Journal of Strategic Security

Volume 8
Number 5 *Volume 8, No. 3, Fall 2015 Supplement: Eleventh Annual IAFIE Conference*

Article 11

From WMD to WME: An Ever-Expanding Threat Spectrum

Bowman H. Miller Ph.D.
National Intelligence University

pp. 110-122

Recommended Citation
Miller, Bowman H. "From WMD to WME: An Ever-Expanding Threat Spectrum." *Journal of Strategic Security* 8, no. 3 Suppl. (2015): 110-122.

From WMD to WME: An Ever-Expanding Threat Spectrum

Abstract

One of the challenges the United States and its intelligence community confronts today, if not the foremost challenge, is the girth of its national security problem set. The array of threat types, as well as the potential sources of those threats, is unprecedented and growing. The burdensome task for intelligence at all times, but especially given the present rate of change and the increasing porosity of borders, is to try to cope with an escalating mix of challenges and rising expectations of what intelligence can provide. Existing tasks persist; they are not replaced. The number and types of potentially threatening actors have exploded. Nation-states are now joined by countless ethno-religious groupings, terrorists, criminals of all stripes, drug cartels, transnational movements and issue groups, and malevolent and delinquent individuals. Threats come from all quarters and in all sizes these days, and the mission of intelligence, i.e., to track indicators to provide warning and to reduce uncertainty for decision-makers, is monumental.

Introduction

"The world is a more dangerous and unpredictable place than it has been since the end of the cold war…."[1]

One of the challenges the United States and its intelligence community confronts today, if not the foremost challenge, is the girth of its national security problem set. The array of threat types, as well as the potential sources of those threats, is unprecedented and growing. The burdensome task for intelligence at all times, but especially given the present rate of change and the increasing porosity of borders, is to try to cope with an escalating mix of challenges and rising expectations of what intelligence can provide. Existing tasks persist; they are not replaced. The number and types of potentially threatening actors have exploded. Nation-states are now joined by countless ethno-religious groupings, terrorists, criminals of all stripes, drug cartels, transnational movements and issue groups, and malevolent and delinquent individuals. Threats come from all quarters and in all sizes these days, and the mission of intelligence, i.e., to track indicators to provide warning and to reduce uncertainty for decision-makers, is monumental.

The objective of this brief discussion is to sketch some of that threat complexity across a sweeping continuum that continues to evolve, as hostile actors seek to take advantage of any U.S. vulnerability that will succumb to their objectives. And, sadly, the older, pre-existing WMD concerns are not replaced as the spectrum changes but are simply expanded upon. We also now encounter heightened concerns about insider threats. The U.S. has to contend with a revolutionary dispersal of power: nation-states have seen both non-state actors and individuals equipped with the ability to wreak havoc undeterred by the threat of criminal justice or retaliation, or even of discovery. In the words of the most recent iteration of the United States' National Security Strategy, published by the White House in February 2015,

> "[the increasing interdependence of the global economy and the rapid pace of technological change] create shared vulnerabilities, as interconnected systems and sectors are susceptible to the threats of climate change, **malicious cyber activity**, pandemic diseases, and **transnational terrorism and crime**."[2] (*Emphases added*.)

After the denouement of the Cold War, Western intelligence focused heavily on regional and intra-state conflict issues and the consequences of the Soviet Union's demise. A metaphor for the post-Cold War transformation employed by two former CIA directors (and others) has it that, in the case of the Soviet Union, the West faced one huge dragon, an enemy that was easy to identify but impossible to eliminate. Now, however, we confront hordes of venomous snakes, ones relatively easy to kill but nearly impossible to

[1] Philip Stephens, "Cameron takes a Holiday from the World," *Financial Times*, March 20, 2015, 11.
[2] The White House, *National Security Strategy of the United States of America 2015* (Washington, D.C.: The White House, February 2015).

find.[3] With the dissolution of the USSR twenty-five years ago, China seemed to be the next big issue for intelligence in the United States – until 9/11 when al Qaeda suddenly assumed prominence for Americans and devoured huge security resources. While the U.S. was preoccupied with transnational terrorism, letting some earlier priorities slip, the vast and vexing cyber phenomenon then sprouted up to challenge terrorism (or too often is combined with it) for pride of place in U.S. intelligence and national security concerns.

In the last two decades or so, the U.S. intelligence community has also seen its list of tasks expanded to include climate change questions, pandemics, a host of non-state actors, self-radicalized extremists, and more. And, since the 9/11 attacks fourteen years ago, U.S. intelligence has been in what it deems a full-court press against terrorism worldwide, with a special focus on the threat of possible weapons of mass destruction (WMD) employment – or the threat of it – by terrorists, be they Islamists or others. Thus, in today's world, resort by extremists to carrying out various types of terrorism (or threatening its use) is taken by U.S. intelligence agencies to be a given. What is not static, however, is the spectrum of risk and vulnerability to threats, articulated or realized. WMD and the possible destruction of many lives and a large city or part of the nation's infrastructure is no longer our sole or, perhaps, even most pressing concern. Thus, a key challenge for intelligence in this twenty-first century will be to better anticipate, understand and respond to a much wider, more complex threat spectrum.[4] Complicating that challenge is what might be called a post-9/11 letdown when it comes to U.S. intelligence manning and budgeting, both of which are threatened with large cuts, meaning fewer personnel to deal with more issues and concerns that emanate from many more potential sources.

A hearty perennial threat remains the problem set of nuclear and other weapons of mass destruction. The world has been in the throes of WMD concerns for at least a century by now, beginning with gas attacks in World War I through Enola Gay and Hiroshima/Nagasaki to the continuing nuclear stand-off involving the two nuclear superpowers and lesser nuclear weapons states and aspirants.[5] Thus, the threat of some form of WMD in warfare has long been with us, recalling the earlier nomenclature of ABC weapons – atomic, biological and chemical. After the sarin poison gas attacks in the Tokyo subway system by the messianic terrorist group Aum Shinriyko in 1995, the fear was realized that a non-state actor (undeterred by traditional state to state counter-force capacity) might resort to WMD as a terrorist technique. Today, however, the more likely, practicable threat may well be the disabling of a massive subway system in a metropolis, short of resort to deadly force. Regardless of intent, in all WMD cases U.S. intelligence

[3] The author has heard these attributed both to R. James Woolsey and USAF General Michael Hayden.
[4] For a much deeper treatment of key aspects of this issue, see Joseph S. Nye, Jr. *The Future of Power*, and his Viewpoint re "Power Shifts," *Time*, May 9, 2011. Nye characterizes those shifts as power transition and power diffusion, with the latter "more difficult to manage…" He adds that "…for all the fashionable predictions that China, India or Brazil will surpass the U.S. in the next few decades, the greater threats may come from modern barbarians and nonstate actors." (*Time*, 29)
[5] German forces used chlorine gas against the French in April 1915, marking the advent of chemical weapons warfare.

has been tasked with collecting against such potentialities, analyzing their likelihood, and helping to come up with counter-measures.

Threats without Borders

WMD have long been seen as the ultimate threat to world civilization and, more recently, of mass casualty terrorism. But weapons of mass destruction are not our only, most likely, or even most persistent source of worry. The overall national security threat must now be more accurately understood as a variety of new threats stemming from what I call WME – ***weapons of mass effects***. Destruction is only one element of this broad range of potential, plausible threats to the U.S. and other societies. The challenge to both U.S. policy and intelligence in the coming years is every bit as likely to come from capabilities of adversaries to massively disable, damage, disrupt, and deceive – without resort to outright destruction. "The most significant risks to the United States in cyberspace are daily cyber attacks that undermine our national economic competitiveness."[6]

Hide and Seek – or Catch Me if You Can

When intelligence and other risk analysts examine future scenarios, they tend to assess both the probability of occurrence as well as potential impact. Some instances, including possible terrorist possession of a nuclear device, are still rated as having low probability but threatening a high impact. However, when it comes to weapons of ***mass effects***, e.g., a cyber attack to deny service or disrupt or damage a critical system, such scenarios are fast becoming threats deemed to pose both high probability and high impact. In the words of the Defense Intelligence Agency's Chief Analytic Methodologist Josh Kerbel, the earlier understanding that "there is proportionality between input and output – that a small action will lead to a small outcome or effect and that a large input will lead to a large outcome" is both misleading and encourages linear, "past is prologue" analysis.[7] The few can, in fact, inflict great harm.

Thanks largely to the rapid trajectories of globalizing, trans-border interconnectedness and the spiraling advance of information and communications technology, tomorrow's world is likely to become inordinately more complicated. In the words of *Financial Times* commentator Philip Stephens: "The end of history has made way for the era of systemic disorder….The cold war was dangerous but stable. The great unwinding has created a world that is dangerously unpredictable." [8] Moreover, it appears likely to become more dangerous due to malevolent uses of these globally-employable electronic capabilities. Intelligence has yet to come to grips with the array of threatening issues raised in the cyber realm or in effectively understanding and exploiting social media – a phenomenon that could become increasingly impenetrable depending on the outcome of

[6] *Securing Cyberspace: A New Domain for National Security*, Nicholas Burns and Jonathon Price (eds.) (Washington, D.C.: The Aspen Institute, 2012), 51.
[7] Josh Kerbel, "The U.S. Intelligence Community's Creativity Challenge," *The National Interest*, October 13, 2014, available at: *http://nationalinterest.org/feature/the-us-intelligence-communitys-creativity-challenge-11451?page=show*.
[8] Philip Stephens, "Why the Business of Risk is Booming," *Financial Times*, March 13, 2015, 11.

the worldwide debate over social media transparency versus privacy. Indeed, given the telescoping of time and distance by this globe-spanning electronic connectedness, one might suggest that Francis Fukuyama's thesis on the "end of history" might just as well have focused on the "end of geography."[9]

Seeking Needles in All the World's Hay

This discussion does not purport to focus on the intricacies and plausible further advances in technology. Instead, it seeks to raise basic questions as to how impermeable a future world may become for those tasked with making sense of it, while seeking to provide U.S. national and homeland security decision-makers with intelligence warning and estimates. Intelligence's ability to actually achieve this – given galloping international complexity, overwhelming amounts of communications, and burgeoning denial of access to the huge explosion of social media – will be daunting and most likely diminished. During the Cold War, the United States and its allies sought to obtain information and insights into "denied areas" (many of them lying behind Churchill's "iron curtain") using every means available – human and technical intelligence, diplomats and defense attaches, private citizens, defectors, underground literature, and more. But those areas where Western access was difficult, often impossible, to obtain were physically and geographically limited. They were closed societies, seeking to keep their people ignorant and bottled up, while holding outsiders – and their information and news – at bay.

In today's world, intelligence confronts "technological denied areas" in the form of social media, encrypted communications, and an explosion of different ways and venues for global exchange of useful information, along with threats, recruitment into fanaticism, Internet-conveyed radicalization and terrorist know-how, and other malevolent content. Moreover, determining the origin (and, thus, the motivation and plausibility) of various threats is inordinately complicated by anonymity and global reach via the Internet. Years ago, France declared that its defense policy needed to be postured against all potential adversaries, i.e., a defense against threats from "all directions" of the compass, although even then Paris had a limited geography and range of potential enemies in view. Today, the United States and other democracies must muster another defense in "all directions," even as they face an undefinable, variegated array of threats. The challenge is further complicated by the likely anonymity of many threats' origins, a major capacity for electronic and operational deception, and a vastly broader, layered threat spectrum.

> "Terrorist groups could also wreak havoc by attacking the information systems that control electricity for hospitals, air traffic radar, or banking transactions. Such attacks could be perpetrated with high explosives at the sites of key server computers, but they could also be carried out transnationally by computer hackers tens of thousands of miles away. Deterrence does not provide adequate

[9] This idea was voiced by Dr. Liam Fox, Member of the UK Parliament and former British Defense Secretary, in a discussion of US-UK relations at the Center for Strategic and International Studies, Washington, D.C. March 2, 2015.

> protections against terrorist threats because there is sometimes no return address against which to retaliate…."[10]

While the Internet is a boon in the majority of today's modern societies where it is available and in use, it also enables anti-social forces – from terrorist organizations to "lone wolves" to criminal syndicates – with the means to steal identities, attack and disable infrastructures, and endanger whole societies (and the instruments and institutions upon which they depend for safe food, clean water, dependable energy, financial transactions, reliable and safe transport, and more). The deaths and devastation of the 9/11 attacks remain the touchstone for American thinking about, and fears of, terrorism. However, shutting down a major power grid,[11] disrupting the nation's banking or check/credit card clearing functions, poisoning a major water source, or spreading fear of contagious diseases, either real or virtual, threaten to be significant factors and major challenges in trying to ensure future U.S. national security and the "general welfare." Recall the Ebola scare of 2014, a pandemic with no known human agency involved, aside from contagion. Then envision someone purposely weaponizing such a disease to use as a biological agent, posing a much more virulent, worrisome threat.

Social Media – The Good, Bad and Ugly for Intelligence

American society, and the intelligence community that is engaged in trying to protect it and advance its interests, are heavily focused on social media. Some users worry that they and their privacy are threatened by an overly intrusive, threat-obsessed government. On the other hand, there is the concomitant worry that social media themselves have undercut the viability of personal privacy, once one embraces their use. Social media do not spawn conflicts, but they have already demonstrated the power to ignite a conflagration based on a few sparks, with the so-called Arab Spring a case in point. The widespread, often violent, nationwide outbreaks of protests and sporadic violence over the grand jury decision in the Ferguson, Missouri police shooting of Michael Brown and others in 2015 illustrate the point.

Intelligence confronts the reality of social media from several different perspectives. To begin with, people working in the classified, sensitive U.S. intelligence enterprise are cautioned by their security watchdogs to minimize, if not avoid, exposing personal information in social media, e.g., on LinkedIn, Facebook, Instagram and the like. That is largely based on counterintelligence and personnel security concerns. However, the argument against being active in social media often is either unconvincing to users or totally wasted breath for those who have grown up in a world drenched with social media.

---

[10] Nye, Jr., Joseph S., *Understanding International Conflicts*, 6th ed. (New York: Pearson, 2007), 273.
[11] In testimony before the House Permanent Select Committee on Intelligence in November 2014, National Security Agency Director Admiral Michael Rogers was quoted as saying that "China and 'probably one of two other' countries have the capacity to shut down the nation's power grid and other critical infrastructure through a cyber attack…" Jamie Crawford, "The U.S. Government thinks China could take down the Power Grid," *CNN.com*, November 21, 2014, available at: *http://www.cnn.com/2014/11/20/politics/ns-china-power-grid/*.

Intelligence, however, also looks increasingly to social media and the global telecommunications and information technology arena as a source of information, although determining credibility and coping with its volume remain in many respects unmet, increasingly difficult, challenges. Knowing which users of social media can or intend to create mass effects on a population, be it local, national, regional, or global, is a never-ending issue for intelligence collection and analysis. An added complication is the dual-edged sword of privacy protection, since the vast majority of Internet users are without blemish, while others, few in number but powerful in aggregate, use privacy to conceal their criminality, hostile planning, and extremist recruitment. Moreover, using social media to uncover threats, to deter criminal and terrorist activity, and to track the movement and activities of "high value targets" conjures up the needle in a global haystack metaphor – one which comes nowhere near characterizing the complexity of this intelligence challenge. And, although law enforcement also tries to exploit social media to deter crimes and attacks and to identify those in the process of radicalization and recruitment, such government preventive measures remain difficult to carry out. They are properly subject to specific judicial and legal constraints, and such collection is even undermined, at times, by allegations of police entrapment or "fishing expeditions."[12]

A third aspect of information technology and social media of huge concern to intelligence and to national, homeland, and local security authorities is the ability of hidden actors to intrude into sensitive computer networks and systems upon which so much in today's society depends. This exposure runs the gamut of military systems to vital public utilities to critical infrastructure to information vaults and public, private, secret and proprietary databases. The fact that an entity or person in China, Russia, Nigeria, or even Boise, Idaho can hack surreptitiously into such systems, upon which so much depends, is the Achilles heel of the global IT world. Indeed, this vulnerability of our complex web of information technologies and computer-dependent infrastructure to hostile and hidden intervention by nations, groups, or individuals may well comprise the single point of failure in U.S. national and homeland security. Our dependence on things running on electricity or being run by computers is the epitome of modernity – and the potential scourge of highly developed societies. Trying to communicate using cell phones after a major storm has wiped out electricity illustrates the point. Now imagine electricity being lost for millions of Americans for months on end, and the shape of scenarios in the minds of those who would do us harm takes on clearer, more frightening, *Lord of the Flies* contours.

Patterns, Trends and Discontinuities

A mainstay of intelligence analysis has long been discovering and tracking patterns of behavior and trends in actions. The notion that "past is prologue" continues to typify much of what intelligence analysts do as they mine information, track groups, and

[12] For a forthright discussion of the strictures and procedures concerning U.S. technical intelligence collection and sharing, see Michael Hayden [former director of both the National Security Agency and Central Intelligence Agency], "Balancing Security and Liberty: The Challenge of Sharing Foreign Signals Intelligence," *Notre Dame Journal of Law, Ethics, and Public Policy* 247 (2005).

search for commonalities in the actions, tactics, and procedures of groups, nations, and leaders. That linear approach, however, is beset with shortcomings and ripe for failure, especially in this ever-changing, diverse threat environment. We know that a pitfall among seasoned analysts is the tendency to fall prey to fixed mindsets. Indeed, experts, real or self-acclaimed, often are among the least able to abandon their entrenched views in order to recognize change, not to mention strategic departures from earlier patterns. Indeed, the ultimate surprises and most costly aspects of intelligence uncertainty are those acts or developments that constitute a break, or discontinuity, from earlier patterns and expectations.[13]

Experience with Islamist and other terrorist groups has shown that they are innovative, adaptive, and often highly sophisticated. For every counter-measure employed against them, they seek a new mode or method of attack and of recruitment into their numbers. Recognizing government capabilities to gain human and technical intelligence against them, they eschew most hierarchy, embrace operational security, employ alternative means of communication, and plan their attacks methodically. Intelligence, thus, all too often seems to be reactive, playing catch up with ever-changing *modus operandi*, all the while hard pressed to anticipate the next target by either type or locale.

Threat Range Metamorphosis: The Spectrum is Populated with "D-words"

Until recently, those focused on known or suspected threats to U.S. national security have centered most of their attention and concerns on **destruction**, specifically on weapons of mass destruction in the hands of terrorists, tyrants, or mad men, threats that admittedly could make the attacks of 9/11 pale by comparison. Such concerns are well-placed. However, the spectrum of threats and conceivable outcomes or effects is not limited to outright death and destruction. Indeed, the modern threat spectrum is much broader. It runs along a continuum essentially as follows:

Devastate – Destroy – Damage – Disable – Deny – Deceive – Disrupt – Disturb

This litany of d-verbs shows how broad is the range of possible outcomes of threatened actions by malevolent states, groups or individuals.[14] Moreover, the one thing virtually all of them have in common is resorting to continually evolving, advanced technology, and the ability of various actors from individuals to groups to states to exploit that technology on a global basis – to attack remotely and often anonymously. Borders are a

[13] See also Bowman H. Miller, "U.S. Strategic Intelligence Forecasting and the Perils of Prediction," *International Journal of Intelligence and CounterIntelligence* 4:27 (2014): 687-701; For insights into the issue of mindsets and their impediments to "open-mindedness," see also Richards, J. Heuer, Jr., *The Psychology of Intelligence Analysis*, (Washington, D.C.: Center for the Study of Intelligence, 1999) (especially re cognitive biases), and Fisher, Glen, *Mindsets: The Role of Culture and Perception in International Relations*, 2nd edition, (Yarmouth, Maine: Intercultural Press, 1997).

[14] In his more narrowly focused analysis "Cyber Threats to Critical National Infrastructure: An Intelligence Challenge," Martin Rudner also relies on a range of d-designators to describe the "deliberate [malevolent] actions" directed at computer systems and services, including to "disrupt, deny, deceive, degrade or destroy…." He goes on, later, to list ten known instances of cyber attacks on critical infrastructure, as of 2013. *International Journal of Intelligence and CounterIntelligence 3:26 (2013),* 454, 465-66.

thing of the past in this context, both in state-to-state and domestic versus foreign issues. While we remain preoccupied with a potential chemical or radioactive assault, others are capable of shutting down our access to electricity, pure water, reliable transportation, a sound financial and banking system, and much more.

Besides denying one or more societies the fundamental needs and expectations of modern life and actual survival, the threat of such actions can and may induce new levels of fear and loathing among potential target populations. Trust in government, in intelligence, armed defense, law enforcement, and wise policy will be imperiled, beyond the mounting doubts and paranoia that already typify significant segments of American society. Moreover, much of the target set, i.e., critical infrastructure, is in private ownership and management in the United States. This immensely complicates the issue of intelligence collection, analysis, and target protection, a complex of issues that the Department of Homeland Security remains seized with and agonizing over. How to energize the private sector to take on costly preventive measures while building relationships of trust and conduits for intelligence provision is an unmet objective.

Devastate. Barring unforeseeable change in the next decade or more, the only perceived existential threat to the United States, its security and its population, that is manmade remains the Russian nuclear arsenal and perhaps those of China and North Korea, although the latter one would fall more accurately under the heading "destruction" in this threat spectrum taxonomy. For its part, the U.S. WMD Commission concluded in 2005 that today "there are dozens of entities that could strike a devastating blow against the United States."[15] While the Commission's wording uses "devastating," the number of those with existential threat potential remains very small indeed. For all of their shock, horror, casualties, and continuing financial costs, the attacks of 9/11 were not existential.

Destroy. While the destruction that a WMD attack would unleash would be enormous, it is not the only thing we have to worry about when it comes to the ability to massively destroy. U.S. infrastructure, heavily dependent on computers and electricity, is susceptible to actual destruction by outside forces and even the insider threat. Unknown perpetrators could invade computer systems from afar, rendering them non-functional in severe cases. Moreover, the ability exists to infect such systems with sleeper components, which could lie dormant for months or years, only to be activated in a time of one's choosing, in a crisis or as an act of war. This ability to carry out massive destruction is not limited to traditional WMD or to high technology invasions. An orchestrated attack of arson across a drought-ridden region could cause massive destruction of forests, grasslands, and the cities and towns they surround. Such would not constitute even a low-technology attack but nonetheless would be hugely destructive.

Damage. Less abiding or catastrophic than attacks of actual destruction or devastation, those that can cause damage are very worrisome and both more likely and more frequent. One only has to consider the elements of our infrastructure that are minimally

[15] Cited in Paul Maddrell, "Failing Intelligence: U.S. Intelligence in the Age of Transnational Threats," *International Journal of Intelligence and CounterIntelligence* 2:22 (2009): 199.

secured or completely unprotected but are vital cogs in America's economy, transportation links, and utilities: major bridges, airports, rail hubs, power stations, key industries, shopping centers (which have already been deemed of terrorist targeting interest), schools and universities, government centers (e.g., the Murrah Building in Oklahoma City), sports venues, and the list goes on. While some of these have enjoyed heightened security awareness and precautions, the range of potential targets is well beyond the scope of governments and the private sector to monitor and protect. The same holds for the business of intelligence, i.e., the possible targets of those seeking to damage things in the United States or elsewhere are literally infinite. "The threat of cyber crime is pernicious…heightened by the increasing move to digitization…[and] multiple systems and processes running in parallel are under threat, which could cause 'widespread harm'."[16] The reality of this national security threat is further reinforced by President Obama's issuance in April 2015 of an executive order declaring cyber attacks a "national emergency" and outlining penalties and sanctions for identified, major violators.[17]

Moreover, while the U.S. intelligence community has been pummeled at times for its lack of imagination when it comes to future threat scenarios, decision-makers need actual information upon which to act. Imagination is the grist of novelists, screen writers, and the occasional futurist; it cannot be a mainstay of actionable intelligence.[18] "In counterterrorism extrapolation is even more suspect, since organizations are both heterogeneous and strategic: when air travel was secured after a wave of hostage taking in the 1970s, they switched to other kinds of attacks; as profiling of terrorists improves at our borders they switch to recruiting within our borders."[19] To our detriment, the offensive and selection of targets, as well as the means used in targeting, remain in the hands of our adversaries, whether they are terrorists, hackers, enemy states, socio-political extremists, criminal syndicates, disaffected insiders, lone wolf sociopaths, or others.

Damage takes on another meaning in this and other contexts as well. Once a threat is communicated, let alone acted upon, it is government that suffers damage inflicted on its ability to fulfill the mandate to "provide for the common defense and promote the general welfare." Indeed, it is government's reputation and responsibility for warning, monitoring, countering, and restoring security and service that suffers each time such an attack occurs. And with each successive case of damage, the negative appreciation of

---

[16] Emma Dunkley, "Cyber Crime Thrives on Cost-Cutting Culture," *Financial Times*, March 16, 2015, 1,3, citing Nicola Crawford of the Institute of Risk Management.
[17] Dustin Volz, "Obama Declares Cyberattacks a 'National Emergency'," *The National Journal*, April 1, 2015, available at: *http://www.nationaljournal.com/tech/obama-declares-cyber-attacks-a-national-emergency-20150401*.
[18] The latest buzzword in intelligence is *anticipatory* intelligence, but that effort has been underway with respect to terrorism concerns already for decades. See, inter alia, Charles A. Russell, Bowman H. Miller and Leon J. Banker, Jr., "Out-Inventing the Terrorist," *An Act to Combat International Terrorism: Report of the Committee on Governmental Affairs, United States Senate, to Accompany S2236, Report #95-908*, May 23, 1978, 372-430.
[19] Eli Berman, et al., "How Empirical Studies of Political Violence (Can) Help Policymakers," *Washington Post*, March 1, 2015, available at*: http://www.washingtonpost.com/blogs/monkey-cage/wp/2015/03/16/how-empirical-studies-of-political-violence-can-help-policymakers/*.

governments' abilities to identify and thwart such damaging attacks gains salience among a dubious, if not openly fearful, populace. That is the crux of the terrorism strategy – to produce or threaten violence in order to induce fear in a wider population. Terrorist psychology works if unaffected observers to an attack extrapolate that event into believing that the next time an attack takes place, it may be closer to home or even be directed at them personally. The likelihood that 9/11 could have targeted Rockport, Maine and Brainerd, Minnesota, instead of New York City and Washington, D.C., is remote, but that did not quash fears in such places that residents there could be the next victims. Terrorists want us to believe that "there but for the grace of God go I."

Deny and Disrupt. While the issue of plausible denial of responsibility for an action is made more difficult to uncover in the digital age, as Estonia and Georgia have both experienced, attacks which deny service to a country's computer systems and communications networks are real and achievable. Both of those huge, distributed denial-of-service attacks are attributed to Putin's Russia given the apparent political catalysts for launching them. In those cases Russia made little effort to hide their origins, but such will not be and has not been always the case. Indeed, private groups or individuals can author such disruptions but deflect attention toward third parties as the responsible actors, conceivably prompting a misguided, misdirected response or retaliation. The U.S. military, for its part, worries that, in a future crisis, one or more enemies may well have the capacity to disrupt communications. Enemies could defeat the GPS system upon which battle planning and engagement rely. They could deny service to critical satellite links that provide intelligence, guidance for engagement and targeting of both manned and unmanned aircraft (UAVs), and they could disrupt logistics and resupply for U.S. and coalition forces. The party responsible could be one or more states, but it could also involve surrogates, non-state actors or even hacktivists, as they have come to be known.

In the massive civilian, private sector, the possibilities to disrupt vital services and utilities are immense. They are all susceptible to remote attacks to both deny access and at least temporarily disrupt delivery. The U.S. Department of Homeland Security – still in the throes of its complicated birthing as one, unified cabinet department – continues to seek ways to build networks of cooperation, information sharing, training, and warning between various levels of government and the private sector, which owns most of the significant infrastructure in the country but lacks the power and mandate to collect intelligence or enforce laws independently. Finding ways to share with the private sector more of U.S. warning intelligence and its insights into terrorist planning and plotting, without sacrificing sensitive sources and methods, remains a dilemma.

Deceive and Disturb. The ability to deceive one's adversaries has been a feature of strategy and warfare for ages, long before a Trojan horse appeared. Today that horse is a virtual one. In his day Saddam Hussein was a master at deception, so much so that he managed to befuddle UN weapons inspectors, who were intent on uncovering his presumed WMD program.[20] One could argue that his deception was so "successful" that

[20] For a rich accounting of Saddam's deception tactics, see David Kay, "Denial and Deception Practices of WMD Proliferators: Iraq and Beyond," *The Washington Quarterly* 1:18 (1995): 83-105.

it helped bring about the U.S.-led intervention in 2003 and Saddam's eventual undoing, even as he tried to convince both regional neighbors and the West that he held more destructive power than appears to have existed. For his part, Russian president Vladimir Putin insisted for over a year that his country had not invaded eastern Ukraine, but clearly his forces, masquerading as civilians, were instrumental in organizing and equipping an armed opposition there. Russian Special Forces have provided the point of the spear aimed at the Dombas region, even as Crimea was occupied by Russian units.

Deception involving cyber attacks, however, can and does also often constitute outright theft – of identities, of personal and financial information, of intellectual and proprietary property, of classified national security and defense data, and the like. Attempts to penetrate targeted systems involve all manner of deceptive methods, from spear-phishing and password elicitation via fraudulent emails to intrusive malware and external hijacking of control over entire computer systems. "The indispensable role that cyber has come to play in virtually all areas of life renders us all the more vulnerable to the consequences of an insecure cyber environment."[21] Thus, the U.S. has enlisted another means to combat its misuse with the Executive Order previously cited. Those vulnerabilities include theft but also intimidation and extortion, depending on the motive of the attacker(s).

U.S. intelligence has gone to great lengths and expense in efforts to cut through deception using the full range of sources and technologies, but the challenge remains and is growing. States engage surrogates to carry out attacks, to hack into foreign computers and social media, and to implant malware in targeted systems. While firewalls and security software seek to ward off such onslaughts, those responsible for defending against assaults find it enormously difficult, and often impossible, to identify the origin or responsible party behind such incessant, covert, off-shore targeting. Moreover, thanks to the ubiquity of the Internet, websites and social media, hostile groups can now readily avail themselves of worldwide channels to propagandize, recruit, inspire, and train operatives they will never meet and do not know exist. Convincing teenagers abroad to take up the ISIS call to action in the name of Islam is part and parcel of the deceptive tactics that now flood the Internet. In it privacy tends to enjoy protection regardless of the nature and motivations of Internet users – another bane of intelligence in service to national security. The notion of cyber warfare, thus, recalls the metaphor noted earlier, i.e., hordes of venomous vipers are the challenge for U.S. intelligence now and into the future.

Partial Remedies?

Faced with such daunting challenges, what can the U.S. intelligence enterprise undertake to ease its task and increase the likelihood of useful penetration of hostile actors and cogent warning of any of these levels of attack? The arsenal of aids is limited and not all that promising. But there are some things that would or could help. One is to partner more widely and effectively with foreign intelligence, security, and law enforcement agencies on issues of shared anti-threat collection and warning. Much of

[21] *Securing Cyberspace*, 11.

that is underway, but the U.S. intelligence culture remains captive to bureaucratic-cultural reluctance to share and residual doubts as to other countries' intelligence services' trustworthiness. Risk avoidance must continue to be mediated into risk management. The cliché that it "takes a network to defeat a network" could not be truer than in this connection.

Secondly, since there is no way to trace all potential threatening entities and their intentions or capabilities, a working consensus – arrived at in consultations between intelligence leaders and political-military-homeland decision-makers – must continually set and revise priorities for security protection and intelligence targeting. If every potential target and every non-state actor with known hostile intentions is considered a priority, there will be no priority on anything at all. How those priorities are struck remains an issue. "The tools for cyber attacks and biological warfare are growing ever smaller and ever more accessible…it is not unfeasible that each individual could have access to their 'own personal weapons of mass destruction programme' [sic]…[and] technology means it now only takes one outlier to cause 'infinitely greater damage than ever before'."[22] The protection of human life sits astride the top tier of all concerns, but the threat spectrum contains a widening variety of threats to human life, from death and destruction to lost access to critical, in many cases, life-sustaining services. Loss of electricity may pose an inconvenience for thousands who lose it after a major storm, but that same loss for months on end could well bring loss of life, huge economic costs, and lost confidence in officialdom.

Thirdly, intelligence has never been a panacea. Informed, vigilant citizens remain a vital cog in the business of warning of and warding off threats in democratic, rule of law societies. There is much more that can and should be done to strengthen and mobilize the private sector-government nexus in everything from sharing intelligence and warning to buttressing security, both virtual and physical. Moreover, the U.S. populace and its political leaders, and others among like-minded allies and partners, need to embrace realistic expectations of what intelligence can and cannot accomplish.[23] Most intelligence analysts, and especially those grappling with terrorism, expect other destructive attacks as a matter of course since universal coverage, both in gathering information and protecting conceivable targets, is impossible.

We have to prepare ourselves for dealing adroitly with the aftermath of attacks and recovery from them, even as we work assiduously to prevent them. Erecting monuments and memorials for each of them is hardly the answer. In Israel, where such attacks are now almost the norm, the standard response is to quickly clean up the affected area after rescuing and evacuating victims, seeking to leave no trace of the incident and quickly to return to "normal day-to-day life." The argument is that any commemorations, e.g., heaps of bouquets and teddy bears, abet the terrorists' efforts by repeatedly calling attention to their evils and thus keeping public fears kindled.

---

[22] Hannah Kuchler, "Spider Drones in the Shower and other Cyber Nightmares," *Financial Times*, April 6, 2015: 4.

[23] For an astute overview of this challenge, see Mark Lowenthal, "Towards a Reasonable Standard for Analysis: How Right, How Often on Which Issues?," *Intelligence and National Security* 3:23 (June, 2008): 303-315.

In the final analysis, U.S. intelligence needs the sharpest minds and skills available to meet these burgeoning 21st century challenges. Intelligence in service to national security is a noble calling, and the United States needs the country's best talent engaged in it. Intelligence needs to exploit partnering, with other American and foreign counterpart agencies and services, with the private sector, with the media, and with an informed, more vigilant public to the maximum extent feasible – while protecting its sensitive sources and methods. And it needs, in the context of the foregoing discussion, to widen the aperture of its threat assessment lens to better address and cope with manifold, expanding threats posed by "weapons of mass effects."