaphor is fitting for the Red, Gray, and Blue model, where policymakers and strategists must be informed of not only Other, but also the environment and Self. Applying the metaphor to the Red, Gray, and Blue framework, a policymaker must study the three components of the security environment, Self, Other, and the Environment, to prevent harm to security interests. Without adequate analysis of the three components, security policy is possibly flawed in its design, and unable to protect or further interests.

Within the Realm of Cerberus leadership, deterrence, and other activities take place. Even absent any interaction or communication between Blue and Red other than conflict, that language of conflict is understood by the decisionmaker(s) operating in the Realm of Cerberus. Their understanding of Self, Other, and Environment constitutes the case-specific context within which

security policy is planned and implemented. National security elites must emulate Cerberus and regard three different entities simultaneously and accurately.

The Stalker model, comprised of seven possible worlds, or variants, of relationships, is a finer-grained resolution of the more abstract, paradigmatic Red, Gray, and Blue framework. The seven variants, as generic case models, represent the possible permutations of relationships between Blue, Red, Green, Yellow, and Gray actors. In the variants, Blue and Red represent Self and Threat, respectively. Green represents a neutral actor, Yellow represents a threat actor other than Red, and Gray represents either an unknown actor or actor of unknown intentions. The seven variants of Stalker are: Simple Conflict, Ganging Up on Blue, Ganging Up on Red, Alliances, Factions, Mixed Game, and N-Actor. The Stalker models have seven plateaus. The first plateau is defined as the Status Quo. In this plateau Red does begin to prepare an attack against Blue, and the existing status quo is maintained. In the second plateau, Hold Reconnaissance and Continue Preparation, Red initiates a preparatory stage for attack, but does not begin reconnaissance. In the third plateau, Hold Strike and Continue Preparation and Reconnaissance, Red is conducting preparatory and reconnaissance tasks but has not yet launched a strike. In the fourth plateau, Undetected Strike, Red's strike is not perceived in the sixth dimension by Blue. In the fifth plateau, Unresponsive Target, Blue has perceived Red's strike, but has elected to not respond. In the sixth plateau, Defensive Target, Blue limits its response to Red's strike to strictly defensive measures. In the seventh plateau, Ineffective Retaliation, Blue has conducted offensive retaliatory operations unsuccessfully. These plateaus are further detailed below.

The models are tools to help bridge George's gap between theory and practice. Other tools required to apply theory to operations are typologies and generic case models. Chapter four provided concepts, terms, and intellectual tools below the level of abstraction of paradigm, theory, and model. These tools continued the study's development of the security environment approach to national security policy by extending discussion of it to encompass a level of detail that can, following modification for context, be applied to specific cases. It is this ability to apply theory to cases that is supported by such intellectual tools.

Classification by typology serves many useful purposes. This study's typology of threat classified a number of emerging threats by identity, means, targeting preferences, and ends. This is not an exhaustive listing, nor can it be applied to a specific case without a critical analysis of whether it requires modification for situational context. But it is a concrete point of departure that defines the boundary between past conceptions of threat rooted in a state-centric perspective, and what is increasingly known in this new policy field as emerging threats. Frequent employment of the term

"emerging threats" is made, yet almost as frequently not defined in any meaningful way. This is not helpful in providing in concrete fashion the requisite intellectual tools and concepts that materially contribute to the development of a perspective, from paradigm through case, that can inform policy. The foundation of policy is theory, and the crafting of theory requires precision and detail if it is to bridge the gap between thought and practice. The employment of concepts at the generic case level may not be suitable for employment in specific cases and contexts without some modification. However, generic cases are required in order to provide a start point for such modification, or there will persist a gap between theory and practice that requires each new, specific case to bridge it without the benefit of a common suite of intellectual tools. This bridging of the gap without the direction provided for by a generic case ensures a wide variety of terms and concepts being invented by a series of analysts that may not conform to the higher, more abstract levels' shared tenets, or hard core. Failure to develop the Red, Gray, and Blue framework below the level of theory would be to, in Lakatosian terms, not provide the positive heuristic of the research program, as explained in chapter one. Frequently policymakers and others reference emerging threats, but are not rigorous in their use of the term. If terms are to have substantive meaning, they must be defined. This study's typology of threat does so.

The components of the typology are identity, means, targets, and ends. Each of these components of threat definition provides inherent information that may apply to the other components. If Blue knows it is confronting, for example, an information warfare team employing cyberstrikes to target the nation's electrical grid in retaliation for a US policy, that specific linkage across the typology's categories enables effective counters to be planned to mitigate, and perhaps preempt, the threat. Even knowledge of only one of the components of the threat's definition provides Blue information that is valuable in designing counters.

Until new concepts are placed into a sufficiently detailed form that at least allows criticism there can be little progress. Bacon's dictum, again, calls for clarity and not confusion as the best route of progress. Even flawed notions, provided they are made explicit and thus vulnerable to critical thinking and scholarly debate, can promote the cause of progress in understanding. To this end seven attack model networks that describe variants of the game of Stalker were explicated by the study. An attack model network is a graphical form of knowledge that has formal probabilistic semantics, rendering it suitable for statistical calculations. Such networks incorporate expert knowledge of a process, here in the game of Stalker the attack of Blue by an anonymous, asymmetric, asynchronous Red. Attack model networks are similar to neural networks, with two important advantages: first, the capability to easily encode expert knowledge into the network allows better subsequent discovery of

additional knowledge, and, second, the nodes and arcs in such networks describe processes in terms of causal chains.[49]

Conventional, traditional approaches to modeling threat are of limited utility in modeling anonymous, asymmetric, and asynchronous threats targeting critical infrastructure. State-centric approaches fail to capture the means, methods, and ends of non-state actors. Approaches suitable to state-on-state conflict and emphasizing the conventional military instrument of power are unwieldy intellectual tools when countering emerging threats.

Stalker is a game played by at least two actors: Red (the Stalker) and Blue (Self). The name is derived from the analogy of a person being "stalked" by another individual. A stalker observes the target's activities and behaviors, learning in great detail all aspects of the target's routine. In the current security environment, this study argues, the United States is being stalked by emerging threats targeting critical infrastructure and population. These threats do not need to overtly confront the United States to achieve their objectives; they adopt the Stalker's covert, asymmetric approach to attaining their goals.

An interesting aspect about the game of Stalker is that the victim (Blue) is required to play, even if the threat (Red) is not playing. Denied knowledge of the Stalker's activities, Blue must always be vigilant, monitoring the environment for indications and warnings that signal an asymmetric actor's presence. This means that Blue is always paying the costs of vigilance, even when there is no cost for an asymmetric actor maintaining a passive status of observation.

Stalker is not a zero-sum game, in the formal sense that the sum of losses and wins equals zero. As becomes evident below, Red possesses the initiative at the start of the game, and can exercise the option to withdraw from play at any time. This makes a strategy of "raid and run" a winning strategy for Red.

The game can involve multiple actors in seven possible permutations. The variants of the game establish a minimum foundation for different structures of actor relationships, different actors types, and different numbers of actors. The different number of actors involved is self-explanatory, with one note. The number of actors is a minimum "floor" that contributes to defining a specific "world" or

[49] David Heckerman, "Bayesian Networks for Knowledge Discovery," in Usama M. Fayyad, Gregory Piatetsky-Shapiro, Padhraic Smyth, and Ramasamy Uthurusamy, *Advances in Knowledge Discovery and Data Mining* (Cambridge: MIT Press, 1996), pp. 273-274.

structure of conflict variant. The different actor types are signified by color, and the different structures of conflict are described by the variant titles.

In the first permutation of the game, Simple Conflict, there are exactly two actors: Red and Blue. Red is the Stalker, and is an emerging threat actor. Blue is Self, and a state actor with two Clausewitzian centers of gravity: national critical infrastructures and population. The remaining six variants have encoded within their attack model networks the core of a simple conflict decision tree.

In the second permutation of the game, Ganging Up on Blue, there are at least three actors: one Blue actor, and two or more Red actors. There may exist more than two Red actors, however, for the purpose of this study the minimum required number of actors is used. Consideration of additional actors is unnecessary to define the structure of conflict in a particular world, or variant. The two Red actors in this world pursue a common end, with the potential for betrayal encoded within the network.

In the third variant of the game, Ganging Up on Red, there are at least three actors: one Red actor, and multiple Blue actors. The Blue actors pursue a common end, again, with the potential for betrayal and division encoded at the decision nodes.

In the fourth permutation of the game, Alliances, there are at least two Red actors and two Blue actors, for a minimum of four actors involved in the game. The Red actors are allied to attack at least one Blue actor, and the Blue actors are allied to defend against Red attack.

In the fifth variant of the game, Factions, there are at least three actors, all of whom are independent, non-allied actors. The actors are Red, Blue, and Yellow. Yellow, a threat actor, is not allied with the other threat actor, Red. Third Actor Escalation is possible in this permutation, as it is in all variants of more than two actors.

In the sixth permutation of the game, Mixed Game, there are a minimum of three actors. The actors are Red, Blue, and Green. Green is a neutral actor, or an actor of indeterminate intentions.

In the seventh permutation of the game, N-Actor, there are at least four actors, with various combinations of independent actors and alliances possible. The actors are Red, Blue, Yellow, and Green. Should three alliances form, the game reduces either to the "Factions" or "Mixed Game" permutations. Should Yellow and Red ally, the game reduces to a "Mixed Game" variant. Should the

Green actor ally with either Red or Yellow, or transition to a new threat actor unallied with either Red or Yellow, the game reduces to "Factions." The N-Actor game requires a minimum of four actors.

Stalker's plateaus are characterized as patterns of behavior that can exist over time within the game's structure. There are seven plateaus.

Plateau - 0: Status Quo – This plateau is characterized by a pattern of behavior that accepts the status quo. Red takes the decision to not prepare at node 0 (See Figure 4-1: Simple Conflict), and the game is not started. The plateau is disrupted when Red takes the decision to begin preparations for attack.

Plateau - 1: Hold Reconnaissance & Continue Preparation – This pattern of behavior results from Red's decision at node 0 to begin preparations to strike Blue, but Red stops short of deciding to conduct reconnaissance operations. Blue is thus provided with the opportunity to perceive Red's preparations, and potentially to initiate preemptive operations. This plateau typifies Red as planning, gathering materials and equipment, training, and forming organizationally. Red may persist in this plateau for some time, perhaps indefinitely. The plateau can be disrupted by Red's decision to begin reconnaissance or cease operations, or if Blue preempts Red.

Plateau - 2: Hold Strike & Continue Preparation & Reconnaissance – This plateau results from Red's decision to begin reconnaissance operations. This decision provides Blue with its second opportunity to discover Red and initiate preemptive operations. In this plateau, Red is typified as both continually preparing and actively reconnoitering to ascertain Blue vulnerabilities. The plateau can be disrupted by Blue's discovery and preemption of Red, or Red's decision to strike or cease operations.

Plateau - 3: Undetected Strike – Red takes the decision to strike. Blue is not cognizant of the strike, although it has the opportunity to perceive the strike. This presents Red with the option of continuing in plateau 3 until Blue perceives the effects of Red's strike. The failure of Blue to perceive the strike may be due to the characteristics of the strike, i.e., scale, intensity, location, timing, targeting and other considerations, or the failure to perceive the strike may be due to characteristics of Blue, i.e., lack of feedback system, failure or absence of monitoring equipment or sensors, or negligence. Plateau 3 allows Red to continually strike inflicting damage to the limit of its ability and will. The plateau can be disrupted by Red's decision to stop striking or Blue perceiving the strike.

Plateau - 4: Unresponsive Target – This plateau results from Blue's perception of Red's strike, but Blue's decision not to respond or inability to respond. Blue may choose not to respond for several reasons. One reason may be that the cost of responding exceeds the costs of not responding. This case may pertain to low-level, low-cost attacks mounted by unsophisticated, low-threat actors without success. The decision to observe, but not respond may even serve as training for Blue's forces, where response would remove the opportunity to observe actual Red attacks, and result in Blue having to duplicate the scenario with simulations or self-resourced sparring partners or "red teams." An example would be Blue's decision to not respond to ineffective attempts at penetration of a corporate computer network in order to maintain the defensive force's skills and alertness, minimize the costs of legal action, gather information on developing techniques employed by attackers, and husband resources and efforts for serious threats. Blue may choose not to respond to minimize feedback provided to Red by any action Blue would take, allow the collection of forensic evidence over time to reinforce future anticipated legal action, ascertain Red intentions and information on Red's *modus operandi*, and to feign unawareness while mounting a significant counterstrike. Alternatively, this plateau may persist if Blue possesses no means of responding. This plateau can be disrupted by Red's ceasing of operations or Blue's countering Red's attack.

Plateau - 5: Defensive Target – This plateau results from Blue's decision to pursue an exclusively defensive posture against Red's strike. This allows Red to maintain the initiative and to strike without fear of retaliation. Blue may take this decision when defensive measures are certain and offensive measures are unable to be effectively employed or are very costly, ineffective, or legally problematic. Blue can allow this plateau to persist, however, the potential exists that future T+TTP employed by Red will eventually defeat Blue defenses resulting in damage. Adopting a purely defensive posture is in the mid- to long-term a dangerous proposition. Blue conducting an offensive counterstrike or Red ceasing its operations can disrupt this plateau.

Plateau - 6: Ineffective Retaliation – This plateau results from Blue's decision to conduct offensive operations against Red, but Blue's subsequent inability to effectively engage Red. This condition allows Red to persist in this plateau until Blue can effectively engage and defeat Red. The plateau will be disrupted if Blue's counterstrike is effective or Red ceases operations.

The objective of TAE is to foment conflict between two actors for one's own purposes. By inciting two Others to conflict, Self limits the resources of Others that can be employed against Self. It also allows Self to act as Blainey's proverbial Japanese fisherman, positioned to benefit from conflict between Others acting as fighting waterbirds, and thus able to "catch fish" (benefit from the conflict)

because the waterbirds are occupied with fighting and not fishing.[50] This aspect of conflict dictates that even neutral actors (Green) bear close watching.

TAE can be employed against Self. A danger is that Self will fail to recognize that it is the target of TAE by an Other. Should Self command a thorough knowledge of a specific Red, analysis of attacks may be able to confirm or deny that the true perpetrator of the attack is that specific Red.

There are two types of TAE that Self can employ: 1. Pre-strike TAE, and, 2. Post-strike TAE. Pre-strike TAE occurs prior to reaching node six on the variants' decision trees, and allows Self to engage Other(s) with TAE tools, tactics, techniques, and procedures (T + TTP) that will serve to deflect or lessen resources dedicated to subsequent strikes against Self. Pre-strike TAE is a better course of action for Self than Post-strike TAE, because it has the potential effect of preempting a strike against Self, and involving threats in conflict with each other, also serving Self's interests. Post-strike TAE occurs after having been targeted by an Other, and is designed to lessen an Other's subsequent resources that can be allocated against Self. Post-strike TAE accomplishes this by expanding the conflict to include Others, thus complicating Red's decision calculus, and forcing it to guard itself from multiple actors. Post-strike TAE may relieve pressure on Self, but it may also, but not necessarily, cost resources that could otherwise be employed against Red.

This study has explicated a framework from the paradigmatic level to the generic case model level that is suitable for countering emerging threats targeting critical infrastructure and population. It is functionally adequate to prescribe the strategic design process of national security policy countering such threats, and provides a better framework than the existing one for this purpose.

The Red, Gray, and Blue framework is a security environment approach to the formulation of national security policy. It is rooted in the newest of the national security policy subdisciplines: Critical Infrastructure Protection. However, it constitutes a beginning, and not a completion, of the task of assessing how this field should progress. This study is a contribution to the effort to demolish a past community paradigm during the current Kuhnian paradigmatic crisis.

Future research that applies Stalker's models and decision trees to threats, and encodes the models into automated applications is, in the author's view, the single most important direction of future research efforts among the many that have been raised in the study. This is based on the premise that nothing will serve to shift the national security elite policymakers' framework faster than demonstrated success of this study's concepts against a real-world emerging threat targeting critical

[50] Geoffrey Blainey, *The Causes of War*, 3rd ed., (New York: The Free Press, 1988), pp. 59-60.

infrastructure. This can only be accomplished by bridging George's gap against a real-world case in demonstrable fashion. To this end the most pressing need for further research is a major, applied project that incorporates the Red, Gray, and Blue framework, the threat typology, and the Stalker models into analysis of real-world attacks against US critical infrastructures and population.

Lakatos noted that "*revolutionary activists* believe that conceptual frameworks can be developed and also replaced by new, *better* ones; it is we who create our 'prisons' and we can also, critically, demolish them."[51] This study has attempted to make a contribution to demolishing the vestiges of the Cold War paradigm of national security, and replace it with a new framework capable of intelligently addressing emerging threats. As such, this study advocates "revolutionary activism" in redefining how national security policy is formulated to counter emerging threats targeting critical infrastructure and population using asymmetric, anonymous, and asynchronous strategies.

[51] Lakatos, "Falsification and the Methodology of Scientific Research Programmes," p. 104.

Appendix A: Coding Definitions

This appendix further extends the study's discussion from the paradigmatic level through the generic case models and decision trees. It explicates coding definitions as hard, operationalized tools for conducting analysis within the Red, Gray, and Blue framework. This appendix and the coding definitions are intended to provide a common point of departure for future researchers conducting analysis of emerging threats. As this study has made clear, a common vocabulary is a prerequisite to establishing a coherent research field. To this end, these definitions are contributions to this effort.

Identities:

Autonomous Terrorist Organization:

Definition: A group that is: 1. political in aims and motives, 2. violent, or threatens violence, 3. conducts operations designed to have far-reaching psychological effects beyond the immediate victim or target, 4. organized with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) and, 5. a subnational group or non-state entity.[1]

Usage: For groups conducting attacks, or threatening attacks, based on political aims, and not strongly affiliated with a patron state sponsor. For terrorists with patron states and acting in general accordance with their design, use the term "State Sponsored Terrorist Organization."

Non-usage: Do not use for individuals conducting terrorist acts in accordance with a Leaderless Resistance philosophy. Instead use the term "Lone Wolf."

Example: Abu Nidal Organization, Sendero Luminoso, Tupac Amaru, Gama'a al-Islamiyya, etc.

Cult:

Definition: A separate society resident within a host culture, but isolated from and rejecting the host's mainstream culture, with metaphysical and spiritual beliefs, values, and norms significantly different from the host culture.

Usage: Use for groups that share a belief system and lifestyle and that possess a common commitment to the collective's members beyond the host culture's norms for such relations.

---

[1] Bruce Hoffman, *Inside Terrorism*, p. 43.

Indications include a typically significant sacrifice is expected of members to the collective in financial, time, work, and other measures that are regarded as devotions. Cults frequently possess a rigid hierarchy, although it may be informally codified, capped by an authoritative figure, with a *de facto* class or caste system of recruits, initiates, disciples, and key leadership members.

Non-usage: Do not use for social clubs or organizations that may espouse different values than the host culture, but that do not expect shared lifestyles and heavy sacrifice from members.

Example: Aum Shinrikyo; The Heaven's Gate cult, that committed mass suicide at the appearance of the Hale – Bopp comet.

Economic Warfare Team:

Definition: A group that employs intelligence gathering techniques in conjunction with hostile activities to influence markets, market confidence, financial soundness of other actors, and to exploit data captured for their own economic ends. The team may be state-sponsored, a corporate entity, or a group without recognized legal standing. The activity of an Economic Warfare Team is of sufficient scope to potentially threaten vital interests of at least some system-level actors.

Usage: Theft of proprietary information, intellectual property, or sensitive data concerning products or services important to the economic health, viability, and security interests of another actor.

Non-usage: Petty violations of copyright or trademark for profit. Use the term Transnational Criminal Organization for wide-scale theft of information or activity that falls short of threatening the economic health of another actor or its security interests. For example, the international piracy of music CDs is not a security risk to a system-level actor, and would fall under the activity of a Transnational Criminal Organization.

Example: Commodity dumping is an example of an economic warfare team technique, as is currency speculation or dumping that threatens the stability of another actor's currency or economy.

Fringe Group:

Definition: A group that is outside of mainstream political society within its own culture. Significant ideological and societal beliefs are rejected, and commitment is evident to replace these beliefs with the group's beliefs, frequently with violent means.

Usage: Use for groups that exercise extreme political activism supporting values or an ideology not accepted by the mainstream culture of the society in which it is active.

Non-usage: Do not use for passive, non-violent groups that may hold even radically different beliefs.

Example: The Animal Liberation Front.

Hackers:

Definition: Individuals or a group attacking networks.

Usage: Use for individuals, clubs, and ad hoc groups that attack or attempt to penetrate networks.

Non-usage: Don't use for non-malicious attempts to penetrate a network, for example, as may be caused by a newly-hired individual, believing they are an authorized user, attempting to access a restricted network out of a mistaken understanding or poor training of allowed actions, authorities, and access. (However, some hackers may employ this excuse if discovered and confronted.)

Example: Cult of the Dead Cow.

Information Warfare Team:

Definition: A team, group, or network of personnel formed by a state, non-state actor, or non-hierarchical organization to conduct information operations as a primary responsibility. The team does not have to be permanent, but may be an ad hoc group to accomplish a specific mission. The mission may be either offensive or defensive in nature, or both.

Usage: Groups formed by state or non-state actors with the mission to conduct cyberstrikes against another actor's infrastructures during conflict; the so-called Tactical Internet Response Team as used by the Animal Liberation Front.

Non-usage: Do not use for the case of a sole hacker attacking or defacing a web site.

Example: National Intelligence Services information warfare teams.

Lone Wolf:

Definition: An individual or a few individuals conducting malicious, violent activity in support of his (their) own purposes and objectives.

Usage: The term "Lone Wolf" does not necessarily and strictly mean a sole individual. Frequently an individual may have a support network, or may be assisted in his or her attacks by a very few individuals. The Lone Wolf is the key player or leader. The Lone Wolf demonstrates a method of operating that focuses key activity within his power and control. The Lone Wolf follows his own direction, and is not an agent of a higher authority that provides operational directives.

Non-usage: Do not use for the employment of a single individual for a tactical strike, directed by a higher actor. For example, an assassin conducting operations in accordance with instructions from a political actor, either state or non-state, is not a Lone Wolf, but an agent of the higher actor.

Example: Timothy McVeigh, the Oklahoma City Bomber, was a Lone Wolf actor, although he did have a small support network of others.

Paramilitary Group:

Definition: A group characterized by a quasi-military structure that possesses significant armaments and plans or employs force as the principle means of accomplishing its objectives.

Usage: Use for groups that, regardless of ideology or other beliefs, exhibit an organizational structure that is designed to facilitate military-like, direct action operations employing violence. The term paramilitary group is not an exclusive classification, as a cult or fringe group may also be a paramilitary group.

Non-usage: Do not use for groups that do not plan or intend to employ violence. Although some social clubs meet to shoot weapons, may be constituted by a relatively homogenous core of values and other characteristics, and may even be organized in a quasi-military structure with honorary titles or ranks, they are not paramilitary groups. For example, a local skeet shooting club may have an organizational structure designated by terms like section or squad, may have a so-called "Colonel" as the organization's director, and may have a shared value system, but they do not intend the violent overthrow of a legitimate government. This would not constitute a paramilitary group.

Example: The Private Military Company (PMC) Sandline International.

Spy:

Definition: An individual or small group that conducts intelligence gathering through covert methods.

Usage: Use this term to classify an actor gathering intelligence from another actor using covert or deceptive means.

Non-usage: Do not use this term to describe an actor engaged in fact gathering for other than intelligence purposes, such as a journalist conducting an investigation.

Example: Former FBI Agent Robert P. Hannsen.

State-Sponsored Terrorism:

Definition: A group that is: 1. political in aims and motives, 2. violent, or threatens violence, 3. conducts operations designed to have far-reaching psychological effects beyond the immediate victim or target, 4. organized with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) and, 5. a subnational group or non-state

entity,[2] and that additionally, 6. has logistical, training, intelligence and other support from a state actor, and conducts attacks in accordance with some operational guidance from that state actor.

Usage: When the traits described in the full description are met.

Non-usage: Do not confuse with the "AutoTerr" code, which has first 5 traits, but lacks state actor support and operational guidance traits.

Example: Hizbollah, when working under direction and with support of Iran.

Insider:

Definition: An individual or small group that is trusted by its victim, and has access to information or targets and uses this trusted access to inflict damage on the trusting actor.

Usage: Use for cases where employees attack their employers and are enabled by the degree of access they intrinsically possess as employees. The term connotes a connection between the access an individual has and the type of illicit activity the individual engages in. For example, an employee at a high-tech firm that steals the source code of a software project and sells it to a competitor is an insider.

Non-usage: Do not use for criminal activity within an organization but not related to the organization's purpose, degree of trust, or access to systems. For example, an employee at a high-tech firm caught selling drugs is not an "insider," but is a criminal.

Example: The May 2001 theft of Lucent Technologies PathStar system source code by three Chinese nationals employed by Lucent.

Transnational Criminal Organization:

Definition: A regional or global organization that operates without regard for international borders in a networked, coherent fashion to perpetrate crimes.

---

[2] Bruce Hoffman, *Inside Terrorism*, p. 43.

Usage: Use for organizations that operate in multiple states to accomplish transnational operations involving criminal activity of significant scale. Typically these organizations will command significant logistical capabilities and the ability to launder money.

Non-usage: Do not use for very limited criminal operations that have no effect on a system-actor. For example, the smuggling of limited amounts of petroleum in a handful of fuel trucks across the border between two states by a few family members is not a transnational criminal organization.

Example: The Russian Mafia, Colombian drug cartels.

State:

Definition: A state actor, recognizable by attributes of diplomatic recognition from other states, possession of territory, institutions of government, legal monopoly of coercive power, and *de jure* sovereignty within its borders.

Usage: Countries that have diplomatic ties, territory, and government institutions. United Nations recognition is one possible, but not necessary, characteristic.

Non-usage: Revolutionary groups that challenge the state's authority, even if in possession of significant territory.

Example: The United States of America, France, England, and Spain are examples of states.

Transnational Actor:

Definition: An individual, group, or large organization that operates on a regional or global scale, and employs elements of power beyond the control of any state.

Usage: Use for major international corporations, networks of international business associates that share a common objective, special interest groups organized to support a specific agenda, and other actors that work toward a common purpose beyond the control of a state in a unified fashion to achieve a specific goal.

Non-usage: Do not use for a company or group based in a single country that however conducts business internationally.

Example: International Monetary Fund, Greenpeace, IBM.

Means:

Assassination:

Definition: The killing of a key individual or individuals in pursuit of a political, ideological, or other objective.

Usage: Use for the targeting of key individuals whose death will have an influence on other actors in the political or other arenas. The killing of a key leader in an enemy's organization to deny the enemy leadership and promote confusion surrounding succession is an example of assassination. The target of an assassination typically plays a key, even if bureaucratic, role in policy.

Non-usage: Do not use for cases of murder where political or system-level effect is not the intent. For example, the killing of even a key individual resulting from a failed robbery is not an assassination, but a murder committed during an attempted robbery. Some effects resembling those of an assassination may still result from such a criminal murder, however the action of the criminal was not politically motivated, nor was the key individual targeted out of intent to achieve a political effect.

Example: The assassination of Egyptian leader Anwar Sadat.

Biological Agent:

Definition: A microorganism that causes disease in personnel, plants, or animals or causes the deterioration of materiel.[3]

Usage: Use to describe employment of a microorganism as a weapon.

---

[3] US Department of Defense Dictionary, at http:// www.dtic.mil/doctrine/jel/doddict/data/b/00888.html.

Non-usage: Do not use to describe a naturally occurring incident that has no threat involvement.

Example: The case of followers of the Bhagwan Shree Rajneesh 1984 poisoning of the population of Dalles, Oregon with salmonella typhimurium bacteria.

Bomb:

Definition: Any explosive device.

Usage: Use when the means has as its primary function the creation of an explosion.

Non-usage: Do not use when an explosion is an unintended effect of the device's design or employment. For example, employing a rifle may result in an explosion if directed against a fuel storage tank, but the means employed was not a bomb.

Example: The Oklahoma City Bombing was a case where a bomb was employed.

Chemical Agent:

Definition: "A chemical substance which is intended...to kill, seriously injure, or incapacitate personnel through its physiological effects."[4]

Usage: Use for nerve agents, blister agents, blood agents, various gases and improvised chemical weapons.

Non-usage: Do not use for tear gas or other riot control agents, herbicides, and smoke.

Example: Aum Shinrikyo's attack of the Tokyo subway station used Sarin, a nerve agent.

Cyberstrike:

Definition: A concerted attack from, through, and against computer systems to deny, damage, disrupt, alter, or destroy the ability of the targeted system to function as intended. The result is

[4] Ibid.

systemic in effect, and typically will affect a critical infrastructure system. Additionally includes weapons that target the deep structure of cyberspace itself, such as Electromagnetic Pulse (EMP).

Usage: A computer attack designed to cause the failure of an electrical grid. Employment of an EMP weapon. A concerted attack to disrupt a network.

Non-usage: A sole hacker's penetration of a single computer to steal credit card numbers.

Example: The February 2000 denial of service attacks against major corporations.

Direct Action:

Definition: The direct, physical employment of violent attack, whether by a uniformed, armed force, guerrilla, or terrorist forces.

Usage: A guerrilla attack against a military force's camp. Launching a cruise missile against an opponent's facility.

Non-usage: Don't use for cyberstrikes or non-physical information operations.

Example: Israeli attack of Osirik nuclear facility in Iraq was a direct action strike.

Espionage:

Definition: Theft or unauthorized appropriation of trade secrets, proprietary or classified information.

Usage: Use for incidents where the intent is to gain knowledge illicitly.

Non-usage: Do not use for incidents where the objective is to gain material or equipment with no information content or worth.

Example: The unauthorized downloading of classified information from a penetrated computer network is espionage.

Extortion:

Definition: The application of force to compel a target to surrender concessions of financial or trade worth. The force is not limited to naked aggression, but includes trade sanctions. Actors capable of extortion range form terrorists to states.

Usage: Trade sanctions. A significant case of blackmail.

Non-usage: Theft.

Example: Economic or trade sanctions. Demand for ransom for a key individual.

Deception:

Definition: An act intended to create a false image or impression.

Usage: Use when employed by a threat to gain an objective through false representation or other deception.

Non-usage: Do not use when deception is used to facilitate the employment of different means.

Example: The creation of a deceptively framed social relationship to gain access to sensitive information.

Information Operation:

Definition: Information operations involve actions taken to affect adversary information and information systems while defending one's own information and information systems. IO target information or information systems in order to affect the information-based process, whether human or automated. Such information dependent processes range from National Command Authorities-level decision making to the automated control of key commercial infrastructures such as telecommunications and electric power.

Usage: Deception regarding economic indicators

Non-usage: Do not use for computer network attack, instead use the code "Cyberstrike."

Example: Operations security, deception, psychological operations, electronic warfare, physical attack/destruction, special IO.

Nuclear Weapon:

Definition: "A complete assembly (i.e., implosion type, gun type, or thermonuclear type), in its intended ultimate configuration which, upon completion of the prescribed arming, fusing, and firing sequence, is capable of producing the intended nuclear reaction and release of energy."[5]

Usage: Use for employment of a device designed to release nuclear energy.

Non-usage: Do not use for a device that is designed to emit radiological energy. For example, the employment of a radiological agent, even when coupled with a conventional bomb to disseminate the radiological agent, is not a nuclear weapon.

Example: Any identified nuclear weapon system.

Radiological Agent:

Definition: An agent characterized by the "spontaneous emission of radiation, generally alpha or beta particles, often accompanied by gamma rays, from the nuclei of an unstable isotope."[6]

Usage: Use to characterize a means that incorporates as a principle design purpose materials in any form that emit radioactive energy sufficient and intended to cause harm to people, animals, or materials.

Non-usage: Do not use for miniscule amounts of radioactive materials that are not capable or intended to cause harm; for example, a luminous watch dial that is incorporated into a conventional bomb as a timer is not employed as a radiological agent, but a bomb.

---

[5] DoD Dictionary.
[6] Ibid.

Example: The 1995 Chechen separatists group's employment of Cesium – 137 in Izamilovski Park in Moscow.

Economic Attack:

Definition: Attack of an opponent's economic interests through trade sanctions, freezing of financial and other assets, currency destabilization, or hostile trade practices like dumping.

Usage: Freezing of assets, trade sanctions, dumping, currency destabilization, economic embargoes.

Non-usage: Mobilization or spending of own funds for defensive or offensive measures. That is simply employment of a resource in a conflict that enables attacks, it is not an attack in itself.

Example: Freezing assets.

Genetic Agent:

Definition: Any agent capable of targeting and damage based on DNA sequences or other genetic characteristics.

Usage: Use for pathogens that are designed to act by interaction with genetic material.

Non-usage: Do not use for biological agents or toxins that are not enhanced in their effects or targeting with genetic capabilities.

Example: A genetically-engineered pathogen that targets populations, crops, or livestock based on specific genetic attributes.

Crime:

Definition: A violation of a law.

Usage: Use for means that are forbidden by a law.

Non-usage: Do not use for acts where the means is illegal, but this illegality is not directly relevant to achieving the ends. For example, bombing is illegal, but the means employed that is directly relevant to the effects desired is a bomb, not the commission of a crime.

Example: Theft of research documents from a researcher's university office would be an example of employing a crime to achieve an end.

Targets:

Banking and Finance:

Definition: "A critical infrastructure characterized by entities, such as retail and commercial organizations, investment institutions, exchange boards, trading houses, and reserve systems" and other activities. It is composed of five principal sectors: banks, financial service companies, payment systems, investment companies, and securities and commodities exchanges.[7]

Usage: Use to describe any target connected with the five subsystem components to a degree that disruption or destruction would undermine confidence in the integrity of the US financial system.

Non-usage: Do not use to describe targeting that is not of the scale to affect consumer and other actor confidence in the system. For example, embezzlement of a specific bank's cash holdings by a teller does not constitute targeting the US banking and finance system.

Example: A hypothetical example that would constitute targeting the US banking and finance system would be a cyberstrike that corrupted the major stock exchanges' databases and information.

Biological and Genetic Research / Production / Storage Installations:

Definition: A facility or researcher(s) that possesses and creates knowledge regarding advanced biological or genetic science.

Usage: Use to describe government, private, and academic institutions, laboratories, and personnel that control access to advanced knowledge, technology, equipment, and stores of biological or genetic science materials or research.

---

[7] *Critical Foundations: Protecting America's Infrastructures*, The Report of the President's Commission on Critical Infrastructure Protection (Washington, DC, 13 October 1997), quote p. B-1, p. A-37.

Non-usage: Do not use for common-knowledge applications that have little intrinsic utility for creating WME.

Example: The Center for Disease Control's research facilities; a research university's knowledge banks.

Business:

Definition: A private organization conducting operations involving competition in a market.

Usage: Use as a term to describe targeting a business sector or major corporate actor.

Non-usage: Do not use to describe a government institution or facility.

Example: Theft of high-technology trade secrets or sensitive proprietary information by a foreign national.

Chemical Research / Production / Storage Installations:

Definition: A facility or researcher(s) that possesses and creates knowledge regarding advanced chemistry.

Usage: Use to describe government, private, and academic institutions, laboratories, and personnel that control access to advanced knowledge, technology, equipment, and stores of chemical science materials or research.

Non-usage: Do not use for common-knowledge applications that have little intrinsic utility for creating WME.

Example: US Department of Defense laboratories conducting research on chemical weapon countermeasures and defensive technologies.

Continuity of Government:

Definition: The survival of the US Constitutional form of government in the face of a catastrophic crisis.

Usage: Use to describe as the target when the effects of an emerging threat's attack would jeopardize the continued order of the US government.

Non-usage: Don't use to describe protests against the government, or disobedience to laws that does not threaten the continued order of the US governmental institutions and processes.

Example: A hypothetical example would be a biological agent attack targeting the assembled US Congress with the pathogen released in such a manner as to threaten the health of the US Senators and Congressmen present, with the intent to cause the US government to cease activities facilitating governance.

Diplomatic / Political Target:

Definition: An institution, facility, group or individual that has formal diplomatic credentials or is a key individual with political authority and symbolic importance.

Usage: Use to describe as a target when a threat attack engages an institution or individual commonly recognized as a political or diplomatic actor.

Non-usage: Do not use for attacks that do not include the diplomatic or political quality of the actor in its targeting criteria.

Example: A US Ambassador, Embassy, or Consulate.

Electric Power System:

Definition: "A critical infrastructure characterized by generation stations, transmission and distribution networks that create and supply electricity."[8]

Usage: Use to describe as a target any facility or subsystem that supports the electric power infrastructure.

---

[8] *Critical Foundations*, p. B-2.

Non-usage: Do not use for attacks on infrastructures, like telecommunications, that may cascade and spill-over into the electric power system as a secondary effect, and not the primary effect desired by an emerging threat actor.

Example: A power generation plant.

Emergency Services System:

Definition: "A critical infrastructure characterized by medical, police, fire, and rescue systems and personnel that are called upon" during emergencies.[9]

Usage: Use to describe as a target when a threat attack would disrupt, delay, or otherwise hamper critical services, such as fire, listed above.

Non-usage: Do not use to describe as a target when disruption is an unintended secondary effect of an attack on another critical infrastructure, e.g., electrical power.

Example: A denial of service attack against the emergency 911 telephone service of a major city.

Water System:

Definition: "A critical infrastructure characterized by the sources of water" and facilities that supply water.[10]

Usage: Use for attacks targeting water supply, safety, reliability, and quality.

Non-usage: Do not use for attacks that disrupt water supply as a secondary effect.

---

[9] Ibid.
[10] Ibid.

Example: A direct action strike against a water treatment plant to contaminate the water.

Government Installations:

Definition: A facility, agency, or personnel employed in supporting the US government.

Usage: Use to describe as a target when the desired effect of the attack is to cause either real or symbolic harm to the US government through attacking its agents.

Non-usage: Do not use when the primary purpose is not to cause harm to the US government, but is achieved as a secondary effect.

Example: The bombing of the Alfred P. Murrah Federal Building in Oklahoma City.

Law Enforcement:

Definition: Organizations and individuals charged with serving the public in a police capacity, or an organization charged with enforcement of the law.

Usage: Use for attacks against the FBI, police departments, county sheriffs, and other law enforcement personnel and agencies.

Non-usage: Do not use when the targets quality as a law enforcement actor is not a criterion in targeting the target.

Example: The FBI.

Military Installations:

Definition: A facility, agency, or personnel employed in supporting the US Department of Defense.

Usage: Use to describe as a target when the desired effect of the attack is to cause either real or symbolic harm to the US military through attacking its facilities or personnel.

Non-usage: Do not use when the primary purpose is not to cause harm to the US military, but is achieved as a secondary effect.

Example: The October 2000 boat-bomb suicide attack of the USS Cole in Yemen.

Nuclear Research / Production / Storage Installations:

Definition: A facility or researcher(s) that possesses and creates knowledge regarding advanced nuclear science.

Usage: Use to describe government, private, and academic institutions, laboratories, and personnel that control access to advanced knowledge, technology, equipment, and stores of nuclear science materials or research.

Non-usage: Do not use for common-knowledge applications that have little intrinsic utility for creating WME.

Example: US Department of Energy national laboratories and facilities.

Oil and Gas System:

Definition: "A critical infrastructure characterized by the production and holding facilities for natural gas, crude and refined petroleum" and other fuels, as well as the transportation systems supporting the infrastructure.[11]

Usage: Use for attacks targeting the infrastructure system and designed to disrupt supplies.

Non-usage: Do not use for attacks where the disruption of the oil and gas system is not the desired effect.

Example: Interdicting a petroleum pipeline.

Public Health System:

---

[11] Ibid, p. B-2.

Definition: The critical infrastructure of private and public health care providers, suppliers, and facilities.

Usage: Use to describe as a target when the desired effect is to disrupt or deny the provision of health care to the population.

Non-usage: Do not use when a health care infrastructure is affected by unforeseen, secondary effects of the attack.

Example: The large-scale contamination of medical supplies, e.g., vaccines at a plant during a production run, that degrades the ability to provide health care to the US population.

Telecommunications / Information System:

Definition: "A critical infrastructure characterized by computing and telecommunications equipment, software, processes," facilities, and personnel.[12]

Usage: Use to describe as a target when the desired threat effect is to disrupt or deny communications.

Non-usage: Do not use for unplanned secondary effects.

Example: Bombing of a critical node in the telecommunications architecture.

Transportation System:

Definition: "A critical infrastructure characterized by the physical distribution system critical to supporting the national security and economic well-being" of the United States.[13]

Usage: Use to describe as a target when the desired threat effect is to disrupt or deny the transportation of important commodities required for the economic vitality of the United States.

---

[12] Ibid.
[13] Ibid, p. B-3.

Non-usage: Do not use when attack of a transportation asset is ancillary to the intended purpose of the attack. For example, the cutting of a small oil pipeline with the intended effect of contaminating the water supply of a major city would be classified as an attack against the water supply, not the transportation infrastructure.

Example: Interdiction of the national aviation control system.

Population:

Definition: The people residing within the United States.

Usage: Use to characterize as a target when a threat's desired effects and attack design is intended to cause massive casualties.

Non-usage: Do not use as the target designation when casualties are the result of an attack that targeted a different system, or the effect of causing casualties could not have been foreseen. A hacker that brings down a corporate computer network that as a fluke causes a casualty can not be said to have been targeting the population. This is not the case where a hacker targets a critical infrastructure where an interruption of service could reasonably be expected to cause casualties.

Example: A population concentration in a major metropolitan city.

Food:

Definition: The food supply is a critical infrastructure characterized by a logistical chain from production through distribution to consumption.

Usage: Use when the intended effect of an attack is to cause the loss of confidence or disruption of production or distribution of food.

Non-usage: Do not use when food is used as a simple vehicle or vector for poisoning, similar to the case of followers of the Bhagwan Shree Rajneesh 1984 poisoning of the population of Dalles, Oregon with salmonella typhimurium bacteria. In this case the target was the population.

Example: Employment of Sugar-beet curly top, Hoof and Mouth disease, corn stunt, E. coli, Hoja Blanca, rice blight, corn blight, sugarcane wilt, potato blight, rice blast, or other microorganisms targeting food crops, sources and production.

Ends:

Obtain WME:

Definition: This is an end of some threats: the obtaining of a WMD or CBNR agents, sophisticated cyberweaponry, research that will facilitate their own development programs, or materials to further their development of weapons.

Usage: Could at a second-level of effects be a Means code, if theft is designed to ultimately gain political influence or financial gain. Use for theft of a weapon or critical knowledge, technology, or materials.

Non-usage: Do not use for an attack on a WMD/CBNR site that is not motivated to obtain WMD/CBNR, such as an environmental protest against a nuclear research facility to protest nuclear energy policy.

Example: Computer penetration of the Department of Energy's national laboratories resulting in theft of research, specifications, and plans.

Contain the United States:

Definition: A strategy of limiting the influence of the United States geographically, by issue, or in a specific forum or other dimension.

Usage: Use for a strategy designed to limit the access and influence of the United States as an objective. For example, a policy that forbids the import of goods made in the United States, but permits the import of other actors' goods, is a form of a trade strategy to contain the United States. Strategies designed to contain the United States are not limited to the economic sphere.

Non-usage: Do not use for the exercise of a policy where the motivation is not tied to the United States as the specific identity to be denied. For example, a policy of import restrictions on a

specific food designed to protect an indigenous, politically powerful agricultural constituency and applied against all actors evenly is not a strategy to contain the United States, although it is a trade and free-market issue.

Example: The targeted exclusion of US goods from a country is an economic strategy to contain the United States' influence in a specific market.

Economic Advantage:

Definition: The goal of obtaining a competitive advantage in the economic realm. The actor can be a state or non-state actor. The advantage can be tangible or intangible.

Usage: Economic espionage to obtain information on new product development.

Non-usage: Routine competition in submitting bids against projects.

Example: A state's intelligence agency releasing intelligence regarding a foreign competitor to a national corporation.

Expand Power:

Definition: An objective of increasing absolute or relative measures of power.

Usage: Use to describe as the end for scenarios where the increase in absolute or relative capabilities is an operational goal.

Non-usage: Do not use for unforeseen consequences; for example the defeat of an invading force may result in the expansion of power, however, the defense was not undertaken to expand power, but to survive. For example, the case of the 1973 Yom Kippur war.

Example: The Nazi aggression and offensives of early World War II. For a non-state actor, the internecine warfare between organizational crime syndicates over territory.

Financial Gain:

Definition: The goal of obtaining wealth, in either currency, commodities, or other vehicles of wealth transfer.

Usage: Electronic theft through computer transfer of funds. Obtaining mineral rights through coercion, extortion, or provision of services.

Non-usage: Routine profits through normal trade in legal commodities or services.

Example: Theft of funds through illicit manipulation of computer systems. The occupation of areas in Angola by the PMS Sandline, Inc. is motivated by financial gain through the creation of a diamond cartel.

Hate:

Definition: Extreme hostility and anger.

Usage: Use as an end for scenarios where the motivation for an operation is to inflict harm based only from motivations concerning the target's intrinsic characteristics.

Non-usage: Do not use to describe as an end an operation where other motivations trump hatred as a motive. For example, demonizing the enemy in war is a recurring phenomenon, yet in most cases hatred is not the end motivating war in the first instance.

Example: Genocide.

Ideology:

Definition: A sociopolitical body of concepts.

Usage: Use to describe as an end when the motivation for conflict is based on sociopolitical concepts.

Non-usage: Do not use when the conflict is prosecuted out of other motivations, with ideology used as a fabricated *causus belli*.

Example: The Cold War was an ideological conflict.

Metaphysical:

Definition: A transcendent cause.

Usage: Use to characterize as an end when a spiritual goal is invoked as justification for conflict.

Non-usage: Do not use for scenarios where the blessing of a higher power is later claimed, following the outbreak of conflict.

Example: Jihad.

National Security Advantage:

Definition: The goal of obtaining an advantage over an opponent to further security of the actor. The actor can be a state or non-state actor. The advantage can be tangible or intangible, in any instrument of power.

Usage: When the goal is a quantifiable material advantage in the military realm. When the goal is the intangible advantage conferred by an information advantage in diplomatic negotiations.

Non-usage: Routine processes associated with security of the actor, such as recruiting military personnel, or holding internal meetings.

Example: The acquisition of a negotiating opponent's initial bargaining position and subsequent fall-back strategies through espionage. A direct action strike against an opponent's military facility to gain favorable correlation of forces achieves a national security advantage.

Political Change:

Definition: Political Change is defined as the goal of materially affecting a change in another actor's political structure through a deliberate strategy of attack using any instrument of power.

Usage: Defeat of an enemy in overt, military conflict and occupation of the actor's homeland, with a security policy of radical political change forced on the actor. A guerrilla movement's efforts to overthrow the current regime.

Non-usage: Routine participation in an electoral or political process, within legal boundaries.

Example: Occupation of Japan after World War II. The Sendero Luminoso's efforts in Peru. The IRA.

Political Influence:

Definition: The goal of obtaining influence in a political system as a result of a strategy. The influence is for furthering interests of the actor pursuing the strategy.

Usage: Foreign intelligence services covertly funneling monies to another actor's politicians.

Non-usage: Routine diplomatic statements designed to advance a perspective.

Example: The co-opting of Colombian politicians by the drug cartels.

Retaliation:

Definition: To seek revenge or retribution for another actor's previous actions.

Usage: Use to characterize as an end when the primary motivation for conflict is to inflict injury as reciprocity for previous injury done.

Non-usage: Do not use when retaliation is invoked as an *a fortiori* argument for prosecuting conflict.

Example: Operation El Dorado Canyon, the US bombing of Libya during the Reagan Administration, was retaliation for a terrorist bombing by Libyan agents.

Survival:

Definition: The preservation of an actor.

Usage: Use to characterize as an end in a scenario where the actor is motivated primarily to survive.

Non-usage: Do not use to characterize as an end in a scenario where defeat in the conflict would not cause the demise of the actor.

Example: The defense of the Kuwaiti forces against the Iraqi attack in 1991 was motivated by survival of Kuwait as a political actor.

Vandalism:

Definition: Willful or malicious destruction.

Usage: Use to characterize as an end when no tangible gain is realized by the attacker, and none is expected.

Non-usage: Do not use to characterize as the end of a conflict if the vandalism results from operations, and did not motivate the operations. Combatants burning a building unnecessarily does not mean the conflict was initiated to cause the vandalism.

Example: Defacement and denial of service of web sites and computer networks accomplished as an end in itself.

Bibliography

Acheson, Dean, *Present at the Creation: My Years in the State Department* (New York: W.W. Norton & Company, 1969).

After Action Report: Alfred P. Murrah Federal Building Bombing, 19 April 1995 in Oklahoma City, Oklahoma (Oklahoma City, OK: Oklahoma Department of Civil Emergency Management).

Aldrich, John H., and Forrest D. Nelson, *Linear Probability, Logit, and Probit Models*, Series on Quantitative Applications in the Social Sciences, No. 07-045, Sage University Papers (Beverly Hills, CA: Sage, 1984).

Allison, Graham, *et al*, *Defending the United States Against Weapons of Mass Destruction*, Open Letter to the US Senate (2 June 1997).

Allison, Graham T., *Essence of Decision: Explaining the Cuban Missile Crisis* (New York: HarperCollins Publishers, 1971).

Anderson, James E., *Public Policymaking* (New York: Houghton Mifflin, 1997).

Anderson, Robert H., Phillip M. Feldman, Scott Gerwehr, et al, *Securing the US Defense Information Infrastructure: A Proposed Approach* (Santa Monica, CA: RAND, 1999).

Anderson, Robert H., Phillip M. Feldman, Scott Gerwehr, Brian Houghton, Richard Mesic, John D. Pinder, Jeff Rothenberg, and James Chiesa, *Establishing Minimum Essential Information Infrastructure for U.S. Defense Systems* (Santa Monica, CA: RAND, 2000).

Andrews, Peter, *Electronic Identities: Secure Masks*, IBM Executive Tek Report (Armonk, NY: IBM, 14 August 2000).

Art, Robert J., and Kenneth N. Waltz, *The Use of Force: Military Power and International Politics*, 5th ed., (New York: Rowman & Littlefield Publishers, 1999).

Axelrod, Robert, *The Evolution of Cooperation* (New York: Basic Books, 1984).

Axelrod, Robert, "The Rational Timing of Surprise," *World Politics*, Vol. 31 (January 1979), pp. 228-246.

Axelrod, Robert and Douglas Dion, "The Further Evolution of Cooperation," *Science*, Vol. 242 (9 December 1988), pp. 1385-1389.

Baumgartner, Frank R., and Bryan D. Jones, *Agendas and Instability in American Politics* (Chicago: University of Chicago Press, 1993).

Bennett Requires Pentagon to Report on Cyber-Defense Plans, Press Release (Washington, DC: US Senate, 8 June 2000).

Blainey, Geoffrey, *The Causes of War*, 3rd ed. (New York: The Free Press, 1988).

Boyd, Charles G., *Testimony before the Joint Meeting of the Subcommittee on National Security and the Subcommittee on Economic Development* (Washington, DC: US House of Representatives, 24 April 2001).

Brodie, Bernard, ed., *The Absolute Weapon* (New York: Harcourt Brace, 1946).

Brown, Michael E., Sean M. Lynn-Jones, and Steven E. Miller, eds., *The Perils of Anarchy: Contemporary Realism and International Security* (Cambridge, MA: The MIT Press, 1995).

Bruner, Jerome, *Acts of Meaning* (Cambridge, MA: Harvard University Press, 1990).

Bueno de Mesquita, Bruce, "The End of the Cold War: Predicting an Emergent Property," *Journal of Conflict Resolution*, Vol. 42, No. 2 (April 1998), pp. 131-155.

Bull, Hedley, *The Anarchical Society* (New York: Columbia University Press, 1977).

Buntine, Wray, "Graphical Models for Discovering Knowledge," in Usama M. Fayyad, Gregory Piattetsky-Shapiro, Padhraic Smyth, and Ramasamy Uthurusamy, eds., *Advances in Knowledge Discovery and Data Mining* (Cambridge, MA: MIT Press, 1996), pp. 59-82.

Buzan, Barry, Charles Jones, and Richard Little, *The Logic of Anarchy: Neorealism to Structural Realism* (New York: Columbia University Press, 1993).

Campbell, George K., "Security Expectations for Transnational Corporations," in Max G. Manwaring, ed., *...to insure domestic Tranquility, provide for the common defence...* (Carlisle, PA: Strategic Studies Institute, 2000).

Carmines, Edward G., and Richard A. Zeller, *Reliability and Validity Assessment*, Series on Quantitative Applications in the Social Sciences, No. 07-001, Sage University Papers (Beverly Hills, CA: Sage, 1979).

Carr, E.H., *The Twenty Years' Crisis: An Introduction to the Study of International Relations* (London: Macmillan, 1939).

Cave, Jonathan, *Introduction to Game Theory* (Santa Monica, CA: RAND, 1987).

Chapman, Frederick Spencer, *The Jungle is Neutral* (New York: W.W. Norton & Company, 1949).

Clark, Richard A., *Memorandum* (Washington, DC: National Security Council, 19 July 2000).

Clausewitz, Carl von., *On War*, Michael Howard and Peter Paret, eds. (Princeton, NJ: Princeton University Press, 1976).

Clinton, William J., *Remarks by the President at the United States Naval Academy Commencement* (Annapolis, MD: Office of the Press Secretary EOP, 22 May 1998).

Clinton, William J., *A National Security Strategy for a New Century* (Washington, DC: Executive Office of the President, December 1999).

Cohen, William S., *Personal Accountability for Force Protection at Khobar Towers* (Washington, DC: Office of the Secretary of Defense, 31 July 1997).

Copi, Irving M., *Introduction to Logic*, 4th ed. (New York: Macmillan Publishing, 1972).

Corbett, Julian S., *Some Principles of Maritime Strategy* (Annapolis, MD: Naval Institute Press, 1988).

Commerce Secretary Mineta Announces New Information Technology (IT) Information Sharing and Analysis Center (ISAC), US Department of Commerce Press Release 01-16-01 ITSAC (Washington, DC: US Department of Commerce, 16 January 2001).

Critical Foundations: Protecting America's Infrastructures, Report of the President's Commission on Critical Infrastructure Protection (Washington, DC: PCCIP, 13 October 1997).

Deutch, John M., Director, Central Intelligence Agency, *Remarks to Scientists at Los Alamos* (Washington, DC: CIA Office of Public Affairs, 23 May 1996).

Department of Defense Dictionary of Military and Associated Terms, Joint Pub 1-02 (Washington, DC: Office of the Joint Chief of Staff, 2001).

Department of Defense Regulation 5240.1-R: DoD Intelligence Activities (Washington, DC: Department of Defense, 25 April 1988).

Doctrine for Intelligence Support to Joint Operations, Joint Publication 2-0 (Washington, DC: Chairman of the Joint Chiefs of Staff, 9 March 2000).

DoE: Fossil Energy, US Department of Energy Fact Sheet (Washington, DC: US Department of Energy, 29 April 1997).

Elman, Colin, and Miriam Fendius Elman, "Lakatos and Neorealism: A Reply to Vasquez," *The American Political Science Review*, Vol. 91, No. 4 (December 1997), pp. 923-926.

Executive Order 12333: United States Intelligence Activities (Washington, DC: Executive Office of the President, 4 December 1981).

Executive Order 12938: Proliferation of Weapons of Mass Destruction (Washington, DC: Executive Office of the President, 14 November 1994).

Executive Order 13010: Critical Infrastructure Protection (Washington, DC: The Federal Register, 17 July 1996).

Fayyad, Usama M., Gregory Piatetsky-Shapiro, Padhraic Smyth, and Ramasamy Uthurusamy, eds., *Advances in Knowledge Discovery and Data Mining* (Cambridge, MA: MIT Press, 1996).

Fidler, Stephen, "President Places NSC Back on Top," *Financial Times* (London: 11 April 2001).

Flynt, Bill, "Threat Convergence," *Military Review* (September – October 1999), pp. 2-11.

Flynt, Bill, "Threat Kingdom," *Military Review* (July – August 2000), pp. 12-21.

Fudenberg, Drew, and Jean Tirole, *Game Theory* (Cambridge, MA: MIT Press, 1991).

Gaddis, John Lewis, *Strategies of Containment: A Critical Appraisal of Postwar American National Security Policy* (New York: Oxford University Press, 1982).

Gaddis, John Lewis, "The Long Peace: Elements of Stability in the Postwar International System," *International Security*, Vol. 10, No. 4 (Spring 1986), pp. 99-142.

George, Alexander L., "The 'Operational Code': A Neglected Approach to the Study of Political Leaders and Decision-Making," *International Studies Quarterly*, Vol. 13, No. 2 (June 1969).

George, Alexander L., *Bridging the Gap* (Washington, DC: United States Institute for Peace Press, 1993).

George, Alexander L., "Some Guides for Bridging the Gap," *Mershon International Studies Review*, Vol. 38 (April 1994).

Gilpin, Robert, *War and Change in World Politics* (New York: Cambridge University Press, 1981).

Gilpin, Robert G., "No One Loves a Political Realist," *Security Studies*, Vol. 5, No. 3 (Spring 1996), pp. 3-26.

Gilpin, Robert, *The Political Economy of International Relations* (Princeton, NJ: Princeton University Press, 1987).

Gilpin, Robert, *The Challenge of Global Capitalism* (Princeton, NJ: Princeton University Press, 2000).

Glaser, Charles L., "Realists as Optimists: Cooperation as Self-Help," *International Security*, Vol. 19, No. 3 (Winter 1994/95).

Global Proliferation of Weapons of Mass Destruction: A Case Study on the Aum Shinrikyo, US Senate Government Affairs Permanent Subcommittee on Investigations Staff Statement (Washington, DC: US Senate, 31 October 1995).

Global Trends 2015: A Dialogue About the Future with Nongovernment Experts (Washington, DC: National Intelligence Council, 13 December 2000).

Hayden, Michael V., "NSA Head: Tech Weakness Makes US Vulnerable," *CBS 60 Minutes II* (12 February 2001).

Hayden, Michael V., "Remarks to the Kennedy Political Union of the American University," *National Security Agency Press Release*, 17 February 2000.

Heckerman, David, "Bayesian Networks for Knowledge Discovery," in Usama M. Fayyad, Gregory Piatetsky-Shapiro, Padhraic Smyth, and Ramasamy Uthurusamy, *Advances in Knowledge Discovery and Data Mining* (Cambridge, MA: MIT Press, 1996), pp. 273-306.

Hermann, Margaret G., "Introduction: A Statement of Issues," in Margaret G. Hermann and Thomas W. Milburn, eds., *A Psychological Examination of Political Leaders* (New York: Free Press, 1977).

Hobbes, Thomas, *Leviathan* (London: Penguin, 1985).

Hodge, James S., and James A Dewar, *Is It You or Your Model Talking? A Framework for Model Validation* (Santa Monica, CA: RAND, 1992).

Hoffman, Bruce, *Inside Terrorism* (New York: Columbia University Press, 1998).

Hopf, Ted, "The Promise of Constructivism in International Relations Theory," *International Security*, Vol. 23, No. 1 (Summer 1998), pp. 171-200.

Horak, Ray, *Communications: Systems and Networks*, 2nd ed. (Foster City, CA: M&T Books, 2000).

House Resolution 525: Preparedness Against Domestic Terrorism Act of 2001 (Washington, DC: US House of Representatives, 8 February 2001).

House Resolution 1292: Homeland Security Strategy Act of 2001 (Washington, DC: US House of Representatives, 29 March 2001).

House Resolution 1158: The National Homeland Security Act (Washington, DC: US House of Representatives, 21 March 2001).

Huntington, Samuel P., "The Clash of Civilization?" *Foreign Affairs*, Vol. 72, No. 3 (Summer 1993), pp. 22-49.

Interview of the President by the New York Times, White House Press Release, January 23, 1999 (Washington, DC: White House Office of the Press Secretary).

Jenkins, Brian M., "International Terrorism: A New Mode of Conflict," in David Carlton and Carlo Schaerf, eds., *International Terrorism and World Security* (London: Croom Helm, 1975).

Jervis, Robert, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976).

Jervis, Robert, "Cooperation Under the Security Dilemma," *World Politics*, Vol. 30, No. 2 (January 1978), pp. 167-214.

Jervis, Robert, "Perceiving and Coping with Threat," in Robert Jervis, Richard Ned Lebow, and Janice Gross Stein, *Psychology and Deterrence* (Baltimore: The Johns Hopkins University Press, 1985).

Johnson, Janet Buttolph, and Richard A. Joslyn, *Political Science Research Methods*, 3rd ed. (Washington, DC: CQ Press, 1995).

Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington, DC: Chairman of the Joint Chiefs of Staff, 9 October 1998).

Joint Special Operations Targeting and Mission Planning Procedures, Joint Pub 3-05.5 (Washington, DC: Chairman of the Joint Chiefs of Staff, 10 August 1993).

Kaplan, Morton A., "Variants on Six Models of the International System," in James N. Rosenau, ed., *International Politics and Foreign Policy* (New York: The Free Press, 1969), pp. 297-300.

Kennan, George F., *Memoirs: 1925-1950* (Boston: Little, Brown and Company, 1967).

Kennan, George F., "The Long Telegram," transcribed from *Foreign Relations of the United States, 1946, vol. VI: Eastern Europe, The Soviet Union*, US Department of State Publication 8470 (Washington, DC: Government Printing Office, 1969), pp. 696-709, part 5.

Keohane, Robert O., ed., *Neorealism and Its Critics* (New York: Columbia University Press, 1986).

Keohane, Robert O., and Joseph S. Nye, Jr., *Power and Interdependence: World Politics in Transition* (Boston: Little, Brown and Company, 1977).

Keohane, Robert O., and Joseph S. Nye, Jr., "Power and Interdependence in the Information Age," *Foreign Affairs*, Vol. 77, No. 5 (September/October 1998), pp. 81-94.

Khong, Yuen Foong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton: Princeton University Press, 1992).

Kingdon, John W., *Agendas, Alternatives, and Public Policies*, 2nd ed., (New York: HarperCollins College Publishers, 1995).

Kuhn, Thomas S., *The Structure of Scientific Revolutions*, 2nd ed. (Chicago: The University of Chicago Press, 1970).

Kuhn, Thomas S., *The Copernican Revolution: Planetary Astronomy in the Development of Western Thought* (Cambridge, MA: Harvard University Press, 1957).

Kuhn, Thomas S., "Postscript – 1969," in Thomas S. Kuhn, *The Structure of Scientific Revolutions*, 2nd ed. (Chicago: The University of Chicago Press, 1970), pp. 174-209.

Kuhn, Thomas S., "Second Thoughts on Paradigms," in F. Suppe, ed., *The Structure of Scientific Theories* (Chicago: University of Illinois Press, 1974), pp. 459-482.

Lakatos, Imre and Alan Musgrave, eds., *Criticism and the Growth of Knowledge* (Cambridge: Cambridge University Press, 1970).

Lakatos, Imre, "Falsification and the Methodology of Scientific Research Programmes," in Imre Lakatos and Alan Musgrave, eds., *Criticism and the Growth of Knowledge* (Cambridge: Cambridge University Press, 1970), pp. 91 – 196.

Layne, Christopher, "Kant or Cant: The Myth of the Democratic Peace," *International Security*, Vol. 19, No. 2 (Fall 1994).

Layne, Christopher, "The Unipolar Illusion: Why New Great Powers Will Rise," *International Security*, Vol. 17, No. 4 (Spring 1993).

Liberman, Peter, "The Spoils of Conquest," *International Security*, Vol. 18, No. 2 (Fall 1993).

Lynn-Jones, Sean M., and Steven E. Miller, eds., *The Cold War and After: Prospects for Peace* (Cambridge, MA: The MIT Press, 1993).

Machiavelli, Niccolo, trans. by Luigi Ricci, *The Prince* (Chicago: The Great Books Foundation, 1955).

Mahan, Alfred Thayer, *The Influence of Sea Power Upon History, 1660-1783* (New York: Dover, 1987).

Masterman, Margaret, "The Nature of a Paradigm," in Imre Lakatos and Alan Musgrave, eds., *Criticism and the Growth of Knowledge* (Cambridge: Cambridge University Press, 1970).

Mearsheimer, John J., "Back to the Future: Instability in Europe After the Cold War," *International Security*, Vol. 15, No. 1 (Summer 1990).

Mearsheimer, John J., "The False Promise of International Institutions," *International Security*, Vol. 19, No. 3 (Winter 1994/95).

Mearsheimer, John J., "Why We Will Soon Miss the Cold War," *The Atlantic Monthly* (August 1990), pp. 35-50.

Meier, Kenneth J., *The Politics of Sin* (New York: M.E. Sharpe, 1994).

Morgenthau, Hans J., *Politics Among Nations: The Struggle for Power and Peace*, 4th ed. (New York: Alfred A. Knopf, 1967).

Morrow, James D., *Game Theory for Political Scientists* (Princeton, NJ: Princeton University Press, 1994).

Moul, William B., "The Level of Analysis Problem Revisited," *Canadian Journal of Political Science*, Vol. VI, No. 3 (September 1973), pp. 494-513.

National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue (Washington, DC: National Security Council, 7 January 2000).

National Security Presidential Directive – 1 (Washington, DC: National Security Council, 15 February 2001).

Neustadt, Richard E., and Ernest R. May, *Thinking in Time: The Uses of History for Decision Makers* (New York: Free Press, 1986).

Nunn, Sam, *Managing the Global Nuclear Materials Threat: Policy Recommendations* (Washington, DC: Center for Strategic and International Studies Press, 2000).

Oehler, Gordon C., Director, Central Intelligence Agency Nonproliferation Center, *Remarks to the US Senate's Armed Services Committee* (Washington, DC: CIA Office of Public Affairs, 27 March 1996).

Oye, Kenneth A., "Explaining Cooperation under Anarchy: Hypotheses and Strategies," in Kenneth A. Oye, ed., *Cooperation under Anarchy* (Princeton, N.J.: Princeton University Press, 1986), pp. 1-24.

Partnership for Critical Infrastructure Security Public Policy White Paper (Washington, DC: Partnership for Critical Infrastructure Security, March 2001).

Peace Operations, US Army Field Manual FM 100-23 (Washington, DC: Department of the Army, 30 December 1994).

Perrow, Charles, *Normal Accidents: Living with High-Risk Technologies* (New York: Basic Books, 1984).

Plato, *The Republic*, trans. G.M.A. Grube (Indianapolis: Hackett, 1974).

Presidential Decision Directive 39: US Policy on Counterterrorism, unclassified, redacted Freedom of Information Act Release (Washington, DC: Executive Office of the President, 21 June 1995).

Presidential Decision Directive 62: Combating Terrorism, unclassified press release (Washington, DC: Office of the Press Secretary, 22 May 1998).

Presidential Decision Directive 63: The Clinton Administration's Policy on Critical Infrastructure Protection (Washington, DC: Executive Office of the President, 22 May 1998).

Public Law 104-201: National Defense Authorization Act for Fiscal Year 1997, Title XIV, The Defense Against Weapons of Mass Destruction Act of 1996 (Washington, DC: US Congress).

Rauch, Leo and David Sherman, *Hegel's Phenomenology of Self-Consciousness* (New York: SUNY Press, 1999).

Reagan, Ronald, *Remarks at the Annual Convention of the National Association of Evangelicals in Orlando, Florida*, White House Press Release (Washington, DC: Executive Office of the President, 8 March 1983).

Remarks by the President to the Troops and Personnel of US Joint Forces Command, USJFCOM press release (Norfolk, VA: US Joint Forces Command, 13 February 2001).

Road Map for National Security: Imperative for Change, Phase III Report of the United States Commission on National Security / 21st Century (Washington, DC: 31 January 2001).

Roberts, Lisa J., "Thomas Kuhn's The Structure of Scientific Revolutions," *E-Prime, ΣEOS, and the General Semantics Paradigm: Revolutions, Devolution, or Evolution?* (Concord, CA: International Society for General Semantics, 1999).

Sabatier, Paul A., ed., *Theories of the Policy Process* (Boulder, CO: Westview Press, 1999).

SAFE: A Security Blueprint for Enterprise Networks, White Paper (San Jose, CA: Cisco Systems, Inc., 2001).

Scambray, Joel, Stuart McClure, and George Kurtz, *Hacking Exposed*, 2nd ed. (Berkeley: Osborne / McGraw Hill, 2001).

Schroeder, Paul, "Historical Reality vs. Neo-realist Theory," *International Security*, Vol. 19, No. 1 (Summer 1994).

Schweller, Randall, "Bandwagoning for Profit: Bringing the Revisionist State Back In," *International Security*, Vol. 19, No. 1 (Summer 1994).

Schweller, Randall L., "New Realist Research on Alliances: Refining, Not Refuting, Waltz's Balancing Proposition," *American Political Science Review*, Vol. 91, No. 4 (December 1997), pp.

Singer, J. David, "The Level-of-Analysis Problem in International Relations," Phil Williams, Donald M. Goldstein, and Jay M. Shafritz, eds., *Classic Readings of International Relations*, 2nd Edition (New York: Harcourt Brace College Publishers, 1999), pp. 105-119.

Singer, J. David, "Threat-perception and the armament-tension dilemma," *Journal of Conflict Resolution*, Vol. II, No. I (March 1958), pp. 90-105.

Singer, J.D. and M. Small, *The Wages of War, 1816-1965: A Statistical Handbook* (New York: Wiley, 1972).

Smithson, Amy E., *Ataxia: The Chemical and Biological Terrorism Threat and the US Response* (Washington, DC: Henry L. Stimson Center, 1999).

Spykman, Nicholas John, *America's Strategy in World Politics: The United States and the Balance of Power* (New York: Harcourt Brace, 1942).

Spykman, Nicholas John, *The Geography of the Peace* (New York: Harcourt, Brace & World, 1944).

Statement by Treasury Secretary Lawrence H. Summers on Financial Services Information Sharing and Analysis Center, US Treasury Department Press Release LS-135 (Washington, DC: US Department of the Treasury Office of Public Affairs, 1 October 1999).

Stern, Jessica, *The Ultimate Terrorists* (Cambridge, MA: Harvard University Press, 1999).

Suppe, Frederick., "The Search for Philosophic Understanding of Scientific Theories," in F. Suppe, ed., *The Structure of Scientific Theories* (Urbana: University of Illinois Press, 1974).

"Tbilisi: The Tip of the Nuclear Iceberg," *Proliferation Brief*, Vol. 1, No. 1 (Carnegie Endowment for International Peace, 23 April 1998).

The National Money Laundering Strategy for 2000 (Washington, DC: US Department of Justice, March 2000).

Thomas, Bryn, et al, *India* (Hawthorn, Australia: Lonely Planet, 1997).

Thornberry Introduces Legislation to Realign Federal Government, US Congress Press Release (Washington, DC: US House of Representatives, 21 March 2001).

Thucydides, *The Peloponnesian War*, revised by T.E. Wick (New York: McGraw-Hill, 1982).

True, James L., Bryan D. Jones, and Frank R. Baumgartner, "Punctuated-Equilibrium Theory: Explaining Stability and Change in American Policymaking," in Paul A. Sabatier, *Theories of the Policy Process* (Boulder, CO: Westview Press, 1999), pp. 97-115.

Understanding SCADA System Security Vulnerabilities, Riptech, Inc. White Paper (Alexandria, VA: Riptech, January 2001).

Van Evera, Stephen, *Guide to Methods for Students of Political Science* (Ithaca: Cornell University Press, 1997).

Van Evera, Stephen, "Elements of the Realist Paradigm: What Are They?" typescript, 27 January 1992, p. 4, in Benjamin Frankel, *Realism: Restatements and Renewal* (London: Frank Cass, 1996), p. xiii.

Vasquez, John A., "The Realist Paradigm and Degenerative versus Progressive Research Programs: An Appraisal of Neotraditional Research on Waltz's Balancing Proposition," *American Political Science Review*, Vol. 91, No. 4 (December 1997), pp. 899-912.

Vertzberger, Yaacov Y.I., *The World in Their Minds: Information Processing, Cognition, and Perception in Foreign Policy Decisionmaking* (Stanford, CA: Stanford University Press, 1990).

Viotti, Paul R., and Mark V. Kauppi, *International Relations Theory*, 3rd ed. (Needham Heights, MA: Allyn & Bacon, 1999).

Vistica, Gregory, "Inside the Secret Cyberwar," *Newsweek* (21 February 2000).

Walt, Stephen M., "Alliances, Threats, and U.S. Grand Strategy: A Reply to Kaufman and Labs," *Security Studies*, Vol. 1, No. 3 (Spring 1992).

Waltz, Kenneth N., "The Emerging Structure of International Politics," *International Security*, Vol. 18, No. 2 (Fall 1993).

Waltz, Kenneth N., *Man, the State, and War: A Theoretical Analysis* (New York: Columbia University Press, 1959).

Waltz, Kenneth N., *Theory of International Politics* (Reading, MA: Addison-Wesley, 1979).

Waltz, Kenneth N., "Evaluating Theories," *American Political Science Review*, Vol. 91, No. 4 (December 1997), pp. 913-917.

Wendt, Alexander, *Social Theory of International Politics* (Cambridge, UK: Cambridge University Press, 1999).

Wendt, Alexander, "Anarchy is What States Make of It: The Social Construction of Power Politics," *International Organization*, Vol. 46, No. 2 (Spring 1992), pp. 391-425.

Wendt, Alexander, "The Agent-Structure Problem in International Relations Theory," *International Organization*, Vol. 41, No. 3 (Summer 1987), pp. 335-370.

Wohlforth, William C., "Realism and the End of the Cold War," *International Security*, Vol. 19, No. 3 (Winter 1994/95).

Wohlstetter, Roberta, *Pearl Harbor: Warning and Decision* (Palo Alto, CA: Stanford University Press, 1962).

Zakaria, Fareed, "Realism and Domestic Politics: A Review Essay," *International Security*, Vol. 17, No. 1 (Summer 1992).