The Surveillance of Individuals in International Politics

DISSERTATION

Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy in the Graduate School of The Ohio State University

By

Jason Alan Keiber

Graduate Program in Political Science

The Ohio State University

2014

Dissertation Committee:

Alexander Wendt, Adviser

Randall Schweller

Jennifer Mitzen

Abstract

In an increasingly interconnected world in which individuals are more empowered than ever to harm state interests, states seek to protect their interests from individuals with nefarious intentions. In order for states to neutralize such threats, they must first know about them. Surveillance, therefore, is important. But while states enjoy something of a monopoly on legitimate surveillance domestically, states cannot effectively conduct surveillance on the citizens of other states with abandon. As recent NSA spying revelations demonstrate, such surveillance abroad is controversial.

While the field of International Relations has much to say about how states spy on other states, it has little to say about how states spy on the citizens of other states. This dissertation argues that the surveillance of individuals outside of domestic contexts is a significant international political practice which helps structure international security in the 21st century. To make this case I begin with a conceptualization of the surveillance of individuals abroad—what I call *i-veillance*—to help structure the empirical research. I use this conceptual framework to document the institutional underpinnings of *i-veillance* and detail the practices themselves. Most of the empirics are drawn from U.S. *i-veillance* activity, much of which is done with some cooperation from other states. In addition to demonstrating the extent of *i-veillance*, the empirical work highlights the particular ways, some surprising and unanticipated, in which surveillance is conducted.

In addition to the empirical work I explore the theoretical implications of *i-veillance* today. I argue that changes in norms, interests, and identity suggest a common international purpose in fighting terrorism—a task for which *i-veillance* is an indispensable tool. Second, I argue that there is an incipient internationalization of the state's surveillance function, itself a critical part of what it means to be a state. Finally, I argue that these internationalizations of purpose and power suggest an internationalization of authority with respect to *i-veillance*. This is not to argue that there exists *an* international state, but it is suggestive of how states might respond to a future in which individuals are increasingly empowered by and connected through technology at a global scale.

Dedicated to the memory of my father, Kingsley H. Keiber Jr.

He was a wonderful dad who taught me the values of hard work and honesty.

Through him I know love better.

Acknowledgments

No one can cope single-handedly with writing a dissertation. Although I spent many hours toiling by myself, the journey was made possible by many colleagues, friends, and family.

I was fortunate to be part of an amazing International Relations graduate cohort (starting Fall 2006). We were an eclectic bunch with broad interests and an affinity for theory. I grew a lot with this group. In particular Caleb Gallemore, Nina Kollars, Fernando Nuñez and David Traven were a great source of unwavering enthusiasm and helped push my work in better directions. The "Wendt Dissertation Group" of Bentley Allen, Zoltán Búzás, Aldous Cheung, Tim Luecke, Fernando Nuñez**,** John Oats, and David Traven was another helpful space to develop ideas. Two other of my classmates—Austin Carson and Bentley Allan—deserve special mention. They both have an infectious enthusiasm for big ideas and clever arguments. Our many discussions gave me grist for the intellectual mill and confidence when I needed it most.

The faculty at OSU has also been a tremendous help and inspiration. Alex Thompson and Bear Braumoeller in particular helped me in many small ways throughout the dissertation process. I also owe the Mershon Center for International Security Studies a special thanks for grant money that sent me to Washington D.C. to do interviews.

I owe a substantial debt to my friends and family who saw me along the way. My dear friend Nick Garcia (who is pursuing his PhD in Rural Sociology at OSU) has been sharing ideas with me since our days as undergraduates, and his impact is present in the

pages that follow. My brother King, his wife Ingrid, and their wonderful children—Reece, Egan, and Declan—provided me with emotional refuge during the past few years. I could escape to their home and be happy. My uncle Eric Keiber has been a great supporter of mine throughout my graduate career, and he provided helpful copy edits for the dissertation.

To my parents, Linda and King, I owe everything. They made me a believer in education from an early age. Throughout graduate school they provided all the support, guidance, and patience I needed. My father passed away in January 2012. My work could have easily derailed around this harrowing time had it not been for my mother. She provided such strength and stability for me and the family.

In 2010 I met Amanda, my girl. She has brought a lot of joy to my life and showed me how to focus on things outside of academia. In addition to encouraging me over the past few years, Amanda (herself a writer) helped me craft language in key passages of the dissertation. We'll be getting married on June 28, 2014. It is going to be awesome.

Finally I would like to acknowledge my committee. I was fortunate to work with such eminent and creative thinkers that push IR in new directions. Jennifer Mitzen has a twin vision that kept me focused on the interesting big picture ideas and the small grained details required to support them. Randy Schweller helped me keep the arguments direct and the theory straightforward (I'll never forget him imploring "too much exposed plumbing!"). He also motivated me to take my writing more seriously. Alex Wendt, my advisor, inspired me throughout my time at OSU. I benefitted from his uncanny ability to work with graduate students to explore and magnify their ideas. He helped me develop, focus, and take chances. All the while he was incredibly patient and generous with his time. I was fortunate to have him as my advisor, and cannot imagine working under anyone else.

Vita

2003 ..... B.A. The Ohio State University

2003-2006 ..... Research Assistant
The Center for Strategic and International Studies

2007-2014 ..... Graduate Student Associate
The Ohio State University

Fields of Study

Major Field: Political Science

Contents

List of Tables

List of Figures

Chapter 1: International Surveillance of Individuals

"We Track 'Em, You Whack 'Em"
-Motto at the NSA's Geolocation Cell[1]

States are information consumers. Historically, the state's appetite has been split. Within its borders the state feasts on information about its subjects, whereas outside its borders the state forages for details on the intentions and capabilities of other states. But increasingly some states are focusing their attention on learning about *individuals* who live *outside* their borders. How do states pursue the surveillance of individuals in international politics? The field of International Relations does not have much to say on the matter. But the phenomenon is growing. Information and communications technology has permeated the globe and saturated it with information about individuals. States concerned about international terrorism and transnational crime have increased their surveillance capabilities to take advantage of this.

In the summer of 2013 such surveillance ambitions came to light. A U.S. National Security Agency (NSA) contractor revealed, among other things, that the NSA collects and keeps metadata on all calls made in the U.S. and has direct access to servers of the largest online social media sites enabling, for example, NSA access to the content of Facebook messages between two people living overseas. We also learned that across the Atlantic Britain's Government Communications Headquarters (GCHQ) maintains wiretaps on major fiber optic cables that run in and out of the UK. It can store the

[1] Priest 2013.

content of communications for three days and the metadata for 30. What is more, the GCHQ and NSA cooperate on this program.

The world is awash in the personal details of individuals, and the NSA and GCHQ programs are examples of state surveillance practices which have gone global to gobble up these details. Since 9/11, the NSA's "workforce has grown by one-third, to about 33,000 [...] [its] budget has roughly doubled, and the number of private companies it depends on has more than tripled, from 150 to close to 500."[2] One NSA program, named "Boundless Informant," tracks the information intake of the agency, and one disclosure suggests that the NSA accumulated 97 billion pieces of metadata in *one month* in 2013.[3] According to Congressional testimony, the Director of the NSA claimed that the revealed programs have been instrumental in thwarting at least 50 terrorist plots around the world. This suggests that surveillance has become a mainstay of security policy for states trying to crack down on terrorism and transnational organized crime.

Surveillance is important to study because, if for no other reason, it is the basis upon which states administer, arrest and kill individuals. Consider that from 2002 to early 2013 an estimated 425 attacks by United States' Unmanned Aerial Vehicles (UAVs) or "drones" in Pakistan and Yemen killed upwards of 4000 people.[4] Each drone attack was based on extensive surveillance from all types of sources, including drones themselves. The intent is to identify the correct target and establish the most opportune time to strike so as to minimize the death of innocents. Or consider arrests made through international law enforcement cooperation as exemplified by the aftermath of the failed 2010 car bombing in Times Square. Three days after the incident, Pakistan made arrests

---

[2] Ibid.

[3] Greenwald and MacAskill 2013a This is one of the programs disclosed by former NSA employee Edward Snowden.

[4] For numbers on drone strikes see Bureau of Investigative Journalism 2013; For the fatalities see New America Foundation 2013. This does not include deaths in Somalia or inside the war zones of Iraq, Afghanistan, or Libya.

in Pakistan on behalf of the U.S. The speed of this arrest is comparable to that of a purely domestic case, yet it transpired between jurisdictions separated by roughly 7000 miles. The arrest was made possible by information sharing within a previously established law enforcement liaison with the U.S. FBI stationed in Pakistan and the Pakistani authorities.[5]

Drone attacks and arrests made in foreign jurisdictions represent the tip of the spear in efforts to fight terrorism, but what makes them possible—the spear's shaft, as it were—is a large surveillance apparatus that collects and analyses information on individuals globally. A standing capability to identify who is doing what, when, and where is a boon for any state that wishes to develop a reliable capability to make interventions against individuals abroad.

These surveillance practices are "idiocentric."[6] The Greek prefix *idio* means "distinct" or "personal." The neologism captures the fact that some state-led surveillance targets citizens of other states. Idiocentric surveillance tries to individuate this-person from that-person, but also to individual*ize* people so as to know details about an individual prior to making an intervention against that person. Whereas some foreign surveillance focuses on other states and their agents, we need a term to capture surveillance activity that focuses on denizens of other countries who are not spied on because of their affiliation with another state. Idiocentric surveillance targets criminals and terrorists, and is therefore different than Cold War era spying in which the U.S. spied on Soviet assets and functionaries and vice versa. Idiocentric surveillance is the

[5] According to U.S. Representative Jane Harman on this matter, 'Our liaison relationship with Pakistan intelligence is yielding impressive results.' Susman and Serrano 2010.

[6] An alternative label is "anthropocentric", but that suggests a focus on people or humans generally. Idiocentric captures how states want to be able to individuate threats, to burrow down to the details.

subject matter of the dissertation. In the spirit of the times I will henceforth refer to as *i-veillance*.

My basic thesis is that *i-veillance* is a significant international political practice which helps structure international security in the 21st century. "[P]ractices are socially meaningful patterns of action, which [can be] performed more or less competently."[7] They are "materially mediated" activity (or "doings") reliant on shared stocks of knowledge (which practices also serve to reproduce).[8] Diplomacy is an example of an important international practice.

I-veillance is a practice in this respect. States perform *i-veillance* with a shared understanding that terrorism is a global problem which can be mitigated by international cooperation and information sharing in particular. States conduct surveillance through technologies that collect, transmit, and store data. The 'competence' of *i-veillance* can be assessed according to technical standards (how good is a state's surveillance capability), cooperative standards (how much does a state cooperate with other states), and through results (how successful is the surveillance activity).

An explicit focus on "practices" is currently in vogue. Such work comes in many flavors[9] and is not without detractors.[10] I do not use a particular theory of practice,[11] nor do I theorize about practices (e.g. regarding their ontological status). I simply take for granted that thinking through practices is very useful for understanding world politics. And because *i-veillance* is both under-theorized and under-empiricized, a first step in an analysis of *i-veillance* is making the descriptive inference that it is an important and meaningful practice.

---

[7] Adler and Pouliot 2011a, 4.
[8] Schatzki 2001, 11.
[9] See some of the work in Adler and Pouliot 2011b.
[10] Ringmar 2014; Duvall and Chowdhury 2011.
[11] As does Pouliot 2010.

A study of the practice of *i-veillance* takes me "down to the ground," and in the empirical chapters I detail institutions, technologies and processes of surveillance. I find diverse forms of international partnerships that constitute an interconnected infrastructure of technology and institutions that conduct *i-veillance*. I show that states work around anarchy and sovereignty in clever ways. And because surveillance is a form of state power, one with an intimate relationship between the state and those over whom the state exercises that power, the extent of *i-veillance* suggests incipient internationalization of state power. This, in turn, has implications for the people over whom such power is wielded.

A comprehensive study on this type of surveillance is timely and important for both the practice of international security and the discipline of International Relations.[12] Since 9/11 the U.S. has made fighting terrorism a priority. Running behind the more flashy coercive acts of counterterrorism is an infrastructure that spans the globe to conduct surveillance on individuals. The conduct of domestic surveillance is not new, and neither is state-to-state surveillance. But the substantial and sustained effort by the U.S. to surveil individuals abroad is new. If recent revelations regarding the NSA have made anything clear, it is that *i-veillance* continues to grow and is very controversial. We need to better understand the practice.

There is also a lot to learn about the international politics of *i-veillance*. The U.S. is not sole actor here. It has, indeed often requires, partners. As the saying goes, a global problem—nefarious individuals who can travel extensively and communicate instantaneously—often calls for a global response. Whether it is information exchange, law enforcement liaison, or permission to conduct surveillance abroad, the U.S. leans

[12] A 'research project should pose a question that is "important" in the real world' and it 'should make a specific contribution to an identifiable scholarly literature by increasing our collective ability to construct verified scientific explanations of some aspect of the world.' King, Keohane, and Verba 1994, 15.

heavily on other countries to either avail itself of their information or to collect information in their territory. This is, in part, what makes studying *i-veillance* so interesting. The U.S. has also been at the forefront of institutional efforts—through the UN for instance—to facilitate surveillance. And countries other than the U.S. are engaging in similar practices.

The dissertation details *i-veillance,* but is not seeking to answer the question "why is *i-veillance* happening?" Before asking causal questions about *i-veillance*, IR first needs to know about the practice itself and to what extent and how it is unfolding internationally. As a result, as I explain more below, I am engaged in descriptive inference. To assist me I develop a conceptual framework for *i-veillance* to use in mapping the terrain of these practices. Once we know what to look for it becomes clear how much activity is going on. The range of surveillance practices include the exchange of airline passenger information, personal details collected at ports of entry, criminal profiles shared between law enforcement agencies, terrorism data entered into a shared database, drones conducting reconnaissance in foreign countries, and much more. The technologies and institutions involved have, and continue to, propagate internationally. For instance the U.S. transmits technology and knowledge to many countries to help them track potential terrorists. There is no review of these phenomena in IR.

But the argument I will be making is not just that there is a lot of surveillance going on. The surveillance of individuals in other countries is fundamentally an international political practice under conditions of anarchy and in the face of sovereignty norms typically unfavorable to foreign state intervention in another state's domestic affairs. I not only conceptualize *i-veillance,* but I look at the specific modalities of surveillance and the international politics at play. As a state's appetite for information on individuals grows so too does the chance of roping other states into that effort. Today's

demand, driven as it is by the U.S. in particular, is enormous. IR needs to study the diverse international partnerships that constitute *i-veillance*, and to chart how different states' surveillance infrastructures interact.

A comprehensive study of *i-veillance* is important for International Relations theory as well. How does a state surveil citizens of another state under such conditions of anarchy and in the face of sovereignty? Pursuing a strategy of unilateral brute force surveillance would be extraordinarily difficult and ineffective. There are incentives for states to cooperate on transnational issues such as terrorism and crime.[13] However, there are also disincentives, particularly in regard to surveillance. Because of a state's domestic sovereign prerogatives, we shouldn't expect it to wantonly share information about its citizens with other states. There is no extant theory to deduce observable implications about how states should act in these matters. The dissertation, therefore, pays attention to the strategies and politics of *i-veillance* to inductively establish prevailing patterns.

The dissertation treats state surveillance as a form of power. On the one hand, *i-veillance* is conducted with varying degrees of consent and coercion with other states. On the other hand, *i-veillance* is an administrative act of power over another state's citizens. The deeper and broader the surveillance the more the subjects of that surveillance get caught up with a foreign state's administrative apparatus. The final two chapters of the dissertation takes up these issues.

There is one final reason why a study of *i-veillance* is important: it is a political practice that is here to stay. Individuals will always be spied upon so that states, when necessary, may kill and arrest them with greater ease and sophistication. The NSA revelations of 2013 show that the U.S. was seeking to *increase* its access to private

[13] For instance, international regimes dealing with terrorism can be understood, in part at least, by the traditional institutionalist insights regarding reduced transaction costs and information provision. Keohane 2005, 51–2; For a detailed exploration of these issues with respect to policing see Andreas and Nadelmann 2006.

companies' data stores as recently as 2012. President Obama did not blink when confronted with whatever outrage the revelations have stirred. Defending the programs he said flatly they "have been repeatedly authorized by Congress. Bipartisan majorities have approved them. Congress is continually briefed on how these are conducted. There are a whole range of safeguards involved. And federal judges are overseeing the entire program throughout." In July Congress was given an opportunity to dial down some of the NSA's surveillance. It said "no."

In addition, states continue to address terrorism—which is the primary driver of *i-veillance*—as a top-tier threat. In 2013 UK Prime Minister David Cameron referred to al Qaeda as a global, existential threat.[14] In the same year the French military were chasing al Qaeda affiliates through the African Sahel. In a further display of resolve the French Interior Minister recently said "I don't know if it's global, regional or local, but the war against terrorism is far from being over."

Sketching the Argument

To begin thinking through *i-veillance*, start with a domestic analogy. Modern states tend to be good at controlling individuals *within* their borders. There are two necessary components for states to effectively control individuals. The first is the familiar monopoly on the legitimate use of force. Second, if the state wishes to coerce (i.e. arrest or kill) an individual, the state needs a surveillance capacity in addition to its coercive capacity. It must know *who* is doing *what*, *when* and *where*. Then, and only then, can the state make an intervention against an individual. Domestically, states keep basic information about their citizens and residents so they can perform acts of administration and intervene in the affairs of those individuals within their borders, for example in

[14] Wintour 2013.

order to levy taxes. In the words of James C. Scott, the modern state makes its subjects "legible" so that it can manipulate them when needed.[15]

Today international security practices pay close attention to individual actors. States are trying more and more to manipulate and intervene in the affairs of those individuals *outside* their borders. How do states make *those* individuals legible? The answer is surveillance. If legibility is the end goal, surveillance is the means.

Surveillance is more than eavesdropping. It includes all practices that collect, retain, and analyze information on individuals and the environments (e.g. territory) in which they move and transact. The value of surveillance for the state is that it can bring information about individuals—their behavior, associations and transactions—into finer and finer degrees of resolution. This idea of "resolution" captures a specific way in which surveillance increases the legibility of people. Higher resolution information enables the state to make more precise interventions against the individual(s) in question and to take more refined precautionary measures if the state anticipates a threat.

The collection of information is achieved through "sensors." Sensors are the humans and technologies that collect information and the databases that store it. Examples include satellite surveillance, internet snooping, and law enforcement operations in foreign jurisdictions. Taken as a whole, a state's *i-veillance* sensors form an infrastructure of surveillance.

Because *i-veillance* is a security practice, states will try to cover not only unanticipated behavior from known threats but also *unknown* threats. This means that *i-veillance* infrastructure will tend toward a wider distribution and continuity in its coverage. Put differently, if the state thinks the potential threat could come from any corner of the world, the state will try to build its surveillance apparatus globally as well. I

[15] Scott 1998; Scott 1995.

don't want to overstate things too much. In reality interested states are likely to focus more on some regions and less on others. But the general point is important.

Unlike domestic surveillance, any state conducting surveillance outside its borders necessarily implicates other states. After all, it is the citizens of another state that are being spied upon or monitored. This is where surveillance practices get thorny and interesting for International Relations. Specific requests for information or access to specific individuals who live abroad are not rare, and they are often granted. But routine *i-veillance* (often with cooperation) is different. But as I aim to show, such cooperation is becoming *de rigueur* in international security.

If a state wants information about an individual in another country, the former state has to deal with the realities of sovereignty and international law (to say nothing of technological and resource constraints). This imposes constraints and presents challenges. A state cannot unproblematically conduct intelligence in another state's territory. Some level of cooperation or consent is to be requested, but as mentioned above, we shouldn't expect states to welcome surveillance in their own territories with open arms. We might expect various international agreements and institutions to exist that facilitate *i-veillance*. I review some of these in chapter three.

To understand *i-veillance* is to catalog states' infrastructure of sensors and how these various infrastructures work with one another. This view looks beyond traditional intelligence practices such as wiretapping. For instance, law enforcement liaison relationships make for a network of sensors that scoop up information that would not be accessible if not for the liaison. The scanning of passports and visas at international borders are not simply practices to keep unwanted individuals at bay, but are also practices that feed databases with data on the identity and movement of individuals.

Analysis of financial transactions reveals information that then gets cross checked against other data. Mapping this type of activity is the task that lies ahead.

Findings

The dissertation makes five principal findings. I address them in ascending order of abstractness.

First, the U.S. may be adopting (knowingly or not) the role of a global intelligence provider. (Similarly the EU is becoming a regional intelligence provider.) An analogy will help make this point. The U.S. National Counterterrorism Center (NCTC) is the "primary organization in the [U.S.] for integrating and analyzing all intelligence pertaining to counterterrorism."[16] A bunch of intelligence and analytical products go into the NCTC and out comes intelligence assessments that then go to various "customers" in the government. Between its global law enforcement and customs partnerships, information sharing agreements, and cooperative intelligence arrangements, the U.S. is effectively becoming a global clearinghouse for terrorism related details. Information as a result of bi-and multi-lateral arrangements (in addition to U.S. intelligence operations) flow into the U.S., and the U.S. can then push out threat warnings, intelligence and analysis (essentially providing a reciprocal *i-veillance* function) to other states in order to stop international terrorism.

The second finding gives a preliminary answer to the question suggested above: how do states conduct *i-veillance* under anarchy and in the face of sovereignty. The empirical chapters show how the U.S. creates an infrastructure of surveillance with surprising little resistance. Much of the more visible (i.e. non-secret) acts of *i-veillance* are being done through previously existing practices and institutions which grease the wheels of expanding *i-veillance*. And when less visible *i-veillance* defeats the friction of

[16] NCTC 2013.

anarchy and sovereignty, it does so by virtue of being secret or otherwise kept off the books (often in the form of bi-lateral agreements). Moreover, surveillance infrastructures are created piecemeal and through networks of state officials.[17] Surveillance capacity is thereby built more discreetly and without obvious central coordination.

Related to this is the third finding: there is emerging global governance regarding the surveillance of individuals. The concept of "global governance" is contested but generally refers to the ways in which international and transnational actors establish systems of rule to "steer" global affairs. Some scholars like Thomas Risse focus on non-state actors and non-hierarchical modes of steering.[18] Others focus on state roles in global governance. Jennifer Mitzen, for instance, shows how states can collectively intend (that is, "concert" their power) to order international affairs.[19] The empirical work that follows, especially Chapter 3, highlights multiple international organizations and bi-lateral arrangements that govern the flow of information on individuals engaged in illicit activity. These governance structures are steered by Western states and the U.S. in particular. This provides further reasons to push back against the neoliberal bias in global governance studies in which state-guided activity is neglected in favor unguided economic processes.[20]

The fourth finding is primarily of theoretical interest. In Chapter 7 I argue that an important security prerogative of the state is being internationalized. I argue that—because it is so essential to the exercise of force and administration—surveillance is a constitutive part of what it means to be a state. I then show how both *infrastructures*

---

[17] Slaughter 2009.
[18] Risse 2004.
[19] Mitzen 2013 see pp 12- 18 in particular for a helpful typology of intentionality in global governance.
[20] Ibid. Mitzen also notes that 'the wariness of public power that characterizes neoliberalism carries over [to global governance studies], and it is difficult to advance a positive role for the state and state-like power.' (p 3) Whether or not i-veillance is a positive practice remains to be seen.

and *processes*[21] (i.e. practices) that underpin state surveillance *links up with* those of other states in order to perform surveillance. This represents an internationalization of the state's surveillance functions.[22] If the majority of the evidence suggested unilateral surveillance of people abroad, then that would not be a real internationalization (rather, it would be a practice that happens to be international). The following chapters, however, provide what I believe to be ample evidence of cooperation. This is more than a form of neo-medievalism,[23] and it is not reducible to the interactions between disaggregated elements of the state officials involved.[24] A particular set of state security functions are being internationalized. Surveillance is key to the state and it is being internationalized. As James C. Scott writes, "To follow the process of state-making, then, is to follow the conquest of illegibility."[25]

The last finding is a bit more speculative and is found in the concluding chapter. I argue that there will be continued growth of *i-veillance* which will foster the growth of a global citizenship. While some actors promulgate the norm that states and the international community have a "Responsibility to Protect"[26] (R2P) citizens, there is a flip side to this which my dissertation illuminates. Individuals are also increasingly viewed as international subjects *from whom* the *state* must be protected. As individuals become increasingly empowered by technology and easier access to information and communications, states will feel more threatened. The result will be increases in *i-veillance*.

---

[21] I focus on three processes that are bound up with the state's coercive power—processes of coercion, processes of territorialization, and processes that bind state-society together.
[22] I stress 'an internationalization.' I am not arguing that security has been completely internationalized. And I am not arguing that a world state exists.
[23] Ruggie 1993; Friedrichs 2001.
[24] Slaughter 2009.
[25] Scott 2010.
[26] International Commission on Intervention and State Sovereignty and International Development Research Centre (Canada) 2001.

As states increase *i-veillance*, citizens of distinct states will increasingly see themselves as commonly affected and suffering from a democratic deficit.[27] Eventually they will mobilize, and some may even turn to violent forms of resistance. The eventual result, I argue, is that this common cause against international state power will contribute (along with other factors of globalization) to discourses of global citizenship.[28] Surveillance and the use of personal information by states is itself a component of state power that people will negotiate over, reflecting perhaps a new social contract in the digital age. [29] In the aftermath of the NSA disclosures there has already been a substantial international backlash from global civil society.

Where We Are, Where We've Been, and Who Else is Here

Why do states pursue i-veillance?

Although the dissertation is not about why states pursue *i-veillance*, it is worth a general discussion to help frame things. The state's focus on individuals abroad is likely overdetermined. One contributing factor must be that individuals are empowered to disrupt societies and put a dent in state interests.[30] Whether or not it is warranted,[31] the threat puts some states on edge. Given that contemporary state-based threats feel prosaic, and major power war is not probable, states may view individuals as the next-best-threat to address. There is geo-political slack[32] so to speak. And in a world in which major predators are absent, we shouldn't be surprised to see states turn their attention to pests.[33]

---

[27] Moravcsik 2004.
[28] Williams 2009.
[29] Chesterman 2011, 11–12.
[30] Homer-Dixon 2002.
[31] For forceful arguments that the threat of terrorism is inflated see work led by John Mueller. Mueller and Stewart 2012; Mueller and Stewart 2010; Mueller 2009.
[32] This language comes from discussions with Randy Schweller.
[33] The 'predator' / 'pests' language is borrowed from Frydl 2006, 18.

But beyond the "empowered individual" and the "swat the pest" theses, another enabling condition deserves special mention. Put simply, states have never been more capable of intervening in individuals' lives via the information individuals leave behind. Two trends are largely responsible for this. First, the amount of recordable information about individuals' behavior has and continues to grow. Individuals are increasingly engaging with media which leave a data trace, and there are more ways in which data can be generated (consider all the mobile apps which have only recently existed). Therefore, individuals produce more recordable data. The result is a staggering and chaotic explosion of information.[34] A recent report by an IT consultant firm suggests that the amount of data being produced is doubling every year, and in 2020 the "digital universe" will be roughly 40 trillion gigabytes.[35] Second, there is more technology which can syphon up and record data concerning individuals lives. New technology makes information more easily recorded and stored. And sure enough there is growth in data collection and aggregation by corporate actors—mainly, governments and private companies. The mere accumulating information is not new as it is inherently useful to any actor wishing to influence others. But the development of these trends are of unprecedented orders of magnitude.[36]

---

[34] See Schweller 2010 for relevant remarks on the information age (pp 151-153) and the effects of entropy for international politics.

[35] Gantz and Reinsel 2012.

[36] There is an argument that connects the security concerns of states with the volumes of information produced by individuals. Here I am inspired by Randall Schweller's (2010) work on entropy. A physical system may have a 'macro' configuration that one can observe, but it may be made up of any number of possible 'micro' conditions. Taking the roll of two dice as an example, a roll which yields a macro configuration of '12' can only be made up of one possible micro configuration of '6' on both dice. The entropy here is low. A roll that sums '7', however, can have many possible micro configurations—'1 & 6', '2&4', etc. The entropy here is higher. The entropy of a given system can be understood as the missing information one needs in order to know the underlying micro-configurations that underlie the macro-configuration. When a state confronts a known adversary (the macro-state) it still faces a lot of uncertainty as to how that threat will manifest itself (the micro-states). If the 'macro' threat is, say, the Soviet Union, the potential micro-configurations that make up that threat—different troop positions, warhead counts, military expenditures, etc—are numerous. If the 'macro' threat is al Qaeda,

From Predators to Pests[37]

Although the extent of today's surveillance is unprecedented, it is not as if states have never been interested in keeping tabs on individuals—even those who are not agents of a state—outside their borders. In the literature on modern state formation scholars note the differentiations of the state's security apparatus, a splitting of an outward facing military and inward facing police. Internal surveillance is an essential part of this. But it didn't take long for states to take an extraterritorial policing interest.

The mid-19th century saw popular upheaval, and in the late 19th century European states were rocked by assassinations by anarchists. In 1878 assassination attempts were made against the German emperor, the king of Spain and the king of Italy. Russian Tsar Alexander II was assassinated in 1881, as was the president of France in 1894, the premier of Spain in 1897, the empress of Austria in 1898 and the king of Italy in 1900.[38] The U.S. itself suffered an assassination when President McKinley was shot in 1901. Around this time the Europeans and Russians were considering an international effort to combat anarchism and pressuring the U.S. to join it.[39] The resulting 1904 St. Petersburg Protocol facilitated law enforcement cooperation and information sharing (the U.S. did not sign on to it).[40]

Another notable moment in the story of *i-veillance* would be the creation of the FBI in 1908. This was important for two reasons. First, it established a national law enforcement agency for the U.S. This allowed the U.S. to more effectively develop liaison relationships with counterpart agencies of other states. Second, the FBI was a major part

---

the potential micro-configurations are, if not more numerous, at least more difficult to know. The entropy here is higher. This motivates states fighting terrorism to ramp up surveillance to minimize entropy.

[37] Maybe we can add terrorist 'mosquitos' and criminal 'termites' to the IR menagerie of lions, lambs, jackals, and wolves. Schweller 1994.

[38] Miller 1995, 28.

[39] Jensen 2001.

[40] See Jensen 2013 for a broader treatment of this effort.

of the early U.S. efforts to conduct surveillance on individuals abroad. In the 1940s, Roosevelt carved out a special program from the FBI—the Special Intelligence Service (SIS). The SIS worked in Latin America to keep track of and stop agents and sympathizers of the Axis-powers. The SIS was disbanded shortly after the war. Later the FBI would truly cut its teeth as an international law enforcement agency—effectively conducting *i-veillance*—in the late 70s and early 80s as it worked with Italian counterparts to bring down the Mafia.

Much of today's *i-veillance* capabilities were born out developments in traditional intelligence which trained its gaze on the activities and personnel of other states. From the time states developed modern intelligence services, they have also found ways to cooperate. One cooperative arrangement deserves special attention—the UKUSA agreement to share and cooperate on signals intelligence during WWII. The arrangement continues today and in addition to the UK and U.S. it includes Canada, Australia and New Zealand. Although details of the agreement and capabilities are not well known, it is widely believed that the countries have relied on their arrangement to share information with regard to terrorism. That is, UKUSA has shifted from a traditional surveillance function (targeting states) to an *i-veillance* function.

One more trend deserves special mention—the U.S. war on drugs. The Nixon administration declared war on drugs in 1971, and subsequent presidents continued it. An important part of this "war" was the development of a global U.S. law enforcement presence. In the mid-1970s the U.S. already had roughly 1/10th of its 2141 DEA agents stationed in 43 countries.[41] By the early 90s, 300 DEA agents were present in over 70 states.[42] The physical presence of these agents served a surveillance function. Moreover,

[41] Andreas and Nadelmann 2006, 129.
[42] Andreas and Nadelmann 2006.

the U.S. trained foreign law enforcement agents and replicated its own models of drug enforcement. The result was lasting liaison relationships.

The events of 9/11 takes us up to today. For the U.S. and other states, the emphasis on individuals as a security threat has never been greater. As Andreas and Price put it, "the role of the advanced state's externally oriented coercive apparatus has been shifting in emphasis from warfighting to crimefighting functions."[43] The state has gone from focusing on other state predators to focusing on individual pests. And to swat pests, the state first has to know about them.

SCO & RATS!

Some readers might dismiss all of this as a Western thing. Although most of the empirics in the dissertation come from the West, and the U.S. in particular, other states pursue *i-veillance* as well. To make the point, I present a case with no connection to the West.

After 9/11 there was no shortage of international condemnation of terrorism. The U.S. wasted no time in reaching out to other states to make sure terrorism and counterterrorism were taken seriously. President Bush made rhetorical statements of solidarity ("History has called America and our allies to action."[44]) and more muscular statements aimed to yoke other states in line ("You're either with us or against us in the fight against terror."[45]).

The time was ripe for states to take advantage of the new fervor to fight terrorism and focus or rebrand their own domestic struggles in war-on-terror terms. The Russians had the Chechens. The Chinese had Uighurs. But common cause has only run so deep. Andrew Phillips argues that after 9/11, two different internationalisms—one liberal and

---

[43] Andreas and Price 2001, 35.
[44] See Bush 2002 State of the Union Address.
[45] See his November 6, 2001 statements with French President Jacques Chirac

one illiberal—entailed two different strategies for dealing with terrorism. The former, pursued by the U.S., focused on pushing democracy and a version of sovereignty emphasizing a responsibility to take care of one's own territory to prevent terrorism. The latter internationalism, pursued by Russia and China, focused on "privileging sovereign authority and respect for pluralism and non-intervention."[46] This illiberal form of internationalism was, in part, a reaction against the track taken by the U.S., the perceived intention of which was, "let's all be good liberals now."

Phillips overstates the U.S. push for liberal governance. The U.S. was, and in fact *is,* quite happy with some authoritarian regimes—for instance Mubarak's regime in Egypt (support was revoked once Mubarak's fate was all but sealed), Saudi Arabia, and Bahrain. But Phillips is right in that the U.S. pursued a more internationalist strategy focused on international forums and "fixing" some regimes in liberal ways. Russia and China, not desiring outside meddling in their affairs, turned to their own strategy to fight "terrorism." One of these strategies was articulated through the Shanghai Cooperation Organization.

The Shanghai Cooperation Organization (SCO) has its origins in meetings in the mid and late 90s among "the Shanghai Five"—Russia, China, Kazakhstan, Kyrgyzstan, and Tajikistan. Initially discussions concerned "military relations" and "reducing their military forces along their mutual borders," but "the scope of their discussions eventually expanding to political, security, diplomatic and economic issues."[47] Beyond its stated objectives, the SCO also serves to maintain regime stability in the face of spreading democratic norms—that is the SCO works to 'sustain authoritarianism'.[48] One way the SCO works to enhance member security is to cooperate against the "three evils" of

[46] Phillips 2013, 89.
[47] Ambrosio 2008, 1326.
[48] Ambrosio 2008.

terrorism, extremism, and separatism.[49] To achieve this the SCO set up the Regional Anti-Terrorist Structure (RATS).

The SCO RATS case is illustrative for two reasons. First it shows that the U.S. is not alone in publicly talking about terrorism as if it were a major security threat. This is no cheap talk, because, and this is the second point, the SCO member states have set up an information sharing arrangement to address their 'evils'. The SCO Secretary has stated publicly that "that terrorism, separatism and extremism still remain to be [sic] the most serious threat to peace, security, stability and development in the region."[50]

Weitz describes RATS activity more in depth:

> Since officially beginning operations in June 2004, the RATS has coordinated studies of Eurasian terrorist movements, facilitated information sharing about terrorist threats, and provided advice on counterterrorism policies. It has also coordinated exercises among SCO security forces and organized efforts to disrupt terrorist financing and money laundering. [...] In June 2006, Russian Foreign Ministry spokesperson Mikhail Kamynin stated that the information exchanged through the RATS had thwarted hundreds of attempted terrorist acts.[51]

Moreover, SCO members also cooperate in fighting organized crime and has apparently fashioned itself as a mediator of sorts with non-SCO countries with respect to counterterrorism efforts. For instance at a 2006 SCO summit Afghanistan President Karzai and SCO officials created a "Contact Group", the function of which served a clear surveillance purpose—"to exchange counterterrorism information and provide Afghanistan with reconstruction assistance."[52]

---

[49] Aris 2009.
[50] Quoted in Ambrosio 2008, 1332.
[51] Weitz 2007, 105.
[52] US Diplomatic Cable 2009a.

Structure of the Dissertation

My dissertation uses descriptive inference, the use of "observations from the world to learn about other unobserved facts."[53] There is not much empirical work on what I call *i-veillance*, and it has never been conceptualized. The Surveillance Studies literature lacks an IR perspective, and to the extent that IR is interested in 'surveillance, the literature tends to focus on how intelligence communities interact. As King, Keohane and Verba write, "[s]ometimes the state of knowledge in a field is such that much fact-finding and description is needed before we can take on the challenge of explanation. Often the contribution of a single project will be descriptive inference." Good description and conceptualization is crucial to the social sciences, and at the end of the day causal arguments rely on descriptive arguments.

To structure my inferences, in the next chapter I conceptualize *i-veillance*. This helps me determine "what's in and what's out [in order to] locate the boundaries of a specific practice."[54] I begin with a conventional understanding of surveillance and build out from there. The chapter closes with an explanation of my standards of evidence and the reasoning behind my case selection. As will be explained, the main empirical chapters (4-6) will revolve around sensor types. My intention is to give a 'lay of the land'—to describe some of the capabilities involved and to chart their use. This allows me to take stock in the final chapters. But before the sensor chapters, I review in chapter 3 some of the legal and institutional arrangements that enable and facilitate *i-veillance*. Whereas chapters 4-6 focus on actual practices of surveillance, chapter 3 finds the political arrangements that undergird many *i-veillance* practices. I focus on information

---

[53] King, Keohane, and Verba 1994, 8.
[54] Karp 2013, p975. Karp identifies four methods for identifying practices. My approach represents a fifth, which might be called 'conceptual denotation'. My approach lets the concept guide determinations of 'what's in and what's out.'

sharing and capacity building arrangements led by the U.S., UN Resolutions effectively mandating surveillance, international organizations, and legal assistance treaties. The picture that emerges here is an international framework that either calls for or encourages *i-veillance*.

Chapters 4-6 look in detail at the types of sensors used, how they function as a form of *i-veillance*, and looks at cases to tell us something about the politics of and thinking behind their use. To what extent do sensors rely on the cooperation of other states? Are sensors developed and deployed *de novo* or as part of previously existing practices. How do different types of sensors contribute to the state's effort to create high resolution maps of individuals?

Chapter 4 looks at "databased" sensors. These include databases, database interfaces (such as those that scan travel documents at ports of entry), and internet snooping technologies. I examine a case where the U.S. assists Caribbean countries in setting up an information system to track foreign travelers. Chapter 5 looks at "remote" sensors—those sensors that collect information through technologies but at some distance. These include imaging platforms (satellites and drones) and signals intercept platforms as well. I go into greater detail about how the U.S. conducts aerial surveillance in Africa. Chapter 6 examines "human" sensors (a concept similar but broader than what the Intelligence Community refers to as 'HUMINT'). I look at how FBI liaison relationships abroad form an *i-veillance* infrastructure that interacts with the domestic surveillance infrastructures of partner states.

Chapter 7 examines the theoretical implications of the empirical work. The evidence I amass in the following chapters suggest that states share *i-veillance* infrastructures and work together on *i-veillance* processes. I argue that this amounts to an internationalization of surveillance understood as a constitutive feature of what it

means to be a state. I further argue that there is a related internationalization of authority. The concluding chapter explores implications for state authority over international subjects, both from the state's perspective and from the perspective of those subject to surveillance. As hinted above, I make an argument that *i-veillance* will continue to grow thereby contributing to discourses of global citizenship.

Chapter 2: i-veillance

Introduction

The premodern state was, according to James C. Scott, "partially blind."

> It knew precious little about its subjects, their wealth, their landholdings and yields, their location, their very identity. It lacked anything like a detailed 'map' of its terrain and its people. It lacked, for the most part, a measure, a metric, that would allow it to 'translate' what it knew into a common standard necessary for a synoptic view. As a result, its interventions were often crude and self-defeating.[55]

The modern state has overcome its blindness at home, however it remains blind to the details of individuals who live outside its territory. Many states are seeking to overcome this affliction so they can make more fine-tuned interventions against individuals abroad. But how?

The answer given in the introduction is that states pursue "idiocentric" surveillance practices that individuate and individualize people. I call this *i-veillance*. If a state wants to kill, capture, or otherwise disrupt an individual's life, the state must first know things about that individual. What was the infraction? Who did it? Where is he now? For any intervention against an individual there must exist state-led surveillance on that individual. In contemporary world politics there are many states that wish to conduct *i-veillance* if for no other reason than that they can be prepared if someone wishes to damage the state's interests. The more information the state has about the "bad

[55] Scott 1998, 2.

guys" that wish to do it harm, the better equipped the state is to make an intervention against them.

In this chapter I unpack what is meant by surveillance in general and *i-veillance* in particular. I close with an explanation of my research design. Overall the exposition is fairly straightforward and is "conservative" insofar as it sticks to intuitive understandings of surveillance. Once we have a working conceptual framework we will understand what empirical phenomena fit. There is no need for conceptual stretching or muddying of theoretical waters. Once we combine some basic insights of the surveillance literature and theorists such as Anthony Giddens, Michael Mann, and James C. Scott the analysis flows readily.

The conceptualization below allows me to meaningfully identify *i-veillance* practices.[56] The approach is a "synthetic" generalization meant to demonstrate "that diverse attributes of a topic revolve around a central theme which unifies the attributes, lending coherence to an otherwise disparate set of phenomena."[57] This can be contrasted with a typology where "the goal is to sort phenomena into discrete categories that are mutually exclusive and exhaustive on the basis of a uniform categorization principle or principles."[58] Because my dissertation is interested in explaining what these surveillance practices are, not *why* they are, it is descriptive.[59] However, the chapter also provides an "explaining what really" form of explanation that, through the concept of *i-veillance*, points to new practices and illuminates old practices in new a light.[60] (For example, border checkpoints not only keep people in or out of territory, but they also serve a

---

[56] Karp 2013 provides different methods to identify practices. My concept-driven method is different from those he identifies.
[57] Gerring 2012, 727.
[58] Ibid.
[59] '[A]ny empirical proposition that attempts to answer a what, when, whom, out of what, or what manner question is classified as descriptive.' ibid., 743.
[60] Dray 1964.

surveillance function.) This sets the stage for the empirical chapters in which I subsume phenomena under the *i-veillance* concept.[61]

Although *i-veillance* practices are international (as I have defined them), to understand them it helps to start with a domestic analogy. After all, the story of the modern nation state is largely a story about how the state developed centralized power over the individuals within its territory. Fundamentally, for a state to maintain anything resembling a monopoly over the use of force (and more generally an administrative monopoly) it must have the capacity to (a) know its subjects and (b) make interventions against individuals who are threatening or do not abide by established legal norms. As Dandeker remarks on the Weberian formulation: "rational administration is a fusion of knowledge and discipline." This entails two feats for the state. On the one hand the state tries to enhance the "legibility" of its population.[62] A state maintains some level of surveillance and record keeping[63] on its subjects so it can "read off" details of their habits and behaviors. On the other hand, a state must be capable of making an intervention based off of that knowledge in order to, say, arrest or kill an individual. Some states are better than others at these feats, hence the familiar distinction between strong and weak or failing states. Strong states are those with what Michael Mann calls infrastructural power—the ability for the state penetrate and implement its will throughout its territory.[64]

States interested in pursuing idiocentric security practices will seek both knowledge of and capability over individuals, but with respect to individuals who live

---

[61] This method is what Dray (1964) refers to as 'subsumption under a concept' where the goal is to 'to look for certain dominant concepts or leading ideas by which to illuminate [...] facts, to trace connections between those ideas themselves, and then to show how the detailed facts become intelligible in light of them.' Walsh 1951, 62. Cited in Dray 1964, 32.

[62] Scott 1998.

[63] Giddens 1981.

[64] And Mann notes that states can wield such power more or less 'despotically'. Mann 2008; Mann 1984.

and move *abroad*. In this dissertation I focus on idiocentric surveillance. But before I get there, I review the basics of surveillance.

Basic Surveillance

The study of surveillance has its own discipline, yet it is relatively new. The field of Surveillance Studies "covers a huge range of activities and processes, but what they have in common is that, for whatever reason, people and populations are under scrutiny."[65] A representative definition of "surveillance" is: "the focused, systematic and routine" collection and analysis of "personal details for purposes of influence, management, protection or direction.[66]

Various elements of the definition deserve attention. First, surveillance is focused and routine. This suggest it is, at the very least, purposive, and incidental acquisition of data would not count as surveillance proper. Second, it includes both collection and analysis. Note also that collection entails the activity of gathering information as well as the storage of it. Storage, for example of data in a database, is an important component of surveillance because it enables those conducting surveillance to keep track of information over time and recall that information when needed. Analysis is included because often the collected data does not speak for itself. For example most information is classified (sorted) as it gets stored, and classification is itself a form of analysis. Moreover, technology increasingly enables automated data analysis and data mining to discover patterns and novel information. Third, according to the definition above different actors can conduct surveillance—governments, corporations, civic organizations, parents, etc. For my purposes the focus will be on governmental forms of surveillance.

---

[65] Lyon 2002, 1.
[66] Lyon 2007, 14.

Finally, surveillance is about people. Students of international politics may pause here—what about surveillance of material things like missile sites and nuclear enrichment facilities. Surveillance Studies, which has roots in sociology and human geography, is primarily interested in surveillance as a *social* and political phenomenon. That being said, sometimes surveillance of objects can provide a lot of information about what certain people are doing. This is well within the purview of surveillance studies. For an IR example, IAEA monitoring of gas centrifuges is similar to workplace monitoring intended to check whether or not employees are doing their job. On the other hand there is some material-focused surveillance which Surveillance Studies doesn't address. For example satellites and seismic and atmospheric monitoring constantly operate to detect nuclear detonations, but this is activity that Surveillance Studies is not too interested in.

Under the understanding that "[s]urveillance directs its attention in the end to individuals"[67] there is a lacuna in the Surveillance Studies literature that an IR focus helps bring to light. Because Surveillance Studies is primarily interested in domestic activity it takes one important thing for granted—territory. A domestic bias in the literature treats the state's access to people as a *fait accompli*. There are however cases in which the state cannot penetrate its own territory (or, in the international context, the territory of other states) effectively enough to closely monitor individuals. That is, sometimes the state is not *present enough* to even know where individuals are to monitor them. As a result states may monitor territory as a means by which to understand people. U.S. aerial surveillance along the Mexican border is an example of this. The surveillance of territory is still surveillance that "directs its attention in the end to individuals."

---

[67] Ibid.. And he goes on to note 'aggregate data [...] may be used to build up a background picture'.

The discussion of territory can be generalized in a useful way. IR's sensitivity to states' desire for security and certainty suggests that the state should focus on *any* domain in which individuals may be conspiring to harm the state. Surveillance can be applied to *any environment* in which individuals operate. This includes land and virtual spaces. Scholars of Surveillance Studies would not object to this. I am merely highlighting a point that doesn't get emphasized in the literature. This leads me to the following definition of 'surveillance':

> *State-led surveillance involves the collection, analysis and storage of information about people, their activity, and their environments for the purposes of influence and intervention.*

Though my focus is on state-led surveillance it is important to note how surveillance does not necessarily take the form of a naked application of power in which one agent (the state) exerts itself clearly against the will of another (the individual). The effects of surveillance—its power—can be more insidious. Foucault and his Panopticon metaphor in particular loom large in discussions of surveillance.[68] The Panopticon was a penitentiary model developed by Jeremy Bentham. The basic idea was to construct a prison in which jail cells would be constructed along a circular perimeter, with a guard tower at the center. The cells would be designed such that at a glance the guard in the center would know what the prisoners were up to. Moreover, the guard tower could be constructed so as to conceal the presence of the guard. In this way good behavior might be induced because of the uncertainty as to whether a guard was on duty. Foucault took Bentham's architectural design as a metaphor for disciplinary models in society. The

[68] Foucault 1995.

panopticon represents a technology of power in which the few can watch the many. Foucault highlighted how certain institutions—prisons, schools, hospitals, factories—worked as such. He also pointed out how, even without direct supervision, subjects might internalize the gaze of such norm enforcement and therefore regulate their own behavior according to relevant norms. Surveillance studies have gone beyond Foucault's imagery (though his insights have not been discarded). For instance, surveillance occurs not only when the few watch the many, but also when the many watch the few. Mathiesen refers to this as the 'synopticon'.[69]

The insights of Foucault are fecund for thinking about domestic surveillance, but less so for international surveillance. Thinking *international* surveillance of individuals—what I call '*i-veillance*'— through a governmentality lens or with an emphasis on the Panopticon would be an awkward fit. This would be inappropriate primarily because governmentality concerns practices which render *populations* as subjects of government concerning economic and biological practices.[70] Whereas *domestic* surveillance practices (e.g. epidemiology or credit scoring) can dispose actors in the way governmentality suggests, *i-veillance* better resembles a blunt coercive practice. Moreover, *i-veillance* transpires without the thicker social and normative environments that make governmentality, disciplinary power, and biopower proper lenses of analysis. Finally, Foucault's writing on surveillance was connected to his study of government, not sovereignty (the distinction is Foucault's). He writes, the purpose of government is "the welfare of the population, the improvement of its condition, the increase of its wealth, longevity, health, etc.; the means [...] are in some sense immanent to the population; it is the population itself on which the government will act either

[69] Mathiesen 1997; See also: Lyon 2006.
[70] Foucault 2007; Dean 2010.

directly through large-scale campaigns, or indirectly through techniques that will make possible, without the full awareness of the people [...]."[71] Sovereignty, on the other hand, "is not exercised on things, but above all on a territory and consequently on the subjects who inhabit it."[72] The purpose of exercising sovereignty is the maintenance of sovereignty itself. Using Foucault's own terminology, *i-veillance* is a sovereign practice. Perhaps in a (future?) world in which we see something like a world state a Foucaultian analysis of *i-veillance* would be more fitting.

In the run-up to the discussion of *i-veillance* it is more helpful for me to focus on how surveillance is used as "compulsory" and "institutional" forms of power serving government interests.[73] Governments engage in surveillance because, broadly speaking, it facilitates the task facing governments vis-à-vis their populations—administration. When conducted by agents of the state, surveillance is a form of administrative power—a means by which the state can influence the affairs of people.[74] Administrative practices subsume the comparatively muscular activities of 'social control'--"all those mechanisms which discourage or forestall disobedience, which either punish such behavior once it has occurred, or prevent those with inclinations to disobedience from acting on those inclinations."[75] In this case, surveillance "entails a means of knowing when rules are being obeyed, when they are broken, and, most importantly, who is responsible for which [as well as] the ability to locate and identify those responsible for misdeeds of some kind."[76] One can see that surveillance is the silent partner to the state's coercive monopoly. A mark of the "modern" state is a reliable surveillance capability that ensures

---

[71] Foucault, Burchell, and Gordon 1991, 100.
[72] Ibid., 93.
[73] As opposed to power's more constitutive effects. Barnett and Duvall 2005; For Political Theory work on power see Hayward 2000; Lukes 2005; Gaventa 1982.
[74] Giddens 1985.
[75] Rule 1974, 20 Rule's text is an early and prescient work in the field of surveillance studies.
[76] Ibid., 22–23.

the state can exercise power throughout its territory. From the Weberian perspective states "possess a legal and administrative order comprising a body of formalized legal norms and a rational bureaucracy. [...] The bureaucracy is charged with implementing such legal norms over the state's territory and population. This activity involves a permanent and continuous exercise of surveillance."[77]

For a better appreciation of what surveillance achieves for the state's administrative capability I turn to James C. Scott. Although Scott is not focused on surveillance *per se*, he writes incisively on how states render society 'legible'—that is, understandable to the state. To wield administrative power, society must be legible to the state. Just imagine the task facing a modern state seeking to administer a large population, upon whom the state is dependent for, among other things, tax revenue. It truly is an astonishing feat we take for granted. Administrating a population is further complicated by the size and geographic diversity of a territory. This prompts Scott to ask, "How did the state gradually get a handle on its subjects and their environment?"

> Suddenly, processes as disparate as the creation of permanent last names, the standardization of weights and measures, the establishment of cadastral surveys and population registers, the invention of freehold tenure, the standardization of language and legal discourse, the design of cities, and the organization of transportation seemed comprehensible as attempts at legibility and simplification. In each case, officials took exceptionally complex, illegible, and local social practices, such as land tenure customs or naming customs, and created a standard grid whereby it could be centrally recorded and monitored.[78]

When it comes to understanding how states manage their internal population, we need to appreciate that behind and alongside the state's coercive power is the power to render society legible.

To render society legible, and thereby shore up administrative power, the state conducts surveillance on its subjects. As mentioned above this entails the collection of

---

[77] Dandeker 1994, 10.
[78] Scott 1998, 2; Li 2005 offers an 'amplification' of the main themes of Scott's work.

information, the storage of information, and the analysis of information. Information can be collected in the first instance by instruments or by direct observation by a person. I refer to these means of collection as *sensors*. Examples of instrumented sensors include cameras, audio recording equipment, and wiretaps. Increasingly databases themselves act as sensors insofar as transactions—credit card purchases or cell phone calls—are immediately and automatically recorded. Humans—the cop walking her beat or the DEA agent tracking a suspect—can be sensors too. Much of the data collected by sensors finds its way to a written or digital record. The *storage* of information is an important part of surveillance. Storing personal data empowers the state in numerous ways. Beyond facilitating basic record keeping, it allows the state to track changes over time, establish important links with places and persons, and make impressive inferences. Anthony Giddens thinks of such personal information as an 'authoritative resource'—a resource that the state can use to control people—which redounds to enhance the state's administrative power.[79] "Storage of authoritative resources is the basis of the *surveillance* activities of the state, always an undergirding medium of state power."[80]

The state's capacity to conduct surveillance is difficult to measure, especially for more sophisticated modern states. States can "reach deep" so to speak and increase their capabilities if given circumstances warrant it. A state's surveillance apparatus is better thought of as a "surveillant assemblage"—"not a single physical entity or system, but the sum total of the surveillance capacity that can be trained on a location or population. As such, it is less a 'thing' than it is a potentiality that can be actualized to varying degrees depending on what and how observational regimes are combined and aligned."[81] The surveillant assemblage concept usefully underscores that there is an active surveillance

[79] He contrasts 'authoritative' with 'allocative' resources which give the state power over the material world. Giddens 1985, 4,47.
[80] Giddens 1981, 5.
[81] Haggerty and Gazso 2005, 173.

apparatus that can ramp up or tap into other sources of information collected by other actors, and different practices and technologies of surveillance although operating separately may interface with one another, for example through information sharing or data searching. This is illustrated by the U.S. government investigation in the immediate aftermath of the 9/11 attacks (See Table 1). The U.S. government did not maintain all the data used in the investigation itself. Rather it simply tapped into it when needed.

Table 1. Forms of surveillance used to track actions of September 11th terrorists[82]

Air Traffic Control Airline Flight Records Arrest Warrants (outstanding) Automobile Registration Automobile Rental Records Automobile Financing Records Bank Records Black Box (airplane) Credit Card Records Criminal Records DNA (recovered from crash sites) Driving Records (i.e. speeding tickets) Driver's License E-mail Logs Employment Records Fingerprint Records Ferry Records Flight School Records Forensic Evidence Hotel Booking Records Immigration Files Intelligence Databases	Mailbox Rental Records Medical Records Pilot's License Parole Records Passport Personal Computer Records (suspected terrorists) Photo Identification Card Radar Tapes Refugee Claims Rent Subsidy Cheques Securities and Exchange Trading Records Student Records Surveillance Camera tapes (airport, banks, etc.) Taxi License Telephone Logs Telephone Numbers Transponders (airplane) Vehicle Registration Video Footage Visa (records, applications) Wedding Photographs Wiretaps

The NSA's collection of metadata from private telecom companies serves as another example. In this particular instance the NSA collects the data so it can use it itself, *if necessary*. This highlights that governments (though, not all) have a unique ability to seek additional data from the private sector (by request, court order, or through investigations) that is not available to other private sector actors. For example, it is likely easier for the government than it is for Google to secure hotel rental information across a

[82] Table pulled from ibid.

certain period of time. So, despite the impressiveness of data held by a company like Google, state-led surveillant assemblages can be more powerful (even though it might rely on the data provided by the private sector).

There is a lot of data to tap into. Here is where data analysis is clearly relevant to surveillance. As storage capabilities have increased and with the advent of searchable databases and sophisticated data analysis tools, the state can take classification (or "cladistic" practices) to a whole new level. Lyon argues that "social sorting has become central to surveillance. [...] Abstract data [...] are manipulated to produce profiles and risk categories in a liquid, networked system. The point is to plan, predict, and prevent by classifying and assessing those profiles and risks."[83] Advances in data storage, computing, and analytical tools have amplified surveillance capabilities tremendously. The term "dataveillance" describes a type of surveillance which doesn't watch or listen per se, instead it combs through large amounts of data to reveal new information about or create profiles of individuals. "Data mining" is the popular term describing how analysts (with the help of automated algorithms) search for new patterns and links within large data sets, sometimes with the purpose of predicting certain phenomena. The post-9/11 "Total Information Awareness" program by the U.S. military's cutting edge research wing, DARPA, is the most well-known example of datamining. The program, which was cancelled due to its controversial intent and capability, would have combed through large masses of data on U.S. citizens to look for patterns of actions and transactions that resembled patterns observed in the planning and execution of terrorist attacks.[84]

---

[83] Lyon 2003, 13.
[84] Although this specific program was cancelled, its mission and technology lived on in other forms.

The feared East German Stasi "amassed security files that took up two hundred kilometers of shelf space" that "was searched manually."[85] However, the capabilities of today make the surveillance capabilities of even a generation ago look like an anachronistic joke. Josef Teboho Ansorge has drawn attention to the effect of databases and what he calls 'digital power'.

> Mastering databases is a part of practices which make 'states' into modern stable states; which constitutes the difference between formal-legal sovereignty and technical-actual sovereignty. In this way, databases are fundamental means of reproduction of individual societies and thereby of the international system. They are both a way of knowing and devices of order. Accepting the premise that 'Power is the production, in and through social relations, of effects that shape the capacities of actors to determine their circumstances and fate'[86] impels a recognition and close study of the particular type of political power exercised through information technology. This forces the question: 'What is seeing like a state when the state sees through databases?' The answer is a new form of radicalised bio-power that is sufficiently distinct to warrant its own signifier, digital power.[87]

The use of databases, dataveillance and more modern forms of risk-based governance[88] has facilitated surveillance on abstractions of subjects, rather than direct observation of the subjects themselves. "[R]isk is based on using statistical techniques in order to deduce or infer profiles of people who are not under the immediate gaze of the observer. [...] Thus, 'surveillance is practiced without any contact, or any immediate representation of the subjects under scrutiny'"[89] This represents de-territorialized surveillance that occurs in abstract space.

---

[85] Marquis 2003, 227.
[86] Here he cites Barnett and Duvall 2005, 42,25.
[87] Teboho Ansorge 2011, 73. He argues that the paradigm for the database—a 'blueprint for digital power'—is not the Panopticon, but rather 'Cuntz's Tower.' Erwin Cuntz detailed plans for a single 25 story building storing information on all German citizens. He penned his plans for Hitler in 1934. Luckily they were ignored.
[88] See Ericson and Haggerty 1997. On the role of 'risk' in governance see work by Ulrich Beck and Anthony Giddens.
[89] Zureik 2003, 39 citing Castel 1991.

Surveillance produces profiles of people and their lives. Profiles will be of varying degrees of 'resolution'—meaning, the higher the resolution the more detailed the profile.[90] As a power resource, surveillance enables the state to make interventions against individuals,[91] and the state can make more or less precise interventions depending on the information it has. More precise details enable the state to make more precise interventions. As the state accumulates more details on individuals, it gains higher resolution picture of their lives. The higher the resolution of information, the more details the state can 'see', and the more precise its interventions can be. For example, say that British intelligence services learn that an al Qaeda member has an account with Barclays bank. With that information alone the British could not do much. If it had the last name of an account holder, it could monitor or freeze all accounts that match that name. If the name were common this course of action would likely be imprecise and unhelpful. More information—ideally an account number—would enable the government to make the precise intervention it needs.

This concept of resolution is also intended to convey that different types of information can bring different features of the individual's life in to focus. The content of communications help clarify intentions. Photographs help resolve identity. Travel records bring resolution to an individual's area of operation. Of course different types of information will be more or less relevant depending on the type of intervention the state wishes to make. But in general, the greater resolution helps the state to *individuate* individuals from one another and to *individualize* people by understanding more details of their individual lives.

---

[90] I intend 'resolution' to subsume 'fidelity,' a concept that captures whether the information about an individual truly corresponds to that individual rather than someone else.

[91] Again, this is one of the takeaways from James C. Scott (Scott 1998, 183).

This point about resolution is not a common theme in the surveillance studies literature.[92] Again I suspect that the reason is that most of the literature presupposes a domestic context for surveillance. In the domestic context it is easier to for the state to do what it needs to know what it needs to know, so certain details of surveillance don't get thematized. As we move to the international context things change. States cannot simply do whatever they want with respect to individuals living in other states.

To sum up what has been said thus far: The state wields administrative power over individual subjects. A basic requisite of this power is the ability to render society legible. To achieve this, the state engages in surveillance. The state collects information through sensors—instruments, databases, and humans. It stores information in databases of immense capacity. And it analyzes its data stores to learn even more about the state's subjects. Data begets more data. Higher-resolution profiles of individuals enable the state to take preventative actions or interventions against individuals it deems threatening. As a surveillant assemblage with sovereign prerogatives the state can expand its capabilities often through tapping into infrastructures of other states or of private corporations.

i-veillance: The Surveillance of Individuals Abroad

I-veillance is the collection, analysis and storage of information *by one state* about people, their activity, and environments *of another state* for the purposes of influence and intervention. The concept marks a practice that differs from domestic surveillance of individuals and foreign surveillance of states (and

[92] In a recent report about how police use license plate readers to record license plates as they go by, the ACLU makes use of the idea of 'resolution' in a way similar to me. 'More and more cameras, longer retention periods, and widespread sharing allow law enforcement agents to assemble the individual puzzle pieces of where we have been over time into a single, high-resolution image of our lives.' American Civil Liberties Union 2013, 2.

their agents). Practically speaking, the surveillance on individuals abroad is more difficult than in domestic settings. While the fundamentals remain the same the context has changed. The state is no longer working within the familiar confines of its own borders, armed with the authority and resources to surveil (by force if necessary). What does it mean for a state to pursue a robust surveillance capability against individuals abroad? What does this idiocentric surveillance look like?

There are two main features of i-veillance that distinguish it from traditional forms of foreign and domestic state-led surveillance practices. On the one hand i-veillance is different from what IR may regard as surveillance in that the ultimate goal of i-veillance is to know about individuals, not states. On the other hand, unlike domestic surveillance i-veillance focuses its sensors outward to foreign, not domestic, jurisdictions.

Targeting Individuals Abroad

We begin by distinguishing *i-veillance* from the more traditional international surveillance conducted against states and agents of other states. The traditional state-focused surveillance focused on gathering information about foreign states' capabilities, interests and intentions. Early U.S. satellites, for example, were dedicated to photographing Soviet military assets. And insofar as individuals are targeted under traditional surveillance, they are targeted so as to understand what another state is up to. *I-veillance* targets individuals who themselves, not acting on behalf of a state, are a potential threat to the state's interests. So the targets are individuals *qua* bad-guys, not *qua* state-actors.

Targeting individuals requires a different approach from targeting state-related targets. This is so for two reasons. First, the behavior of each is different. Second, the

information relevant for gaining resolution on each is different. Contrast how individuals and states behave over time and in space. They each work in different "time-space scales" as it were. Whereas states operate in relatively fixed spaces demarcated by territorial boundaries, individuals flow more easily within and between jurisdictions. Whereas states move and think slowly like the leviathans they are depicted to be, individuals move and think in real time as it were.[93] That is, meaningful or otherwise operationally relevant action of individuals occur in real-time and real-space, whereas relevant state behavior is stretched over larger time-space scales.[94] This helps explain why the US intelligence community had to reorient and recreate itself after 9/11.

The important upshot for conceptualizing *i-veillance* is that states seeking a reliable ability to gain high resolution profiles of individuals have to develop an infrastructure of surveillance that can operate at the relevant scales of individuals. At the extreme this means developing sensors that can capture all the micro-moments of our lives. Yes, it is relevant whether or not a bad guy intends to detonate a bomb on a bus. But from a surveillance perspective the minutia of his life is relevant as well. What is his daily routine? Who does he call? Who does he visit? Where has he travelled? Where does he get money from, and where does he spend it? A state interested in *i-veillance* will try to deploy sensors to get this information. But because this information circulates in difficult to reach places such as personal and virtual spaces, the state is faced with the challenge of deploying sensors where it might not have easy access.

Access to information is difficult enough when the target is an individual, and even more difficult when that individual lives in a foreign state. Now add to this the fact that globalization has altered how individuals interact in space and time at a global level.

---

93 True, individuals whom the state focuses on typically operate as parts of larger organizations or networks, they nevertheless operate at different time-space scales than the state.

94 Again, there are exceptions, especially in the conduct of war.

"Rising geographical mobility, plus the stretching of social relationships enabled by … new transport and communication technologies, [… means] the general decline of face-to-face relationships."[95] Individuals can conspire in virtual space with others whom they have never met and who live thousands of miles away. Communication is instantaneous. The flow of people and goods is voluminous and fast. The state, seeking to surveil and know individuals outside its borders, has the challenge of operating in the space and time scales that are relevant to the interaction of individuals on a global scale. Interested states are likely to extend their surveillance infrastructure into dense transaction spaces of individuals.

How states project *i-veillance* is also informed by the fact that states are conducting *i-veillance* over individuals for security purposes. The targets of surveillance include not only known individuals, but also those individuals who might become a problem for the state. And individuals, especially unknown ones, might be anywhere within a given territory.[96] Similarly, individuals may commit infractions or otherwise show up on the state's radar at any given time.

The implication of all this is that states pursuing an i-veillance capability will tend toward developing an infrastructure that is (a) distributed throughout multiple foreign jurisdictions and (b) is continuous (or, in other words, persistent). The state can achieve this by putting its surveillance capabilities closer to those individuals or throughout the environments (e.g. territory) where they move and transact. A more comprehensive distribution of a persistent surveillance capability will contribute to the resolution a state can achieve. Within surveillance studies there is not much of a focus on distribution and continuity. Again, I suspect this results from a domestic bias in the literature.

---

[95] Lyon 2007, 125.
[96] Following this logic, the U.S. sometimes extends its surveillance web to cover loved ones of suspected and known terrorists.

Domestically, a well distributed and readily available surveillance structure is a *fait accompli* (at least for stronger states).

Recall that any such surveillance capability can be regarded as a 'sensor'. An array of sensors make for a surveillance infrastructure. The more sensors, arrayed properly, the higher the resolution. Imagine the U.S. listening to cell phone chatter of suspected terrorists using its own sensors (satellites). It may get a partial picture of who is talking to whom. The U.S. then receives information from the sensors of others, say listening posts in Australia, and the picture becomes clearer. Perhaps it becomes clear that a suspected terrorist in Pakistan is in touch with an extremist group in Indonesia. The CIA might then get in touch with its Indonesian counterparts, compare notes, and increase the overall resolution of who is doing what, where, and when.

We can use the eye as a metaphor here. The eye is designed such that certain light receptors (cones) are more densely packed near the center of the retina (known as the fovea). This allows for more detailed focus in the center of the visual field. The state requires greater resolution for its center of focus—e.g. known and suspected terrorists. The state develops its retina. It packs it with as many receptors as possible. The state then uses its own receptors and the receptors of others when available.[97]

Infrastructure in Foreign Spaces

The fact of *i-veillance*'s focus on individuals abroad forces us to think about the state's infrastructure of sensors it projects abroad. This is the second aspect of *i-veillance* that deserves more attention. The questions of interest are: How is the infrastructure

---

[97] We expect the state to pursue less resolution for individuals that come from populations the state deems less threatening risky. Note also that with time capabilities change. In particular the capability of extracting more information and the capability of storing more and more information. As these capabilities increase, so does the state's visual center of field. That is, the state can afford to keep track of more and more individuals, even those whom the state does not view as threatening.

articulated into foreign spaces, and what is the relationship between one multiple states' infrastructures in the conduct of *i-veillance*?

Sociologist Michael Mann distinguishes two types of political power.[98] The first is infrastructural power, "the capacity of the state to actually penetrate civil society and implement its actions across its territories."[99] It is an "institutional capacity" giving the state "'power through' society, coordinating social life through state infrastructures."[100] Examples include the ability of the state to extract taxes at the source, regulate business, and establish an effective police presence.

This idea of infrastructural power is contrasted with "despotic" power—"the range of actions that state elites can undertake without routine negotiation with civil society groups."[101] This is the state's power *over* and against civil society. As Mann writes, "despotic power can be 'measured' most vividly in the ability of all these Red Queens to shout 'off with his head' and have their whim gratified without further ado—provided the person is at hand."[102]

I introduce this language, and the idea of infrastructural power in particular, because it captures well how surveillance works in the modern age. "Infrastructural power is connected to the Weberian tradition of the state as a set of institutions that exercise control over territory and regulate social relations."[103] When the state works despotically it sends an agent to muscle you around or kill you. When the state works through infrastructures the state might be exerting control through bureaucrats, agents, or processes with which you interact on a regular basis. Mann refers to this feature of

---

[98] For my purposes can also be thought of as two forms of 'administrative power' referred to earlier. Nothing hangs on this distinction.
[99] Mann 2008, 355.
[100] Mann 1993, 59.
[101] Mann 1989, 113; Mann 1993, 59.
[102] Mann 1989. Originally published in The European Sociology Archives. Vol. 25, pp. 185-213.
[103] Soifer 2008, 233.

infrastructural power as "caging social relations." An *infrastructure* of surveillance therefore usefully captures how the state surveillance apparatus insinuates itself into the warp and weft of society, caging social relations within its operations. When surveillance happens it is not necessarily something that is suddenly summoned and foisted upon us in some obvious intrusive way. Rather, it often already a part of peoples' daily routines. Surveillance exists *in potentia* when we make a phone call, search the internet, make a purchase, or when we walk down the street.

The point is we can think about a state's *i-veillance* capacity as an *infrastructure of sensors* that penetrates throughout the globe and insinuates itself about the lives of individuals. It used to be that if one state wanted to get information about an individual who lived abroad, that state would have to contact representatives of the state in which that individual lived and make the request. This could occur through a liaison relationship, an embassy contact, or the diplomatic instrument known as "letters rogatory." Gone are those days. The idea of an infrastructure of sensors captures a more diffuse and penetrating form of surveillance in which data is collected more routinely and often automatically. And more information concerning social interaction is being captured by this infrastructure. The result is a greater amount of infrastructural / administrative power.

We might expect varying degrees of cooperation and coordination when one state wants to pursue *i-veillance* in another state. The U.S. for instance negotiates the terms of, among other things: the presence of personnel, the provision of technology, and the nature of information sharing. Regardless, this draws our attention to a peculiar dimension of i-veillance. Domestically we are accustomed to thinking about the state's coercive and administrative monopoly. That is, there is one state infrastructure throughout a given political territory. But *i-veillance* entails projecting infrastructure

within the territory of another state. What then are the types of relationships that occur when we see two or more infrastructures at play within a given territory?

There are two types of infrastructural relationships between states (call them the "projecting" and "host" state) which cooperate on *i-veillance*. The infrastructures could be *shared* or *synaptic*. Shared infrastructure occurs when the projecting state and the host state both contribute to the practice at hand. The extent of sharing can vary. On one end of the spectrum there may be a merging of state resources and personnel. On the other end, the host state may simply give permission for the projecting state to conduct surveillance.

Synaptic infrastructure exists when the infrastructures of the projecting and host states are brought closer and closer together such that they can more easily interact when necessary to conduct *i-veillance*. Infrastructures can be brought closer in different ways. First, they can literally be closer in proximity. Having a legal attaché in another country is an example of this. The law enforcement agents of the hosting state can literally walk to the U.S. embassy and chat with the U.S. attaché. Second, closeness can be achieved by working toward interoperability and common standards. For instance when the U.S. helps another country set up information systems to monitor or track individuals, the U.S. imposes its own IT standards. This makes working with that country and its data easy. Either way, in these cases *i-veillance* occurs when the synaptic infrastructure "fires." Closeness is achieved as the two countries bring their infrastructures closer together, either in space, time or in terms of minimizing the effort required to achieve the intended goal. Even in the midst of a privacy debate between the EU and the U.S., the desire to keep things close is evident. William Kennard, the US ambassador to the EU, said "As we both modernise our data privacy systems we must make sure that we build interoperable systems that protect privacy and protect our

citizens from transnational criminal threats." Interoperability brings the nation's surveillance systems closer together.

Despite all its power, it is wrong to think that the U.S. has all the information and other states go to the U.S. to learn about what threats they face. The U.S. certainly has access to and stores of data. But it is certainly true that some states have stronger privacy laws that prevent unrestricted data sharing. This would be the case for the EU for instance. And such cases would seem to cut against the thesis of the dissertation. But instead of direct, unfettered access, what we see are infrastructures that facilitate and encourage surveillance. The US-EU example might be conceptualized as synaptic. That is U.S. surveillance infrastructures and EU surveillance infrastructures are brought closer together. The closer they are, the more interoperable they are, etc. the more likely the synapse can 'fire.'

In addition to projecting capacity abroad, a state can build the surveillance capacity of other states with the intent of tapping into it. Examples of this can be found in various state building enterprises engaged in by the U.S. The U.S. will help a state build its capacity in ways that facilitate information collection and sharing. Finally, a state can develop a shared capacity with another state. Examples here include intelligence sharing arrangements.

Like all surveillance, *i-veillance* seeks to "make visible the identities or the behaviours of people of interest."[104] The more information the better. In practice, however, *i-veillance* is limited to certain types of information. Resolution is enhanced by information sources that shed light on an individual's: Identity, Intentions, Capabilities, Time-Space Habits, Social Network. Table 2 outlines some main categories and provides examples.

---

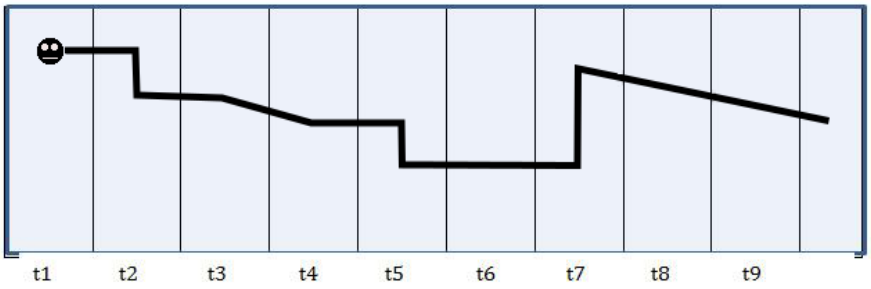
[104] Lyon 2002, 2.

Table 2. Information types	
Information Type	**Example**
Imagery	Satellite / Drone Imagery
Communications Content	Content of an Email or Call
Communications Metadata	To/From Details, Call Length
Personally Identifying Information	Passport, DNA, Fingerprints
History of Illicit Activity	Criminal Records
Financial Data	Bank Account Information
Commercial Transactions	Credit Card Statement
Social Network	Who are family and friends? Often a product of further data analysis.
Other Behavioral Information	Daily Routines, Diet, Habits, etc.

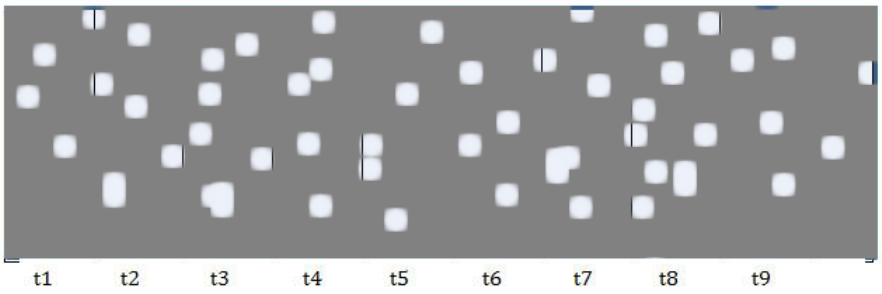
The most essential details concern individuals' movements, routines and interactions in time and space. "Coordinates are key. Anyone who can pinpoint the time and place of some event or activity already has a handle on the situation."[105] Coordinates are rudimentary for administering individuals. The more precise space and time details concerning an individual's life, the higher the resolution. This also explains why states might sometimes train their surveillance on an expanse of land in order to document activity there. But beyond knowing the coordinates that help individuate people, there might be additional details that help individualize people. The higher the resolution the more options the state has for intervention (See Figure 1)

[105] Lyon 2007, 16.

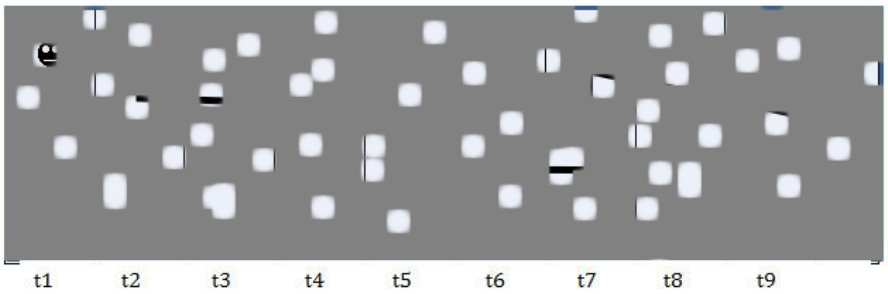
Figure 1: Example of Resolution Enhancement



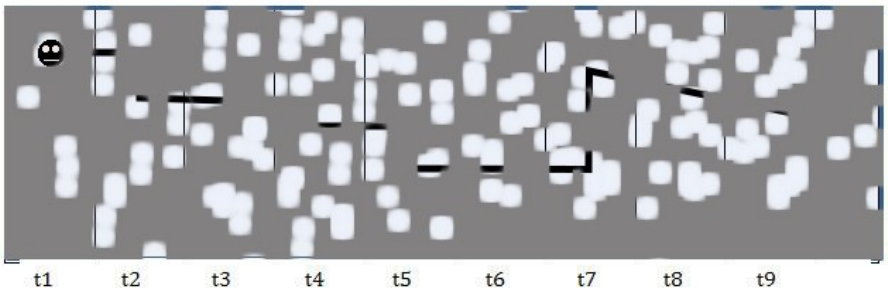
This first frame represents perfect knowledge of an individual moving through space at different times, *t*. A vertical line indicates the person is stationary.



The second frame depicts the state's surveillance capability over the same territory and time. The grey area represents where and when the state is **blind**.



Given the state's capability above, this represents what the state can see of the individual's movement in space and time.



If the state's capability is enhanced, the resolution is increased, and the state can 'see' more information about the individual's movement.

To make precise interventions against individuals abroad the state will deploy or develop sensors to get high resolution profiles of the individuals in question. A well-developed sensor infrastructure can individuate and individualize its targets. A state can develop its own infrastructure, but it can also take advantage of the infrastructures of others thus increasing its capacity as a surveillant assemblage.

What strategies of surveillance are states likely to pursue? States cannot share information or project power willy-nilly. There are important constraints at play, sovereignty being chief among them. A state concerned with individuals abroad will likely rely on or help develop the capacity of a partner state. The surveillance strategy pursued by concerned state will likely be a function of the internal capacity of the host state and the nature of the relationship between the concerned and host states. These dynamics will be evident in the empirical chapters that follow.

Standards of Evidence and Case Selection

With the conceptual work done, what is the upshot for empirical work and analysis? My basic thesis is that *i-veillance* is a significant international practice, a major political phenomenon in its own right. My initial goal, therefore, is to map state infrastructures of surveillance. I detail institutions, technologies and practices of surveillance. But this involves more than just listing. Importantly, I am yoking together a bunch of facts about the world and giving an interpretation of these facts. Therefore I need to explain what types of evidence I use and what standards I use in making my interpretations and inferences.

In the pages that follow I do three things:

a. map surveillance infrastructures and technologies;
b. make empirical claims about the political and strategic circumstances of specific instances of *i-veillance* in the cases presented; and

c. make theoretical claims about the consequences of *i-veillance* practices.

For each of these—the mapping, the empirical claims, and the theoretical claims—I need to convince the reader of my various interpretations. For each, I develop straightforward standards of evidence to which I now turn.

Mapping i-veillance

Knowing what and where the sensors are provides the starting point for understanding surveillance. By detailing sensors, understanding their basic operation, tracing the information flows—from collection to analysis—one can start to see not only how sensors contribute to high resolution maps of individuals, but also the broader surveillance infrastructure and how that infrastructure bumps up against other state's surveillance infrastructure.

The driving standard of evidence here is simply whether or not the sensor fits the concept of *i-veillance* outlined above. That is, does it provide the state with personal details of individuals outside that state's borders, or does it store such details. When it comes to identifying sensors, there is a risk of focusing only on the more obvious kinds associated with spying—say, drones and wiretaps. A bit of imagination is required. We are looking for any practice that is set up in order to collect the personal details of individuals abroad. So something like border controls which are typically regarded in terms of their security function (keeping the bad guys out) can also be seen as a sensor that collects and stores data on travelers—data that can be later retrieved for analysis. Similarly, the existence of a law enforcement liaison relationship might be more than just a tool to make arrests when needed. It might also be a sensor unto itself that serves as eyes on the ground. In addition, recall that a state's surveillance capability should be understood in terms of a *surveillant assemblage*—that is in terms of how the state can inflate its capacity by tapping into additional sources (i.e. other sensors). Finally, when

looking for examples of *i-veillance* only intentional surveillance practices count. Incidental surveillance should not be included.

In the spirit of 'starting with the sensors', I break up collection and the sensors that do the job into three categories: remote (instruments), databased, and human. An empirical chapter (chapters 4, 5, & 6) is dedicated to each. This division deserves some justification.

At first cut, sensors can either be artifacts or human. Artifact sensors can be categorized in different ways depending on how one wants the analysis to proceed. For instance, are the sensors mobile or fixed? Are the sensors collecting raw data (the voice data from a telephone call) or data in an already structured form (the identity of a traveler from a scan of his passport)? We could make any number of distinctions.

Human sensors are relatively straightforward. In this case a human being simply conducts surveillance. Breaking down artifact sensors is not as straightforward. There are at least three types of artifact sensors—instruments, databases, and internet based. "Instruments" are those sensors which collect data at some distance. It can be said that they are directed at or applied to an information source. Examples include satellites, signals intercept technologies, and drones. The second type, databases, act as sensors in two respects. First human users often directly interface with databases which then make a record of that interaction. An example here would be a swipe of a credit card or a scan of one's passport. Another way in which databases act as sensors is that they themselves serve as repositories of information for users to store and retrieve. The third type of artifact sensor would be those that are applied to internet activity. This type of surveillance includes any form of email snooping, hacking, etc.

To keep things simple, I reduce these four (human and three artifact) sensors into three sensor types—human, instrumented, and databas*ed*. In the last type, I merge

sensors involved with databases and the internet into one category. Databased surveillance includes the use of database interfaces, as well as the surveillance of databases and internet activity. It may be a bit of a fudge, but my thinking is that these sensors primarily traffic in digital data (or from another perspective, data that circulates through internet protocols).

I acknowledge there are other ways of breaking down *i-veillance* for the purposes of research. For instance one could start with the different contexts under which sensors are used and proceed from there. Such an approach might break things down accordingly: cooperative, coerced, covert infrastructures. Another approach might start with the type of information collected by the sensors. For instance, one could divide up analysis according to the source of intelligence—Signals (SIGINT), Image (IMGINT), and Human (HUMINT)—and proceed from there. That being said, I think my approach of starting with sensors helps keep politics front and center. Sensors are the things and people which actually get deployed for tactical and strategic reasons. One does not deploy SIGINT. Rather one deploys an antenna array to collect SIGINT. This allows me to focus on *decisions* made by governments in more detail.

Where do I look to find and catalog sensors? My work was done through a lot of sifting of news and government documents. The sensors I describe in the following chapters are among what I believe are the main contributors to i-veillance. I doubtless omit many sensors, but this only suggests that with more time researching, the mapping of surveillance capabilities would only be more impressive. The main document types are listed in table 3. The list is not exhaustive, but very reflective of the research I conducted.

Table 3: Document types used in research		
Government Provided	Leaked Government Documents	Newspapers
• Congressional Testimony • Budget Documents • Congressional Research Service • Department Issued Reports (Defense, State, etc.) • Government Accountability Office Reports • Government Websites	• Wikileaks' Diplomatic Cables • Documents leaked by Edward Snowden	• The New York Times • The Washington Post • The Guardian (UK)

Evidence for Empirical Claims

The principal empirical claim of the dissertation is that i-veillance is a significant international practice that shapes security today. In addition to that larger point, the empirical chapters make other, smaller claims along the way. As sensors are identified an analysis of where they are and how they are used can reveal more details about the surveillance infrastructure. It can also tell us something about the international politics and strategies involved. To take an obvious example, the fact that the U.S. flies drones in Mali but sells drones to Italy might suggest that the U.S. is trying to enhance surveillance coverage of Northern Africa by projecting its own capacity in a weak state on the one hand and empowering an ally on the other.

In each chapter that follows I make empirical inferences about the international politics involved in *i-veillance*. Again, my evidence is based primarily on government documents and news sources. What might be called "gold standard" evidence would be a memo or quote from a practitioner of *i-veillance* explicitly detailing the intent and political considerations behind a particular instance of surveillance. Much of the evidence that I have, however, is more circumstantial. There is either not much written about the various programs or they are conducted in secret. And because much of the gold standard evidence I am after is secret, my research has often led me down peculiar

paths. I look at budgets, budget justifications, testimonies, government audits, speeches and testimonies. I amass as much evidence as possible and make reasonable triangulations. There will be some claims that rest on shakier evidential foundations. I do my best to alert the reader at these points.

Evidence for Theoretical Claims

The penultimate chapter of the dissertation examines theoretical implications. I argue that changes in norms, interests, and identity suggest a common international purpose in fighting terrorism—a task for which *i-veillance* is an indispensable tool. Second, I argue that there is an incipient internationalization of the state's surveillance function, itself a critical part of what it means to be a state. Finally, I argue that these internationalizations of purpose and power suggest an internationalization of authority with respect to *i-veillance*.

My inferences are derived from both the empirics and IR theory. The argument will build on interpretations given in the earlier empirical chapter, and will therefore be as good as that evidence. By the time we get to the final chapter the relevant theoretical issues—e.g. sovereignty, territory, and authority—will be evident. In this chapter (chapter8) I will go into greater detail of what my standards of evidence are for the claims I make at that point.

Case Selection

The conceptual work informs what we look for—that is, what counts as *i-veillance*. In the pages that follow I primarily look at the collection aspect of *i-veillance* and pay less attention to the storing or analysis of the data collected. I do this for two main reasons. First, this is where most of the action is. Collecting information often means placing a sensor somewhere where someone else might not like. At the end of the

day this is the primary sticking point in debates about surveillance,[106] especially when it comes to international surveillance against other countries' persons. Second, as difficult as it is to document collection efforts, it is more difficult to understand how governments store and analyze data.

For each of the "sensor" chapters I discuss the technology, map the usage of sensors and then give a more detailed case study. The goal is to show how the sensors are actually *used* and the politics behind their use. The cases are selected based on (a) whether there is enough grist for the analytical mill and (b) to give me as much illustrative punch as possible. I present the cases to impress upon the reader the dynamics and extent of *i-veillance*.

[106] Though, there is plenty of debate around storage and analysis too. For example, restrictions are sometimes placed on how long data is stored (by private companies as well) to assuage privacy concerns. See, for instance, the "retention" part of a Privacy Impact Statement issued by the U.S. on one of its databases. As for analysis, there is probably no better an example of a contentious program than the U.S. government's aborted "Total Information Awareness" program which would datamine otherwise ordinary and disparate data on individuals to discover patterns that might indicate suspicious behavior.

Chapter 3: Enabling and Facilitating Conditions

While some surveillance is conducted in secret (both unilaterally and multilaterally), there is much that is above board, or at least partially exposed. Importantly there is a lot of surveillance that is made possible by international agreements. So before analyzing surveillance sensors in subsequent chapters, this chapter looks at a few of the main institutional and legal conditions that enable and facilitate *i-veillance*. I argue that there is already a substantial international framework in place that enables or otherwise calls for *i-veillance*. The framework is a product of disparate agreements and institutions, not one overarching scheme. Taken together the agreements suggest a high degree of interconnectedness between states in terms of liaison relationships and information systems (e.g. data sharing). The result has the appearance of a more global *i-veillance* network.

Where to look for relevant agreements and institutions is motivated by the conceptual work done in the second chapter. The question at hand is: what international arrangements[107] create the conditions for *i-veillance*? "Create the conditions for" is vague and intentionally so. We must look not only at arrangements that directly result in surveillance but also at arrangements that indirectly produce surveillance. For the latter, we should add the caveat that such indirect effects count as *i-veillance* when, according the working definition of *i-veillance*, such surveillance is intentional. Imposing this threshold prevents us from picking out any and all arrangements that might incidentally

[107] Moving forward I use the word 'arrangements' as a catch-all for agreements and more formal institutions.

produce the possibilities for surveillance even though those possibilities are not being realized.

The most obvious form of an arrangement would be an information sharing agreement between countries. As a general practice information sharing is routine for intelligence agencies, and therefore it has received attention in Intelligence Studies. But much of this is done in secret.[108] There are however publically acknowledged agreements that specifically call for sharing information on individuals. The emphasis placed on information sharing within the agreement may vary, and it is here where we must be careful not to exclude such an agreement simply because information sharing is not highlighted as the primary purpose. The distinction I have in mind, which will be made clear below, is between so-called HSPD-6 agreements and Mutual Legal Assistance Treaties. In the former instrument information sharing is primary. The latter concerns ways to grease the wheels of judicial and law enforcement cooperation, and information sharing is simply part of the package.

But our sights are not exclusively set on information sharing arrangements. The dissertation is about surveillance more broadly and the cooperative efforts that may contribute to surveillance. Sharing information is but one facet of *i-veillance*. We therefore have to consider other arrangements which include permission to operate sensors in another territory, establishing liaison relationships, and sharing (not only information but) the technological information systems themselves. This highlights another reason I believe the idiocentric surveillance frame is useful. It forces analysis beyond the traditional horizons of intelligence studies to consider practices that may not

[108] Former CIA officer Arthur Hulnick writes, 'Information about relations between intelligence services is among the more sensitive issues in the intelligence profession. Intelligence services would find it difficult to cooperate with each other, if either partner stood the danger of having the relationship itself, let alone details about it, or its sources and methods compromised.' Hulnick 1991, 456.

be explicitly generated for intelligence purposes or which have secondary effects that nevertheless importantly contribute to the collection, storage and analysis of information on individuals' lives.

In this chapter I focus on efforts led by the U.S. and the UN, two international organizations (INTERPOL and Financial Action Task Force), and a commonly adopted treaty instrument—Legal Assistance Treaties—all of which in some way or another facilitate *i-veillance*. The arrangements below either call for or make possible the infrastructure of sensors outlined in the next chapters. Knowing where to look for relevant arrangements has been a product of the research process itself, trial and error, *etc.* Some of these arrangements are not well publicized or obviously connected to *i-veillance*. So the reader is presented with final results of my research, not the flotsam and jetsam that was reviewed along the way.

The United States' Efforts

As discussed in the introduction the U.S. has increased its focus on idiocentric surveillance in the 21st Century. One clear reason for this is the attacks on 9/11. Other reasons include the geopolitical slack afforded by the dearth of great power conflict and the fact that individuals are more empowered than ever to threaten state interests. The U.S. has acted as a prime mover in forging agreements and new international institutions that have a surveillance component to them.

The U.S. Attitude Toward I-veillance

Despite the shroud of secrecy that surrounds intelligence cooperation it is clear the US Intelligence Community (IC) works with "foreign partners". This is not a secret. To the contrary, international intelligence cooperation is a part of business as usual for the IC. Today there are four "partnerships" that the Office of the Director of National

Intelligence (ODNI) describes itself as engaging with—domestic, foreign, military, and private sector. With respect to foreign partners, the ODNI seeks to:

> Develop and implement an enterprise approach to foreign intelligence relationships, aimed at integrating and optimizing Intelligence Community engagement with foreign partners"; "Lead coordination of Intelligence Community sharing and foreign liaison issues"; and "Integrate and align key foreign intelligence relationships [...].[109]

The focus on foreign partnerships is explicit, and the quote suggests the IC seeks a deep engagement with other countries. Not only relationships, but also integration is sought.

9/11 had a major impact on how the U.S. views other states and their responsibility in counterterrorism. There are two features of this U.S. perspective that deserve attention here. First, the US views counterterrorism (CT) as an international *responsibility*. Among the U.S. stated objectives in its earliest "National Strategy for Combating Terrorism" was to "Establish and maintain an international standard of accountability with regard to combating terrorism."[110] It argued that "States that have sovereign rights also have sovereign responsibilities."[111] The U.S. efforts to get other states to take CT seriously relied heavily on the UN. According to the 2003 strategy document, the U.S. promised to "use [the anti-terrorism focused] UNSCR 1373 and the [12] international counterterrorism conventions and protocols to galvanize international cooperation and to rally support for holding accountable those states that do not meet their international responsibilities."[112] The language of responsibility is interesting. On the one hand the U.S. regards this international responsibility as derivative from specific international law. But on the other hand the connection between sovereign rights to CT responsibilities can also be read as something which UNSCR 1373 reflects rather than

---

[109] Office of the Director of National Intelligence n.d.
[110] The White House 2003, 18.
[111] Ibid.
[112] Ibid., 19.

establishes. For instance, the document reads, "Together, UNSCR 1373, the international counterterrorism conventions and protocols, and the inherent right under international law of individual and collective self-defense confirm the legitimacy of the international community's campaign to eradicate terrorism."[113] This line suggests that the legitimacy of the CT campaign pre-exists the international instruments mentioned.

Second, the U.S. divides states into categories depending on how willing and able they are to cooperate in CT efforts. Even though the Bush administration was known for its go-it-alone attitude, international cooperation was integral to the U.S. CT strategy. On the one hand we have the focus on the UN and other international arrangements mentioned above. But on the other hand was an emphasis on working with other states more directly. The initial CT strategy document broke up the world up into four different types of states: those that are "willing and able to be full partners in the campaign", the "weak but willing states", states that are "reluctant [...] to meet their obligations" and states that are simply unwilling.[114] The U.S. approach to working with others is summed up thusly:

> Where states are willing and able, we will reinvigorate old partnerships and forge new ones to combat terrorism and coordinate our actions to ensure that they are mutually reinforcing and cumulative. Where states are weak but willing, we will support them vigorously in their efforts to build the institutions and capabilities needed to exercise authority over all their territory and fight terrorism where it exists. Where states are reluctant, we will work with our partners to convince them to change course and meet their international obligations. Where states are unwilling, we will act decisively to counter the threat they pose and, ultimately, to compel them to cease supporting terrorism.[115]

The language of "willing and able" states persists in the 2006 CT document, but the stark language from 2003 (quoted above) is absent. Instead, for those states "reluctant to fulfill their sovereign responsibilities to combat terrorist-related activities

[113] Ibid.
[114] Ibid., 29.
[115] Ibid., 12.

within their borders" the U.S. would lean on diplomacy and the rest of "the international community to persuade [these] states to meet their obligations to combat terrorism and deny safe haven under U.N. Security Council Resolution 1373."[116] Likewise, the language of "weak" states is all but absent. These states are instead referred to in terms of "ungoverened or ill-goverend areas". The stated approach, however is the same; the US promised to "strengthen the capacity of such War on Terror partners to reclaim full control of their territory through effective police, border, and other security forces as well as functioning systems of justice."[117]

There are two watchwords here—capacity and partnership. Both find increasing use in the subsequent CT national strategies. State "capacity" is used twice in 2003, nine times in 2006, and 17 times in 2011. References to "partnerships" occurred 25, 41, and 59 times in the respective years.[118] The U.S. sees its CT relationship with other "willing" states as that of a partnership. Partnerships with "able" states are exercised through joint efforts. In its partnerships with weaker states the U.S. would help build their capacity to fight terrorism—a capacity that includes surveillance. The expectation is that the U.S. approach to *i-veillance* would be dominated by cooperative efforts with more capable states and assistance for weaker states to shore up their domestic surveillance capability. In what follows I look at each. But I begin by looking at the U.S. approach to "information sharing" which underlies the U.S. approach to working with both stronger and weaker partners.

As suggested by the ODNI quote above U.S. surveillance abroad relies on information sharing with other states. The overarching effort to share terrorism-related information with foreign governments is exemplified in general by the U.S. Information

---

[116] The White House 2006, 16.
[117] Ibid.
[118] For the 2011 CT strategy see: The White House 2011.

Sharing Environment (ISE) and more specifically by the consolidation of the government's approach to screening known and suspected terrorists. The ISE (and its related "Program Manager") was established in 2005 as a response to problems the Intelligence Community had in sharing information in the lead-up to 9/11. The ISE itself is not a database or one identifiable network. Rather it is a set of different information architectures, data standards, and best practices that help different "customers" (federal, state, local, tribal, and international partners) share information with one another. The ISE should be viewed as part of the background and supporting conditions within which much of the information sharing efforts of the U.S. government take place.

The ISE has a strong focus on sharing information with "foreign partners" (the phrase is used 65 times in the U.S. "National Strategy for Information Sharing"). "Strong and effective cooperation with our foreign partners is a vital component of the global war on terrorism. Sharing of terrorism information between [...] foreign partners and allies is therefore essential."[119] Just as the ISE pushes for the creation of an information architecture at home that facilitates sharing while nevertheless maintaining appropriate controls over who has access to specific pieces of information, the ISE works toward similar outcomes for its partner countries. "For foreign partners, it must create an environment in which terrorism information provided to or received from foreign governments is appropriately and adequately safeguarded and is made available, as appropriate to Federal departments and agencies."[120] Regarding "foreign partner needs," among other things the ISE plan recommends "[c]reating a central, electronically accessible repository of information on foreign government and international organization marking and handling regimes so that ISE participants can more readily

[119] ISE Program Manager 2006, 77.
[120] Ibid., 12.

understand the safeguarding and handling rules for different kinds of foreign government information."[121]

According to a 2009 ISE annual report, a "highlight of our [the ISE's] 2008-09 activities regarding the sharing of information with foreign partners was the consolidation and sharing of more than 400 unclassified agreements or agreement descriptions between Federal agencies and their foreign partners."[122] This consolidation of agreements exists in the ODNI's Foreign Intelligence Relationship Enterprise (FIRES) system—a "tool [that] assists officials involved in negotiating agreements and arrangements with foreign governments. The unclassified agreement and arrangement information provides FIRES users with insight into existing relationships between the U.S. and its foreign partners."[123] More detailed information concerning FIRES is unavailable, and unfortunately so is the list of the agreements it houses. However, unclassified portions of the ODNI's Congressional Budget Justification hints that FIRES is still in use and is expanding. The stated goal for FY12 is to: "Expand the range of data in the Foreign Intelligence Relationships Enterprise System (FIRES); and continue to work with IC elements to standardize their data so that it can be automatically uploaded into FIRES."[124]

U.S. Bilateral Information Sharing Agreements

Although the details of the hundreds of information sharing agreements with foreign countries are lacking, one set of agreements concerning how the government screens known or suspected terrorists is better known. In September of 2003 President Bush signed Homeland Security Presidential Directive (HSPD) 6. HSPD 6 required the government to consolidate and continue developing a database of information on

[121] Ibid., 21.
[122] ISE Program Manager 2009, 24.
[123] Ibid.
[124] Office of the Director of National Intelligence 2011, 123.

individuals known or suspected to be involved in terrorism and to "use that information [...] to support (a) Federal, State, local, territorial, tribal, foreign-government, and private-sector screening processes, and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes."[125]

The eventual result was the Terrorism Screening Database, also called the "Terrorist Watch List" (hereafter 'Watchlist'). HSPD-6 also called for "enhancing cooperation with certain foreign governments, beginning with those countries for which the United States has waived visa requirements, to establish appropriate access to terrorism screening information of the participating governments."[126] The result of this has been the proliferation of "HSPD-6 agreements" that deal with the bilateral exchange of "terrorism screening information." This exchange of information revolves around the Watchlist.

Understanding the significance of HSPD-6 agreements for surveillance requires a better understanding of the Watchlist —"the world's most comprehensive and widely shared database of terrorist identities."[127] The Watchlist is used for screening individuals. It is used within the U.S. at the federal, state and local levels, and also by "foreign partners who conduct terrorist screening operations."

> Terrorist screening occurs throughout the world at our embassies, ports of entry, and international postal and cargo facilities. Terrorist screening occurs during police stops, during special events, when a HAZMAT license is issued, or when a gun is purchased.1 Screening occurs when passports or visa applications are processed, as well as when citizenship and immigration applications are processed. Select foreign partners use a subset of the Terrorist Watchlist when they conduct screening operations abroad.[128]

---

[125] Bush 2003.
[126] Ibid.
[127] Healy 2009.
[128] Ibid.

The Watchlist is administered by the FBI with the help of partner agencies. It is a subset of a larger database of identities known as the Terrorist Identities Datamart Environment (TIDE) which managed by ODNI's National Counterterrorism Center (NCTC). The so-called "No Fly" list is an even smaller subset of the Watchlist.

To get on the Watchlist, individuals are first "nominated" for inclusion on the TIDE master-list (however domestic terrorist nominations submitted by the FBI can bypass the TIDE nomination process). Once in TIDE, the nominations receive further review to see if they warrant inclusion on the Watchlist. This requires two conditions to be met.

> First, the biographic information associated with a nomination must contain sufficient identifying data so that a person being screened can be matched to or disassociated from a watchlisted terrorist. Second, the facts and circumstances pertaining to the nomination must meet the "reasonable suspicion" standard of review established by terrorist screening Presidential Directives.[129]

The size of the databases involved are large. As of 2009, the Watchlist had 400,000 people on it, most of which were not U.S. citizens. The No Fly list had 3,400 people, of which 170 were U.S. persons. It has been reported that TIDE had around 570,000 around this time, but has grown significantly since then. After the Boston bombings of 2013 Reuters reported that TIDE had roughly 870,000 individuals listed. It is unclear how large the Watchlist has become.

We also have some indication of how active these databases are:

> During fiscal year (FY) 2009 [...] over 55,000 "encounters" [were processed] from federal, state, local, tribal, and territorial screening agencies and entities. Of those encounters, over 19,000 were a positive match to a watchlisted known or suspected terrorist. Most encounters provide valuable intelligence to the FBI case agent. Each provides information regarding the specific time, place, geographic location, and circumstances of the encounter with the watchlisted individual. During an encounter, additional biographic or biometric identifiers for the

[129] Ibid.

watchlisted individual might be discovered, new derogatory information could be obtained, or additional terrorist associates could be identified.[130]

The Watchlist is very much a product of international cooperation and inputs. As of September 2012, the U.S. has signed over 40 of these HSPD agreements with partner countries.[131] This is up from 34 in 2011, and 17 in 2009. According to the 2012 ISE Annual Report, "These agreements have enhanced current information already contained in the [Watchlist] as well as added new identities to the [TIDE master list] and the information provided downstream to our domestic and international screening partners."[132] The way the FBI describes the overall picture—the Watchlist and the HSPD-6 agreements that feed into it—very much fits the broader description of the global *i-veillance* assemblage presented in the dissertation. "The screening agencies throughout the world who attempt to ascertain if a person screened is watchlisted constitute a global network, dedicated to identifying, preventing, deterring, and disrupting potential terrorist activity."[133] The quote reflects the intelligence community's perspective on what is required to disrupt terrorism. Foreign partnerships that utilize information technology are important. Moreover, the quote suggests global coverage (even though the description of such coverage is a bit of aspirational hyperbole). It should also be noted that HSPD-6 partner countries are offered access to a particular chunk of data known as the "Foreign Partner Extract" of the Watchlist.[134]

---

[130] Ibid.
[131] Ramotowski 2012.
[132] ISE Program Manager 2012, 19.
[133] Healy 2009.
[134] US Diplomatic Cable 2008.

Other Agreements

According to the 2012 Information Sharing Environment (ISE) report to Congress, "89% of ISE agencies are integrating information from international partners into their watchlisting and screening process."[135] That means nearly 9/10th of the intelligence community takes in some information from foreign partners. While HSPD-6 agreements are the pillars of U.S.-led information sharing *i-veillance,* there are other information sharing agreements that plug into the same *i-veillance* infrastructure. Two major ones are Preventing and Combating Serious Crime (PCSC) Agreements and Passenger Name Record (PNR) Agreements. PCSC agreements give the U.S. a "platform for sharing criminal biometric and biographic information with foreign governments."[136] More specifically each party to the agreement has direct access to each other's fingerprint databases.[137] Countries that participate in the U.S. "Visa Waiver Program" are required to sign a PCSC agreements (or some equivalent).[138] As of March 2012, 36 countries had signed up for the VWP. 23 had met PCSC sharing requirements.[139]

PNR agreements involve the sharing of information that individuals give to their airlines or travel agencies prior to travel. This includes: name, address, telephone, and billing details. The exchange of PNR data occurs before departure and are used for screening. The data is useful beyond the immediate screening function. The Department of Homeland Security stores PNR data for up to 15 years.[140] As mentioned in Chapter 2 the storage function of surveillance is very important. It allows states to develop a record

---

[135] ISE Program Manager 2012.
[136] Ibid., 19.
[137] Heyman 2011.
[138] Gambler and Courts 2012, 6.
[139] 24 of these had signed HSPD-6 agreements. All 36 had entered into agreements to share information on Lost and Stolen Passports. Ibid.
[140] This is according to the "System of Records Notice" for the Department of Homeland Security's "Automated Targeting System" which uses PNR data. See the Federal Register Volume 77, Number 99 (Tuesday, May 22, 2012), Page 30302

of an individuals' behavior to better track their lives in space and time. According to the U.S., "PNR information has assisted CT officials in nearly every high-profile U.S. terrorist investigation in recent years."[141] According to a House of Representatives Report:

> In 2008 and 2009, PNR helped the United States identify individuals with potential ties to terrorism in more than 3,000 cases, including the November 2008 Mumbai attack plotter, David Headley, and the perpetrator of the failed May 2010 Times Square bombing, Faisal Shazad. In FY2010, approximately one quarter of those individuals denied entry to the United States for having ties to terrorism were initially identified through PNR data.[142]

In 2012 the U.S. and EU concluded a major PNR agreement, finally overcoming years of Europeans' privacy concerns.

Capacity Building

In addition to sharing information, a major pillar of U.S. counterterrorism policy is building up the capacity of "partner" nations to fight terrorism. Although it isn't obvious at first, I will argue that capacity building often works as a form of *i-veillance*. There are two main programs that deserve attention. The first is the Anti-Terrorism Assistance (ATA) program, the primary way in which the U.S. delivers counterterrorism capacity assistance to other countries. The State Department's FY14 budget justification sells the program thusly:

> ATA programs provide training, mentoring, advising, and equipment to help partner countries build or enhance a wide range of capabilities to detect, deter, and apprehend terrorists, including law enforcement investigations, border security, protection of critical targets, leadership and management of counterterrorism incidents, regional coordination and cooperation, critical incident management, and cyber security. ATA funding also supports the Regional Strategic Initiative, a global program that provides anti-terrorism training and equipment focused on addressing regional challenges.[143]

---

[141] ISE Program Manager 2012, 19.
[142] See House Report 112-272, Nov 4, 2011
[143] U.S. Department of State 2013, 161.

In 2012 nearly $200 million[144] was spent through ATA programs, and ATA funds currently serve 53 countries. Most of the training—over 90% in 2011—occurs overseas.[145] As of 2009, ATA "has trained and assisted more than 67,000 foreign security and law enforcement personnel from 154 countries."[146]

The Department of State Bureau of Diplomatic Security is responsible for assessing the capabilities of countries receiving ATA funds. Country assistance plans are created to outline objectives and the nature of the assistance granted (e.g. education, technology, etc.). ATA funding is then assessed against these plans.[147] In 2012 for instance, 18 "on-site visits assessed partner country critical counterterrorism capabilities and were used to both inform Country Assistance Plans and evaluate progress."[148]

ATA funding supports U.S. *i-veillance*, albeit in an indirect way. What is never stated in government texts is whether or not there is a quid-pro-quo in the sense that the U.S. provides the resources and training but receives information in return. This would be proof of a direct relationship to surveillance. But ATA (and similar) programs nevertheless support an infrastructure that is synaptic in two respects. First it fosters a liaison relationship through repeated contact with foreign counterparts. Second it fosters a reliance on the U.S.

According to the U.S. law that grants authority for anti-terrorism assistance, there are three purposes behind such activities:

> (1) to enhance the antiterrorism skills of friendly countries by providing training and equipment to deter and counter terrorism;

---

[144] U.S. Department Of State, Bureau of Counterterrorism 2013.
[145] U.S. Department of State, Bureau of Diplomatic Security 2012.
[146] U.S. Department of State, Bureau of Diplomatic Security 2009.
[147] The assessment of ATA funding has been problematic. See OIG Report Number AUD/MERO-12-29, April 2012 and GAO-08-336 for examples.
[148] U.S. Department Of State, Bureau of Counterterrorism 2013.

> (2) to strengthen the bilateral ties of the United States with friendly governments by offering concrete assistance in this area of great mutual concern; and
>
> (3) to increase respect for human rights by sharing with foreign civil authorities modern, humane, and effective antiterrorism techniques.[149]

As an example of the second objective above a 2012 Inspector General (IG) report suggests ATA has fostered relationships in counterterrorism. The IG interviewed Department of State Regional Security Offices (RSOs) to assess the effectiveness of ATA funds. RSOs represent Diplomatic Security and are present in all U.S. embassies abroad. Among other things they serve as the embassy's law enforcement liaison to the host state. With the caveat that there is no clear (quantitative?) evidence to tie the following anecdotes to ATA, here is what the IG reported:

> [Several RSOs] stated that ATA training had strengthened bilateral ties between United States and partner countries. They further stated that the ATA program had been a factor in improved relations and coordination between RSOs at U.S. embassies and local law enforcement entities during recent terror attacks in several countries. For example, RSOs in Yemen stated that during the 2008 attacks on Embassy Sana'a, when embassy guards fled, the local Yemeni police force arrived to guard the embassy. The RSO in New Delhi, India, said that after the 2008 Mumbai terror attacks in which six Americans were killed, relations with the Mumbai police facilitated examination of the crime scene by the Federal Bureau of Investigation. The RSO in Algiers stated that the Algerian police had provided information on a dozen terrorist attacks and that the information had helped him make the embassy more secure.[150]

The second example of *i-veillance* through capacity building is the provision of technology that enables partner countries to better conduct surveillance themselves. An example of this is Terrorist Interdiction Program/Personal Identification, Secure Comparison, & Evaluation System (TIP/PISCES) program. TIP/PISCES is a watch-listing system meant to assist other countries with border security. The program "provides computerized screening systems, periodic hardware and software upgrades,

[149] 22 USC Part VIII
[150] U.S. Department of State and the Office of Inspector General 2012.

and technical assistance and training to partner nations that enable immigration and border control officials to quickly identify suspect persons attempting to enter or leave their countries."[151] Through April 2012, the system was working at 184 ports of entry across 18 states. 53 of these across 11 states had biometric capabilities.[152]

Here the role played in *i-veillance* is clearer. In a 2011 "Annual Report on Assistance Related to International Terrorism" the State Department writes that U.S. "agreements for providing this equipment and training included provisions for sharing information gathered at borders and other international POEs [ports of entry]."[153] The amount of information being shared in this way might be tremendous. In 2012 "TIP/PISCES processed an estimated 250,000 travelers every day."[154] This means the U.S. had access to details of the identity and movement of 250,000 people travelling abroad. Future plans include "customized interfaces with local and international databases, as well as deployment of portable PISCES installations for remote locations lacking infrastructure."[155] And similar to ATA funding, TIP/PISCES establishes a link between countries through practice via ongoing funding and training for these systems.

The Global Governance of Surveillance

Governance can be defined as "the processes and institutions, both formal and informal, that guide and restrain the collective activities of a group."[156] "Whereas government suggests activities that are backed by formal authority, by police powers to insure the implementation of [...] policies, [...] governance refers to activities backed by shared goals that may or may not derive from legal and formally prescribed

---

[151] U.S. Department of State 2013.
[152] U.S. Department Of State, Bureau of Counterterrorism 2013.
[153] U.S. Department Of State, Bureau of Counterterrorism 2012.
[154] U.S. Department Of State, Bureau of Counterterrorism 2013.
[155] U.S. Department of State 2013.
[156] Keohane and Nye 2000, 12; cited in Kahler and Lake 2003, 7.

responsibilities and that do not necessarily rely on police powers."[157] This section highlights some of the most significant ways in which states are working together on the global governance of individuals through mechanisms of surveillance.

Table 4. Other counterterrorism programs with major U.S. involvement	
Program	**Explicit Role**
Trans-Sahara Counter-terrorism Partnership (TSCTP)	Capacity Building
Partnership for Regional East African Counter Terrorism (PREACT)	Capacity Building
West Africa Regional Initiative (WARSI)	Capacity Building
APEC Counter-Terrorism Task Force	Capacity Building and Information Sharing
Counterterrorism Finance Training (CTF)	Capacity Building
Caribbean Basin Security Initiative	Capacity Building and Information Sharing
International Law Enforcement Academies	Law Enforcement Training
G8 Lyon/Roma Group	Best Practices / Information Sharing

The United Nations

Although the United Nations does not itself conduct surveillance it has passed significant Security Council Resolutions which have shaped international counterterrorism practices, including surveillance.[158] Resolutions 1267 and 1373, in particular have effectively mandated that states maintain and monitor a list of sanctioned individuals related to terrorism and that states share information with one another. Accordingly, states might be assessed against certain norms and metrics for

[157] Rosenau and Czempiel 1992, 4.
[158] Look at all UN CT related laws: http://www.un.org/en/sc/ctc/laws.html

how well their counterterrorism policies match up. The UN itself monitors state compliance with both resolutions. In addition to motivating specific policies, the UN activity has helped reproduce a certain way of doing the business of counterterrorism. The general template is that states ought to develop capacity that respects certain liberal norms but cracks down on terrorism and shares relevant information with foreign partners. The latter suggests that terrorism is a community problem, as does the very fact that the UN has tasked itself to address terrorism.

Both Resolutions 1267 and 1373 were Security Council resolutions passed under Chapter VII of the UN Charter and reflect substantial moves in international law to fight terrorism. The first, UNSCR 1267 was passed in 1999 and requires states to apply travel bans and asset freezes to the Taliban. It was later modified to include individuals associated with al Qaeda. The 1267-related resolutions require states to impose assets freezes, travel bans and arms embargos to individuals and entities associated with the two groups. Moreover an "al-Qaida and Taliban Sanctions Committee" (aka a "1267 Committee") was created to determine which individuals and entities were deemed to be associated with the two organizations and to monitor states' compliance with the relevant resolutions.

The 1267 Committee was, and remains, controversial. Initially the criteria for adding someone to the sanction list was vague, and the "threshold established … ([for] being "associated with" Osama bin Laden or al Qaeda) was low and ambiguous."[159] The process has been amended,[160] but the fact remains that the listing and delisting process gives a surprising amount of power to the UN Committee over the fate of individuals, essentially implying that these individuals are beholden not to the nations under which

[159] Chesterman 2011, 186.
[160] See Resolutions 1526 & 1617

they have their citizenship, but rather to the international community. And the extent of the Committee's authority is strong. This is evident when "contrasted with the elaborate safe-guards incorporated within the ad hoc tribunals established for the former Yugoslavia and Rwanda [...] [which included] elaborate protections for the accused."[161]

While UNSCR 1267 serves as a 'listing system', Resolution 1373 (and 1540 which tackles proliferation issues) have been regarded as global legislation created by the Security Council.[162] 1373 is essentially about counterterrorism. The intent is to keep states from supporting terrorism and ensure that states take steps to suppress and stop terrorism. The mandatory provisions entail adopting domestic policies that criminalize terrorism, blocking and prohibiting terrorism financing and travel. This has led some to characterize 1373 as "legislation" signifying an important break in the practice of the UN Security Council. Szasz writes:

> In the past, [...] the Security Council has often required states to take certain actions, such as to implement sanctions against a particular state or to cooperate with an ad hoc tribunal, but these requirements always related to a particular situation or dispute and, even though not explicitly limited in time, would naturally expire when the issue in question and all its consequences were resolved. By contrast, as Resolution 1373, while inspired by the attacks of September 11, 2001, is not specifically related to these (though they are mentioned in the preamble) and lacks any explicit or implicit time limitation, a significant portion of the resolution can be said to establish new binding rules of international law-rather than mere commands relating to a particular situation—and, moreover, even creates a mechanism for monitoring compliance with them.[163]

Similarly Schepple writes:

> From a legal perspective, however, the Security Council framework for fighting terrorism was most stunning for requiring all member states to change domestic law in order to carry out the Security Council's requirements. [...] Resolution 1373 therefore started a new era for the Security Council, which now

[161] Chesterman 2011, 187.
[162] Powell 2012.
[163] Szasz 2002.

has the capacity to require all U.N. member states to change their domestic laws in parallel in order to tackle common threats.[164]

Noting that the democratic deficit critique of the UN is "more pointed in light of [these] recent quasi-legislative and quasi-judicial acts," Ian Johnstone has recommended making deliberative reforms (as an additional deficit salve to recommendations concerning reform of Security Council voting procedures or membership).[165]

Important for my purposes are the mandatory provisions in 1373 relating to sharing of information.[166] The resolution stipulates that states 'shall':

> *Take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information*
> *Afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings*

And implicit in the other requirements set forth by 1373, such as stopping terrorism finance and movement, is a requisite surveillance capability that enables the state to know these very things. Resolution 1373 has seen results. It created the Counter-Terrorism Committee to monitor states' compliance with its mandatory provisions, and member states are required to file progress reports to that end. As of 2010 "All 192 U.N. member states filed at least one report with the Security Council's Counter-Terrorism Committee (CTC), a subsidiary body that was created to monitor and enforce compliance with Resolution 1373. [...] By August 2006, 107 countries had filed four reports, and 42 had filed five."[167]

---

[164] Scheppele 2010, 440; See also Roach et al. 2012, 4.
[165] Johnstone 2008.
[166] United Nations Security Council 2001.
[167] Scheppele 2010, 442.

Other International Organizations

There are three other international organizations that deserve special mention—INTERPOL, the Financial Action Task Force, and The Global Counterterrorism Forum. The former two organizations are *the* major institutions that facilitate international law enforcement and anti-money laundering initiatives. The latter CT Forum is reviewed here because it is one of the few new institutions (created *de novo)* with major buy-in from great and secondary powers and therefore offers a possible glimpse of future CT global governance.

The International Criminal Police Organization was founded in 1923 by police officials for the purpose of exchanging best practices, establishing standards, and sharing information. After a rough spell during WWII the organization had to rebuild itself. In 1949 it was granted consultative status with the UN, and after adopting a new constitution in 1956 the organization changed its name to the International Criminal Police Organization-INTERPOL. Today it is known simply as INTERPOL. In 1971 it was recognized formally as an intergovernmental organization.[168]

There are two main features of INTERPOL that facilitate *i-veillance*. The first is establishment of National Central Bureaus (NCBs) in member states. Each member state has an NCB that serve as the contact point and link to INTERPOL's other members. NCBs are the foundation of INTERPOL's cooperative work. Each NCB can also query INTERPOL databases and, importantly, provide data to these databases for other member countries NCBs to use. As such NCBs act as sensors for the broader surveillance network composed by INTERPOL.

---

[168] For an IR take on how INTERPOL has changed over time as an IO see: Barnett and Coleman 2005.

The second role that INTERPOL plays in *i-veillance* is providing the data and databases referred to above.[169] INTERPOL has databases that cover nominal data (records on criminals and missing persons), fingerprints and DNA profiles, notices concerning wanted or missing persons (among other things), and more. To access this data INTERPOL has developed I-24/7 an IT system installed at all 190 NCBs connecting users to each other as well as to INTERPOL's databases. "Authorized users can search and cross-check data in a matter of seconds, with direct access to databases on suspected criminals or wanted persons, stolen and lost travel documents, stolen motor vehicles, fingerprints, DNA profiles, stolen administrative documents and stolen works of art."[170] INTERPOL regards the system as "the foundation of information exchange between the world's police."[171]

Both features of INTERPOL contribute to *i-veillance*. On the one hand we have cooperative efforts fostered through technology and through face-to-face relationships. On the other hand we have the storage and sharing of mass amounts of data on individuals.

The Financial Action Task Force (FATF) works "to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system."[172] The FATF promulgates standards for member states to adopt and monitors whether or not those standards are in fact being adopted.[173] Each

---

[169] Enders and Sandler 2011 look at the reasons why some countries don't adopt one of INTERPOL's database systems.
[170] INTERPOL 2014.
[171] Ibid.
[172] The Financial Action Task Force n.d.
[173] Other regional groups perform a similar function, for instance the Middle East and North Africa Financial Action Task Force and the Asia/Pacific Group on Money Laundering

member state has a Financial Intelligence Unit,[174] a central agency in a state responsible for "receiving, analyzing, and disseminating" certain financial information (reported by financial institutions) pertaining to criminal, money laundering and terrorism financing. FIUs are essential for each state in realizing FATF standards (the U.S. FIU is known as FINCEN). An IMF report on FIUs explains: "it is useful to consider its core functions as generating a continuous flow of information. Reporting entities and other FIUs provide information to the FIU, which, in turn, analyzes this information and passes the results of its analysis along to investigators and prosecutors, as well as other FIUs."[175] FIUs in essence form a network among nations to communicate suspicious and known illicit activity committed by individuals. In this case state infrastructures actually make contact with one another through information systems.

Finally, the Global Counterterrorism Forum (GCTF) is an international organization set up in 2011 to share expertise, best practices, and resources for counterterrorism strategies. Its current agenda focuses on three areas: "countering violent extremism,"[176] developing effective rule of law-based CT, and general CT capacity building. The GCTF is independent from the UN, but it is clear that former draws from the latter (for example Resolution 1373) in its mission. According to its founding political document, "We fully support the central role of the United Nations and the importance of full, comprehensive, and balanced implementation of the UN Global Counter-Terrorism Strategy and the UN counterterrorism framework more broadly."[177] Because the GCTF is new there hasn't been much activity from it, at least not much that has been

---

[174] These exist as a part of the Egmont Group, and not by FATF mandate. The Egmont Group itself could be listed along side of the FATF as part of the global governance of *i-veillance*

[175] Forget, International Monetary Fund, and World Bank 2004.

[176] It is hard to find a straightforward definition of 'Countering Violent Extremism,' but it seems to focus on 'the need to prevent individuals from starting down the path toward radicalization, the embrace of violence, and support for terrorism, as well as to divert those already on that path before they are fully committed and mobilized.' See remarks by Benjamin 2012.

[177] The Global Counterterrorism Forum 2011.

reported. Its goal in enhancing global cooperation on counterterrorism, however, is clear. The goal of capacity building echoes the efforts of the U.S. mentioned earlier. It remains to be seen whether or not this develops into an infrastructure supporting *i-veillance*.

Legal Assistance Treaties

Legal assistance treaties help states investigate crimes of transnational scope by facilitating the exchange of evidence and testimony across state jurisdictions. Historically in order to obtain legal assistance across borders, a court in the requesting state would send a "letter rogatory" to a court in the state which has the sought after information. Legal assistance treaties help to standardize and routinize assistance by stipulating the conditions under which assistance can be pursued, the authorities involved, the procedures to be followed, etc. Regional legal assistance treaties exist in the EU, as well as the OAS and ASEAN.

The Council of Europe's 1959 European Convention on Mutual Assistance in Criminal Matters was a major step in the international adoption of such instruments. The EU now has many vehicles that relate to information sharing in criminal and terrorism investigations. For instance, the Schengen Convention Provisions on Police and Judicial Co-Operation specifies conditions under which EU member states can conduct surveillance on people in another member's territory.[178] Article 5 of the EU Council Decision Establishing Europol describes the first of Europol's six "principal tasks" as: "to collect, store, process, analyse and exchange information and intelligence." Europol has a dedicated "Europol Information System" that facilitates this task.[179] Moreover, a later Council Decision stated that "Each Member State shall designate a

[178] Article 40
[179] (see articles 11-14)

specialized service within its police services or other law enforcement authorities, which, in accordance with national law, will have access to and collect all relevant information concerning and resulting from criminal investigations conducted by its law enforcement authorities with respect to terrorist offences and send it to Europol."[180] The Treaty of Prum (2005) went further to facilitate the exchange of DNA profiles and fingerprint data.[181]

The U.S. has developed its own approach in creating bilateral Mutual Legal Assistance Treaties (MLATs). Today the U.S. has an MLAT with 64 states, including the EU (signed in 2003, in force by 2008). Different MLATs choose to focus on different types of assistance. Language from the UN's model legal assistance treaty gives examples of what is involved.

> Mutual assistance to be afforded in accordance with the present Treaty may include:
>
> (a) Taking evidence or statements from persons;
> (b) Assisting in the availability of detained persons or others to give evidence or assist in investigations;
> (c) Effecting service of judicial documents;
> (d) Executing searches and seizures;
> (e) Examining objects and sites;
> (f) Providing information and evidentiary items;
> (g) Providing originals or certified copies of relevant documents and records, including bank, financial, corporate or business records

In terms of *i-veillance,* legal assistance instruments not only grease the wheels of information sharing on individuals, but make such assistance mandatory.

---

[180] 2005671/JHA Article 2
[181] See also EU Council Decision 2008/615/JHA and the EU Council Framework Decision 2006/960/JHA, and the Schengen Information System 2.

Summary

This chapter has reviewed some enabling and facilitating conditions behind *i-veillance*. The U.S. relies on information sharing arrangements such as HSPD-6 agreements with other states with a specific (but not exclusive) focus on watchlist data and screening. I also argued that the U.S. helps other states build their capacity to combat terrorism. This capacity building assistance takes the form of training and the provision of resources and technology. The upshot for *i-veillance* in information sharing arrangements is relatively straightforward. U.S. and partner countries share specific information on individuals. The upshot from capacity building efforts is less clear, but I argued that they perform an *i-veillance* function by creating conditions that favor surveillance—liaison relationships and relationships of dependency. That being said, some capacity building efforts (TIP/PISCES) more explicitly give the U.S. access to the travel information of foreigners.

I briefly covered two UN Security Council Resolutions that mandate certain actions by member states. Resolution 1267 forces states to take action against a specific UN list of terrorists. Resolution 1373 mandates that states adopt specific anti-terrorism policies, and this includes a mandate to share information and cooperate with other states' law enforcement agencies. International organizations like INTERPOL and FAFT/FIUs and legal assistance treaties further facilitate the sharing of individuals' personal information.

Any one of these examples taken in isolation might seem underwhelming. But taken as a whole these arrangements either explicitly call for active information sharing or require states to share information under specific circumstances. If state X knows of a bad guy about to harm state Y (or of some illicit financial transactions), X should notify Y

either through liaison relationships or data networks fostered by the arrangements listed above. The resulting picture suggests an *i-veillance* network.

The mode of each arrangement is also telling. Aside from the bi-lateral information sharing agreements, all the other arrangements make use of previously existing institutions or programs to achieve some gain in *i-veillance* capacity. Capacity building, for instance, was not invented to support surveillance. Rather, surveillance capacity has been added to some projects. Likewise, the UN, INTERPOL, and FAFT are all institutions that preceded the more contemporary lust for information. These institutions reflect emerging global governance to enhance surveillance. This, I want to suggest, enables states to conduct *i-veillance* quietly and unobtrusively. Anarchy and sovereignty create conditions that are unfavorable for any one state wishing to gain routine access to the information of another state's citizens. Working through existing institutions and established practices finesses the problem.

Chapter 4: Databased Sensors

Introduction

Since the advent of the internet, an increasing amount of surveillance focuses on data that flows through networks and gets stored in databases connected to those networks. For the analysis that follows, I refer to sensors that capture this data as "databas*ed*" sensors.

Surveilling data in transit (i.e. between one user and another) is more the purview of intelligence agencies and, therefore, secret. In 2013 and 2014 a slew of disclosures about the U.S. National Security Agency (NSA) shed some light on this type of *i-veillance*. However, the details have been slim and often technical. I will address the NSA activity briefly below, but the focus of this chapter is on databases and the data they store.

Databases are the predominant means of information storage in the digital age. As such they play a crucial role in nearly all aspects of surveillance. Databases are orders of magnitude larger and more accessible than file systems of the past. Databases are increasingly a part of modern life; personal details of all sorts are stored in databases, often without people's awareness.

Databases enable surveillance in simple and complex ways. Perhaps most straightforwardly, data can be entered and retrieved later for analysis or comparison to other information at hand (e.g. matching an ID card presented by a person against ID numbers in an associated database). On the more complex end of surveillance practices,

the accumulation of information in databases enable analysis on sets of data. Computer programs can churn through mass amounts of data to look for novel information, hidden relationships between data, and specific patterns.

Databased *i-veillance* can target one of two types of data generated by individuals. On the one hand there is data that individuals believe is not directly accessible by the state, at least not without some judicial process. Consider, for example, emails or documents that an individual has chosen to store on the private servers of companies like Google. On the other hand there is data that is part of government-dedicated systems and data collection requirements. For instance, the U.S. keeps track of foreign persons as they move through ports of entry and exit. As another example, the U.S. government collects tax information to determine a variety of obligations and benefits for its citizens.

Sometimes states share with one another data or even access to databases themselves. The sharing of data might be reciprocal or unilateral. Likewise states might have joint or limited access to databases. As one might expect, much depends on the sensitivity (or, perhaps the strategic value) of the data or databases in question.

Chapter Overview

The chapter begins with a survey of major databased sensors used by the U.S. and its partners. It then drills down in a case study of U.S. provided databased *i-veillance* for countries in the Caribbean. Throughout we see states pursuing information sharing as a means to enhance security; throughout we see concerns over data control and data privacy. As might be expected there is variation in the visibility of cooperative efforts. After all, databased *i-veillance* is a security practice that traffics in the information of the citizens of other states.

Perhaps most interesting are the variegated strategies of information sharing. Contrary to *prima facie* expectations, it is not simply the case that a state conducts surveillance only when it is vacuuming in data. One of the major takeaways from this chapter is that a state can achieve its *i-veillance* goals by pushing data out to other countries. Similarly, a state can help another state conduct *i-veillance* by providing it with the technology—stripped of data—to conduct *i-veillance*. If a donor state is confident of how the technology will be used, this type of capacity building can be a boon to its *i-veillance* efforts.

To preview one example, the U.S. Department of State has helped other countries establish border control systems to check travelers against watchlists. While it is unclear to what extent the systems use data provided by the U.S., the systems still check for individuals whom the U.S. deems unsavory (otherwise the U.S. wouldn't provide the systems in the first place). According to the U.S., the systems make roughly 250,000 checks per day. If only 1 in 100,000 travelers raise a flag, there would be over 900 matches every year. Through this effort the U.S. has effectively delegated *i-veillance* abroad.

A Survey of Existing Databased Sensors

Governments maintain large troves of data for various reasons. The collection and databases reviewed below are chosen based on their significance in conducting surveillance for security purposes. All the programs are led by the U.S. They are broken up by government department.

The Department of Defense: i-veillance *for Military Operations*

The U.S. Department of Defense (DOD) runs the Defense Information Systems Network that provides communication and information exchange capabilities for the U.S. military and its partners. There are various subnetworks that limit information

exchange based on whether the information is: Sensitive But Unclassified; Secret; or Top Secret/Sensitive Compartmented Information.

SIPRNET—the Secret Internet Protocol Router Network—is the DOD's network that contains and traffics classified data relevant to U.S. military operations. It also contains diplomatic cables (this is where Chelsea Manning downloaded cables before releasing them to WikiLeaks). It is arguably the most important information network used by DOD.

From public documents it is clear that some foreign countries and their nationals can be granted access to SIPRNET. For instance, Australia, Canada, and the UK receive a special call out in an instructional document explaining how to insure information security.[182] It is unclear when and to what extent partner countries have been granted access. SIPRNET was created in 1991. The earliest example of foreign access I can find dates back to 2002 and was connected to Operation Iraqi Freedom. Australian and British counterparts had some access, but not the Canadians.[183]

More routine access to some data *may* be occurring today but foreign partners cannot view any information marked NOFORN (not releasable to foreign nationals). According to reporting by *US News and World Report,* in 2006 the head of the CIA, Michael Hayden, pushed to extend SIPRNET access to key allies. "For the first time, Australian, British, and Canadian officials had immediate access to video feeds from unmanned Predator drones over Afghanistan and other real-time intelligence that allowed them to better coordinate search-and-rescue operations in Iraq."[184] But according to one source, "as of 2009 the British still do not have direct access to

---

[182] Chairman of the Joint Chiefs of Staff 2011.
[183] Mitchell 2009, 58 This was just the earliest example I stumbled upon. I wouldn't be surprised if there were earlier examples.
[184] Kaplan and Whitelaw 2006.

SIPRNET."[185] Access to SIPRNET may be mediated by other terminals and information networks not directly plugged into SIPRNET. For example, SIPRNET feeds multiple information exchange systems (known as CENTRIXS) which facilitate information sharing between the U.S. and its allies and coalition partners involved in counterterrorism operations, as well as the wars in Iraq and Afghanistan.[186]

Viewed as an *i-veillance* tool, SIPRNET is a network of databased sensors. Not only is it a source of information for the U.S. by the U.S., but also a repository where foreign partners can send information. This makes SIPRNET not just a tool for information sharing within the DOD, but also a surveillance tool for the U.S. military. As other countries upload information concerning individuals (terrorists and insurgents) into SIPRNET, it is U.S. databases that benefit. The U.S. limits what foreign partners can see on the network, but encourages partners to add data. In 2002 an Australian liaison officer noted that it is easier for the foreign partners to send information to SIPRNET than it was to receive information from it.[187]

It may be argued that SIPRNET is not a good example of a surveillance instrument because it is a military network used for operations. This might be true insofar as the network informs more conventional uses of military power. However, the network guides more individuated action against suspected and known terrorists. In practice, therefore, SIPRNET is both a tool to gather information on enemy forces (which is not the type of surveillance that concerns me) and a network of databased sensors surveilling individual actors.

---

[185] Farrell, Terry, and Frans 2010, 38.
[186] The U.S. military maintains a larger portfolio of foreign information sharing efforts known as 'MultiNational Information Sharing' (MNIS). See the following presentations for more information: Pontius 2011; Defense Information Systems Agency 2012.
[187] Mitchell 2009, 60.

A similar network—Joint Worldwide Intelligence Communications System (JWICS)—is supported by the DOD's Defense Intelligence Agency to manage the more tightly controlled Top Secret/Sensitive Compartmented Information. I have not found any evidence suggesting that foreign partners have access to JWICS.

The Department of State: Exporting Border Control Systems

The U.S. Department of State is very active in counterterrorism efforts. One program—the Terrorist Interdiction Program—assists other countries with border controls by collecting and analyzing data on travelers. To support the program the U.S. provides a software application known as PISCES[188] "which provides border control officials at these transit points with information that allows them to identify and detain or track individuals of interest."[189]

The system is operational at 184 ports of entry in 18 countries, some of which have biometric capabilities. The participating countries are considered by the U.S. as suffering from a higher risk of terrorist transit and lacking the infrastructure to address that problem. The countries are: Afghanistan, Cambodia, Cote D'Ivoire, Djibouti, Ethiopia, Ghana, Iraq, Kenya, Kosovo, Macedonia, Malta, Pakistan, Tanzania, Thailand, Uganda, Yemen, Zambia, and Niger. In 2012, the system "processed an estimated 250,000 travelers every day."[190] Installation, training and maintenance is paid for and run by the U.S. The U.S. also makes at least one check-up visit every year.

It is unclear whether or not the U.S. has direct access to the data that gets entered into PISCES systems worldwide. PISCES was once deployed in Pakistan, but the country recently considered scrapping the system partially out of fear that U.S. had direct access to the data. However, both Pakistani and U.S. officials denied that this was true. In 2011

[188] Personal Identification Secure Comparison and Evaluation System. The whole program is referred to as TIP/PISCES
[189] U.S. Department Of State, Bureau of Public Affairs 2002.
[190] U.S. Department Of State, Bureau of Counterterrorism 2013.

a former Pakistani Inteior Minister said that the data "was never available to them [the US] and was solely for the FIA's [Pakistan's FBI] use."[191] A representative from the U.S. embassy in Islamabad echoed that saying, "[t]here is no one at the Embassy who runs the TIP/PISCES programme. The Department of State provides support from Washington but the programme here is run by the interior ministry."[192] After a similar concern was raised in Malta, the U.S. embassy made a similar statement.

> PISCES systems are not interconnected. Each is a standalone system in the country where it has been installed to add to that nation's capacity to protect its national security. Monitoring of PISCES data is carried out by the Government of Malta. None of this data has been shared with the USG.[193]

While the U.S. might not have a direct line in or out of these systems, there are two ways in which the system serves an *i-veillance* function. First, if the U.S. wants information regarding specific individuals or travel patterns, it can make a request.[194] Similarly during check-up visits, the U.S. can make inquiries about data collection and analysis conducted by the host country.

Second, the U.S. *provides* data to the PISCES systems to facilitate checks that would benefit U.S. interests. A 2003 Congressional Research Service report describing U.S.-Pakistani counterterror cooperation states that the PISCES "software is said to make real-time comparisons of photographs and other personal details with the F.B.I. database in order to track the movements of Islamic militants."[195] In addition, according to a 2007 Department of State report, "TIP provided photos and travel history to

---

[191] Imtiaz 2011.
[192] Ibid.
[193] Vella 2004.
[194] Imtiaz 2011.
[195] Kronstadt 2003, 10.

Pakistan of three of the four July 7, 2005 London Metro bombers and hundreds of travelers have been interdicted in Pakistan on suspicion of using stolen passports."[196]

It is clear that PISCES systems can pull, or perhaps duplicate data, from other databases. Yet another Department of State report mentions "U.S. and host nation requests for customized interfaces with local and international databases[…] while ensuring that the PISCES system maintains standards in accordance with international norms."[197] Also, at least some PISCES systems are mentioned as having INTERPOL and Schengen II interfaces.[198] Access to the Schengen system is likely limited to Schengen members which also run PISCES systems. Installation of an INTERPOL interface, however, should not be limited. For example a Pakistani government website describing PISCES mentions using INTERPOL data as well as "linking" to other countries' visa issuance systems.[199]

Regardless of whether the U.S. gets direct access to PISCES data, the systems nevertheless play a surveillance role for the U.S. The fact that the systems can be populated with data from U.S. or other international databases means that travelers' identities are checked against those data entries. To be clear, the data being used for watchlisting could be anything from most-wanted-terrorists to fraudulent document alerts. Nevertheless, at 250,000 checks per day this is a significant achievement for the U.S. If only 1/10th of one percent of those travelers raise a flag, there would be over 90,000 matches every year. The U.S. has effectively delegated *i-veillance* activity through the PISCES program.

---

196 U.S. Department of State 2007, 63.
197 U.S. Department of State 2013, 161.
198 Ibid., 216–7.
199 See Pakistan's Federal Investigation Agency site on PISCES. http://www.fia.gov.pk/prj_pisces.htm

The Department of Homeland Security: Sharing Terrorism Information

One important set of exchanges—HSPD-6 agreements—was already mentioned in Chapter 3. To recap, the U.S. has signed bilateral agreements with over 40 countries to enable the exchange of terrorist watchlist information. The way the FBI describes the overall picture—the Watchlist and the HSPD-6 agreements that feed into it—very much fits the broader description of the global *i-veillance* assemblage presented in the dissertation. "The screening agencies throughout the world who attempt to ascertain if a person screened is watchlisted constitute a global network, dedicated to identifying, preventing, deterring, and disrupting potential terrorist activity."[200]

HSPD-6 agreements are not without controversy. Each agreement is uniquely tailored, and no text has been made public. Negotiations between the U.S. and Sweden were partially exposed in diplomatic cables released by Wikileaks. The Swedish government was hesitant in making commitments to exchanging information due to a recent domestic (to Sweden) issue. The U.S. response demonstrated flexibility, albeit limited, in meeting Sweden's concerns. We know that Sweden ultimately signed an agreement. The cables suggest that such agreements can be controversial and that the U.S. views the agreements as important enough to flex on the demands.

While HSPD agreements may enable the most important unclassified information sharing the U.S. engages in, there are other sharing arrangements in which international partners are granted limited access to major U.S. department-level databases.

The U.S. Department of Homeland Security runs the Homeland Security Information Network (HSIN) to foster information sharing and collaboration for all

[200] Healy 2009.

partners involved in homeland security. HSIN focuses on "sensitive but unclassified" information.[201] Users include federal, state, and local governments, the private sector, and—importantly—international partners. Although there is not much information on the nature of international participation, nearly every description of the HSIN mentions it.[202] It is clear, however, that there is data provided by foreign governments, and foreign users have (limited) access to specific information. Interestingly DHS notes that "access for foreign nationals is normally a long term commitment."[203] This suggests that the countries which the U.S. partners with have a record of trust and cooperation.

DHS is also responsible for orchestrating "Preventing and Combating Serious Crime Agreements" with countries whose citizens do not require a visa for travel to the U.S. These agreements facilitate sharing biographic details, fingerprint data, and other biometric information about criminals. The U.S. has agreements with at least 37 countries.[204] Each agreement is unique. For example, the U.S. agreement with Switzerland seems to limit data exchange to a subset of "serious" crimes,[205] whereas the agreement with Japan gives the U.S. access to Japan's entire fingerprint database.[206]

A final information sharing arrangement facilitated by DHS is the (controversial) sharing of passenger name record (PNR) data between the European Union and the U.S.[207] The agreement (in force as of July 2012) requires air carriers flying from the EU to the US to "push" data entered by passengers in the reservation system to DHS for analysis prior to departure. The agreement also requires DHS to share relevant

---

[201] The Homeland Security Data Network (HSDN) circulates classified information (and is analogous to, and in fact links up with, DoD's SIPRNET). I cannot find any suggestion that foreign partners have access to HSDN.
[202] See any of the Privacy Impact Assessments for more details on how the data is managed.
[203] U.S. Department of Homeland Security, Director of Information Security Policy 2011.
[204] This number is based on the number of "visa waiver countries," each of which the U.S. requires sign a PCSC agreement.
[205] Swiss Federal Department of Foreign Affairs 2012.
[206] Ogata 2013.
[207] European Union and United States of America 2011.

information that results from the sharing of PNR data, and allows EU law enforcement agencies to make specific requests for relevant information as well.

The FBI: Sharing Law Enforcement Information

The FBI also shares information with its foreign partners. One of the most important domestic systems is the N-DEx information sharing network. N-DEx aggregates law enforcement information (concerning arrests, incarcerations, parole, etc) from local, state, tribal and federal records and performs additional analysis to find previously unknown relationships and information.

Some foreign law enforcement agencies are granted access as "limited system participants." Information is shared "bi-directionally" with these users.[208] Confirmed partner agencies include the Australian Federal Police, the New Zealand Police, the UK's Serious Organized Crime Agency, and INTERPOL. According to the N-DEx user manual, "Local, state, and tribal criminal justice agency data shall not be shareable with limited system participants."[209]

The N-DEx System interfaces with other FBI-run records systems which may contain data provided by foreign partners, showing yet another avenue of cooperative *i-veillance*. One important system is the National Crime Information Center (NCIC) which maintains files (i.e. sets of data) on important types of property and persons (e.g. stolen vehicles and individuals being watched by the Secret Service)—21 files in all.[210] One of those files is the "Foreign Fugitive File" on individuals wanted in other countries for crimes that would be considered a felony in the U.S. Only INTERPOL and Canada's Mounted Police can enter records to this file.

---

[208] U.S. FBI, Criminal Justice Information Services Division 2013, 14.
[209] Ibid.
[210] For a helpful overview of FBI systems see: U.S. FBI, Criminal Justice Information Services Division 2010.

The NCIC maintains a file on known or suspected terrorists. This file is populated with data from the U.S. Terrorist Watch List, the main watchlisting dataset used by the U.S. Furthermore, this is the same watch list that gets shared (to different extents) with foreign partners.

The FBI also maintains systems that other states might query but not push data to. For instance other countries can make requests against the FBI's fingerprint database (the Integrated Automated Fingerprint Identification System). For such activity the U.S. is not necessarily taking in new information, and therefore the *i-veillance* function might not be clear. However this type of information sharing helps others conduct surveillance on people of interest to the U.S. The result is an extension of U.S. *i-veillance* efforts.

NSA Programs

The dissertation cannot focus on NSA programs in too much depth. The information is still spotty and doubtless incomplete. It is difficult enough researching the other practices found in this volume. Nevertheless, a brief highlight of some of the recent disclosures is helpful for a deeper appreciation of databased *i-veillance*.

The extent of NSA surveillance capabilities was recently glimpsed when *The Guardian* and *The Washington Post* newspapers disclosed details of two surveillance operations. The first is the collection of all Verizon cell phone metadata on calls made within a certain 90 day period. Metadata does not include the actual content of the call, but rather all the other information about that call: what numbers were dialed, when the call was made, how long it lasted, etc. The program is authorized by the Foreign Intelligence Court pursuant to measures in the U.S. Patriot Act.

The U.S. government received *all* such metadata from U.S. phone carriers and stored it in a database. The data could then be accessed if it was only targeting foreign persons suspected of being involved in terrorism. Nevertheless, information on U.S.

persons inevitably gets swept up in such searches and analysis. For instance information collection typically extends one or two degrees "hops" from the target to include who the target speaks to, and who those associates speak to. Congress has been signing off on such programs since 2007.

The other program came to light just a day after the previous revelation. Named "PRISM", the NSA reportedly has "direct" access to data held by major search engines and social networking sites—Microsoft, Google, Yahoo, Facebook and Apple included. Upon suspicion of foreign activity connected to terrorism the NSA can pull data on the relevant user's (and associates) search queries, pictures, emails, chats, and other stored data.

What is new about these revelation is (a) how sweeping the collection is and (b) how direct the access is (in the case of PRISM). For instance *The Guardian* reported: "The PRISM program allows the NSA [...] to obtain targeted communications without having to request them from the service providers and without having to obtain individual court orders. With this program, the NSA is able to reach directly into the servers of the participating companies and obtain both stored communications as well as perform real-time collection on targeted users."[211] PRISM data has been used heavily by the U.S. IC. Again, according to reporting, "When the NSA reviews a communication it believes merits further investigation, it issues what it calls a "report". According to the NSA, 'over 2,000 PRISM-based reports' are now issued every month. There were 24,005 in 2012, a 27% increase on the previous year."[212]

It is worth noting that surveillance by the NSA has significant consequences. While the metadata collection has only foiled a couple of plots in the U.S., other NSA

[211] Greenwald and MacAskill 2013b.
[212] Ibid.

surveillance contributes to the CIA's program of targeted killing. According to the Washington Post, the NSA uses an array of "cyber-espionage tools" which run the gamut from intercepting communications to actually taking remote control of laptops. NSA surveillance capabilities in the Af-Pak region are more focused. "[R]ecords indicate that the agency depends heavily on highly targeted network penetrations to gather information that wouldn't otherwise be trapped in surveillance nets that it has set at key Internet gateways."[213]

Case: CARICOM, Capacity Building, and *i-Veillance*

In spring of 2007 the World Cricket Cup was hosted by Caribbean states.[214] Before the event the United States, which itself made a failed bid for the 2007 competition, reached out to the Caribbean hosts with an offer to help them with security. The U.S. had concerns that the tournament would bring with it an increased risk of terrorism. After all, cricket is a popular game in Britain and its former colonies, including Pakistan.

With the tournament being held so close to the U.S. and given the anti-Americanism harbored by violent extremists from the "Af-Pak" region and elsewhere, the U.S. wanted to take extra steps to shore up security in the Caribbean. The result was a system monitoring ports of entry and enhanced information sharing among the U.S. and Caribbean states.

With the World Cricket Cup came discussions in 2006 about how to extend U.S. capabilities either directly or through proxy throughout the Caribbean. One might think that with the initial impetus of security cooperation—the World Cricket Cup—gone, that

---

[213] Miller, Tate, and Gellman 2013.
[214] For those that don't follow cricket, the West Indies cricket team or the 'Westies' is a very successful cricket team.

security affairs might revert back to the 2006 status quo. This did not happen. The security arrangements not only stuck but grew. Today the U.S. participates in the "Caribbean Security Basin Initiative" and has deepened information sharing and capacity building efforts in the region. Much of which reflects a deepening of *i-veillance*.

This case shows that *i-veillance* was not a one-off, stop-gap arrangement. Rather, the practices are geared toward managing the broader, chronic "threats" posed by individuals. The cooperation is a clear example of how joint surveillance enhances the resolution of U.S. and Caribbean states' security apparatuses. It also illustrates a more direct form of information sharing, a form in which the U.S. directly receives and analyzes the information of passengers flying into different states.

From Drugs to Terrorism

Prior to September 11, the U.S. and Caribbean countries worked together to disrupt drug trafficking. In April 2001, President Bush referred to the Caribbean as the United States' "third border." This appellation remains in use by both the U.S. and CARICOM states. At the same time he announced a "Third Border Initiative" which was to focus on "HIV/AIDS, disaster mitigation, and law enforcement."[215] After 9/11, terrorism would be added to this agenda.[216]

The 2007 Cricket World Cup (CWC) brought an opportunity for the U.S. to become deeply involved with the security of Caribbean countries. The CWC was co-hosted among ten different states in the Caribbean. Like all major sporting events, such as the Olympics and the (Soccer) World Cup, security for the CWC was a major concern. The disturbing events of the 1972 Munich Olympics in which Palestinian "Black September" members kidnapped and massacred 11 Israeli athletes is perhaps the most

[215] White House, Office of the Press Secretary 2001.
[216] Ereli and U.S. Department of State 2004.

vivid example of what can go wrong at a major world sporting event. The recent attacks on 9/11/2001 only heightened U.S. concerns about terrorism at the event occurring miles away from its territory. Setting the U.S. even more on edge was the added reality that the game of cricket attracts quite a following in Pakistan, and the CWC provided an opportunity for al Qaeda or like-minded groups to send individuals to the region.

At some point in 2006, the U.S. Department of Homeland Security (DHS) had the idea to assist Caribbean countries with their entry and exit security measures. A diplomatic cable covering a meeting between a U.S. delegation and Jamaica's Minister of National Security in late June 2006 explains some of the thinking behind potential security partnership. Randy Beardsworth, an Assistant Secretary at DHS, noted that security enhancements could target: "who is entering the region; the physical security of the match venues; and the response capabilities of the region," but the focus of the Caribbean partnership with the U.S. should be on "keeping the bad actors out of the region."[217]

The focus here is not on one specific individual, but on *all* individuals entering the region. Whereas remote sensing tends to be more targeted, this application of databased sensing is an example of collecting the "haystack" of data to look for possible "needles."

To keep the bad guys out, the U.S. settled on setting up an "Automated Passenger Information System" (APIS) for the Caribbean states. Typically APIS is a way of pre-screening passengers arriving to the U.S. Information is collected on incoming passengers. The information includes the details of the passenger's travel document (e.g. Passport) and destination information.[218] This data is then checked against U.S.

---

[217] US Diplomatic Cable 2006.
[218] U.S. Department of Homeland Security 2008, 5–7.

databases of suspicious or known terrorists, their supporters, or "high risk" individuals. The databases include those held by DHS and the larger data sets held by the U.S. National Counterterrorism Center (NCTC).[219]

The APIS system set up for CARICOM extends the ports of entry where the U.S. collects data. Prior to 2007 the U.S. required APIS data for passengers coming in to the U.S. After 2007 the U.S. was collecting and checking additional data on passengers coming into, not just the U.S., but the CARICOM region as well. The U.S. is receiving information from air carriers arriving in Caribbean countries (plus the Dominican Republic) in the *same way* in which the U.S. receives data from carriers flying into the U.S. Put differently, from the perspective of U.S. advance passenger data collection, Caribbean states are being treated as if they were part of the U.S. As with U.S. APIS, Caribbean APIS information would be checked against U.S. databases for hits, and that information would travel back down the chain to be actionable for U.S. and CARICOM officials.

According to a June 22 diplomatic cable, and confirmed by a later 'Memorandum of Intent', here is how APIS would work:

> The APIS model would involve air carriers to the region sending their APIS information to a CARICOM mainframe, which would be located in the U.S. "Hits" would be reviewed by Customs and Border Protection's National Targeting Center, and then passed to a CARICOM Operations Center. CARICOM Ops could then send the information to the appropriate regional airport authorities to ensure that pre-established actions will be taken. Likewise, the USG would place law enforcement officials at the CARICOM Ops center during the World Cup (and hopefully beyond).[220]

Note the language at the end suggesting the intent to keep the APIS system in place after the CWC. Not only would does the U.S. state it would like to "place law

[219] U.S. Department of Homeland Security 2013.
[220] US Diplomatic Cable 2006.

enforcement officials at the CARICOM Ops center during the World Cup (*and hopefully beyond*)", but according to the same cable the Jamaican National Security Minister "stated emphatically that this was a system that would be a legacy, continuing long after CWC."[221]

Months later, in October, the 14 member countries of the Caribbean Community and the U.S. signed a Memorandum of Intent (MOI) "on co-operation regarding the development of an advance passenger information system."[222] The "Scope of Collaboration" indicates that cooperation is "intended to continue after CWC 2007 for such period pursuant to such terms as determined by the Participants, as part of a long-term partnership."[223]

In addition to APIS, CARICOM worked on other cooperative arrangements to bolster security. The states created an "Intelligence Sharing Network and a Regional Intelligence Fusion Centre, to be jointly manned by CARICOM Member States, friendly third states and INTERPOL."[224]

The regional security legacy of the CWC is substantial. The first meeting of heads of CARICOM countries *after* the CWC stated that they:

> Agree to build on the security arrangements successfully implemented for Cricket World Cup 2007 [...]; Further agree to accelerate the process of intelligence-sharing and human resource development and to develop other relevant bilateral and multilateral security arrangements to supplement limited national resources; Resolve to develop regional law enforcement instruments which will facilitate a coordinated approach to the scourge of organised crime, international terrorism and financial crimes.[225]

---

[221] Ibid.
[222] U.S. Government and CARICOM 2006.
[223] Ibid.
[224] Carrington 2007.
[225] CARICOM Press Release 2007.

At that same event Trinidad and Tobago's head of state reportedly referred to security arrangements put in place during the Cricket Cup as the most important legacy of the event.

One of the most important institutions created after the CWC is the CARICOM Implementation Agency for Crime and Security (IMPACS) and its sub-agencies which manage information sharing (including APIS data) throughout the region and with foreign partners. CARICOM states now have the ability to ingest and analyze APIS data themselves.

The current U.S. role in their APIS system is nowhere made explicit, but circumstantial evidence suggest the U.S. still receives the data just as they did when the system was created. First, we have the above language from CARICOM officials saying they want to extend the system. In April 2008 CARICOM heads of government agreed to keep and expand on the APIS initiative.[226] (However, the document does not explicitly mention U.S. involvement.) Second, there are agreements in place to enable information sharing with the U.S. (though the content of the agreements are not public).[227] Specifically, "IMPACS and the JRCC [the specific agency responsible for APIS data] have co-operative arrangements with the United States for exchange of information."[228]

Third, the U.S. *continues* to contribute to the CARICOM APIS. The U.S. State Department explained in March 2013, "in the area of passenger screening, the United States is working to enhance the capacity of Caribbean nations to identify high risk travelers and execute coordinated interdiction operations utilizing the CARICOM

[226] CARICOM Secretariat 2008.
[227] Brownfield 2012.
[228] Stuart 2010.

Advance Passenger Information System."[229] U.S. officials also train their Caribbean counterparts on the system.[230] A more recent project focuses on Barbados.[231]

Finally, numerous British travel sites have a version of the following boiler plate:

> [A]dvance passenger data, required by and provided to CARICOM States for border security purposes, will be passed to the USA Department for Homeland Security for processing. The UK Information Commissioner's Office (ICO) has accepted that this will not breach the Data Protection Act but has advised carriers operating to CARICOM States to make passengers aware that personal information provided by them may be passed on for processing as above.[232]

To sum up, although there is no single official document in the public domain that says all CARICOM APIS data is routinely passed to the U.S. for analysis, I believe that the circumstantial evidence is conclusive.[233] And while I think the evidence is conclusive on its own, a contact at the Department of Homeland Security assures me this is the case.

It is also worth mentioning that Caribbean states would not be alone in sending APIS data to the U.S. In 2010 the U.S. and Panama signed a Memorandum of Understanding in which DHS would "collect and interpret" APIS data on flights in and out of Panama.[234]

The U.S. involvement with CARICOM border security has been very successful. Not only did the CWC go off without a problem, but the APIS work done in 2006 and 2007 remains in place. The evidence suggests the U.S. now has access to the passenger throughput of (at least) 16 Caribbean countries. In 2008CARICOM's APIS screened just

---

[229] Luna 2013.
[230] Sandrolini 2012.
[231] Luna 2013; Napolitano 2011.
[232] Monarch: http://www.monarch.co.uk/faq/holidays/making-a-booking/advance-passenger-information
Thompson: http://www.thomson.co.uk/editorial/legal/privacy-policy-popup.html
Avro Flights: http://www.avro.co.uk/FAQs/
[233] I think the definitive documents include a 2006 MOU between CARICOM and the U.S. for the initial sharing, and subsequent MOUs.
[234] U.S. Department of State 2011.

under 10 million passengers. This number increased slightly in subsequent years. From 2008 to 2011 the system had a rough average of 1250 hits (likely against CARICOM lists) each year.[235]

It is evident that there exist political risks with this cooperative effort. An early diplomatic cable acknowledged that the U.S. would only move forward if "regional governments would need the political will to share information, put in place appropriate legislation, and see the project through in perpetuity."[236]

"Sharing information" is singled out because it is a controversial practice (as the U.S.-EU PNR agreement reflects). Governments do not freely share data on their citizens or data that they have been entrusted with by other countries. The U.S. is acknowledging that this might be a barrier to moving forward. It turns out it wasn't.

However, two things remain to be explained. First, why is it excruciatingly difficult to find any official document that spells out the nature of the APIS information sharing that exists between the U.S. and CARICOM? We know that the U.S. received direct APIS feeds during the CWC. After the CWC we know information sharing happens, but the precise nature of it is not publicly stated. As argued above, I believe that the U.S. has the same access as it initially did in 2006.

The fact that official documentation is not public suggests an intentional decision to keep the matter out of the public record. If, as I believe to be the case, the U.S. has real time access to passenger data of all foreigners traveling in and out of the Caribbean, publicizing it will likely irritate two groups—citizens of CARICOM countries who might question the outsourcing of their states' security function and any foreigners who care intensely about privacy issues. I don't want to overstate the issue. Many countries

---

[235] CARICOM IMPACS 2013, 28.
[236] US Diplomatic Cable 2006.

require APIS data for passengers arriving in their respective ports of entry. But the U.S. is the only country that receives APIS data for passengers arriving in *other* countries.

The second unresolved question is, wouldn't other countries raise a stink knowing that anytime their citizens travel to the Caribbean their passenger data is going to the U.S. to check against watchlists? Some sources suggest that other countries have taken some interest. According to a 2007 CARICOM document, "Airlines operating out of Canada, the [UK], and Europe were particularly concerned over compliance with their national legislation and the effect the APIS, configured as proposed by the [U.S.] might have on their operations."[237] It further explained that Caribbean negotiations with the U.S. on APIS was to be put on hold "to ensure uniformity with the provisions of any US/EU [passenger data] Agreement."[238] This suggests that any agreement the U.S. was making with CARICOM would be compatible with other U.S. agreements.

One last indication that other countries have taken notice comes from language posted by some travel companies in the UK. What I referred to as "boiler plate" language cited above, suggests that the UK Information Commissioner's Office has looked into whether U.S. access to Caribbean passenger data "breach[es] the Data Protection Act." Concluding it doesn't, the same office has "advised carriers operating to CARICOM States to make passengers aware that personal information provided by them may be passed on" to the U.S.

Both the absence of a clear statement on data sharing and evidence of privacy/data management concerns by other countries illustrate the sensitivity surrounding the sharing of surveillance activity.

---

[237] CARICOM IMPACS 2007, 13.
[238] Ibid.

The Caribbean Basin Security Initiative

The cooperation in 2006 and 2007 formed the foundation for the more involved cooperative efforts of the U.S.-led Caribbean Basin Security Initiative (CBSI).[239] The CBSI was formally started in May 2010 with the purpose of bringing "all members of CARICOM and the DR together to jointly collaborate on regional security with the United States as a partner."[240]

As mentioned above, the U.S. has come to regard the Caribbean region as a 'third border'. If the Caribbean's geographical proximity makes it a *candidate* of concern, it is the perceived lack of the Caribbean states' counterterrorism (and counterdrug) capacity that elevates them to a primary hemispheric concern of the U.S. government. The Joint Caribbean-United States Framework for Security Cooperation Engagement sets the stage.

> The geographical location of the region between the major drug producing states and the consuming markets has increased the vulnerability of Caribbean states to the effects of the transnational illicit drug trade, associated crime and other forms of transnational organized crime. Further, as a region of mainly small territories, the Caribbean lacks the domestic capacity to address these security challenges. In addition, many Caribbean states face challenges from domestic issues related to poverty, high rates of unemployment, social inequality and marginalization, and inadequacies of their criminal justice systems.[241]

---

[239] According to Congressional testimony on Dec. 9, 2009 by Julissa Reynoso, "Work on CBSI began in earnest following unprecedented efforts by Caribbean countries, the United States and international partners to provide security for the 2007 Cricket World Cup

[240] State Department page on the CBSI. http://www.state.gov/p/wha/rt/cbsi/

[241] U.S. Department of State 2010c.

CBSI has two core functions.[242] The first is to build capacity. The CBSI "partnership" is "an ongoing collaboration that draws upon and helps develop the capacity of the Caribbean to address common and related challenges."[243] Document after document of the U.S. highlights this purpose of CBSI.[244]

The U.S. goal, however, is not to simply create indigenous capacity. Rather, the U.S. wants a capacity that leans on the U.S. into the future. The U.S.-Caribbean framework for the CBSI seeks to strengthen "the Caribbean Region's capacity to implement available United States security cooperation instruments and initiatives."[245] The goal is "the institutionalization of a [...] multi-level and regional approach to [...] security cooperation, with mechanisms established in both the Caribbean and in the United States."[246]

As I've argued before, capacity building is often more than just one country throwing money and expertise at another. It represents an ongoing *relationship*. Often this relationship is a means of surveillance. Through liaison presence abroad and provision of technology and expertise, the state providing assistance gains information channels it would otherwise lack. The capacity building aspect of CBSI is a clear example of this.

The second major purpose of the CBSI is to facilitate information sharing both within the region and between the Caribbean states and international partners. Information sharing—one way to enhance a country's surveillance capacity—is

---

[242] For examples of how the CBSI actually operates see the Country Reports section of any recent "International Narcotics Control Strategy Report" from the Dept. of State's "Bureau of International Narcotics and Law Enforcement Affairs."
[243] U.S. Department of State 2010b.
[244] See the May 2010 founding documents of the CBSI U.S. Department of State 2010c; The United States and CARICOM IMPACS 2010; U.S. Department of State 2010a; ibid. and joint declarations made yearly thereafter.
[245] U.S. Department of State 2010c.
[246] Ibid.

increasingly practice within CARICOM through IMPACS. Internationally, information on passenger data (APIS), cargo, ballistics, illicit financing, and fingerprint information is all shared to some extent.[247] CARICOM also works closely with INTERPOL.[248]

It is worth mentioning that outside the CBSI the U.S. works with Caribbean and other regional states to share maritime radar data.[249] Shared radar data amplifies the capability of all to track and interdict illicit activity. This is yet another example of increasing sensors to increase resolution.[250]

Summing up, U.S. data sharing in the Caribbean has not been a stop-gap security effort. The APIS arrangement developed for the Cricket World Cup remains, and related efforts have proliferated. Through APIS and the Caribbean Basin Security Initiative, the U.S. has effectively expanded the range of its own security apparatus to monitor whether potentially threatening individuals enter the region.

Conclusion

Databased *i-veillance* takes many forms. States can "snoop" on data being stored or actively transacted by individuals. Recently disclosed NSA programs targeting the internet communication of private citizens is an example. States can also create above-board (not-secret) data requirements and informations systems that individuals interface with. Examples of this include Social Security Numbers and border control

---

[247] The associated programs are: APIS, Advanced Cargo Information System (ACIS), the Regional Integrated Ballistic Information Network (RIBIN), the Caribbean Financial Action Task Force (CFATF), and the Advanced Fingerprint Information System (AFIS).

[248] INTERPOL 2009.

[249] The relevant programs are the Cooperating Nations Information Exchange System (CNIES) and the Cooperative Situational Information Integration system (CSII)

[250] For instance according to the U.S. official responsible for counternarcotics, 'CNIES terminals generally are in locations around the hemisphere. We have several in Mexico, for example, where we actually share radar tracks with the host government, so they can see where the ships and aircraft are coming as they leave South America.' Douglas 2007.

systems that ingest information from passports. A final form of databased i-veillance is the practice of information sharing between states.

The "sensors" assessed in this chapter primarily represent a combination of the latter two forms of *i-veillance*—creating systems and sharing data. This activity mirrors U.S. practice of capacity building and information sharing. The PISCES program, for instance provides other countries with technology and watchlist data to monitor flows of people through the recipient countries' ports of entry.

Analysis of the programs, PISCES and CARICOM APIS in particular, provide two important takeaways. First, the politics behind databased *i-veillance* are variegated. Putting aside secret surveillance practices (e.g. of the NSA), databased capacity building and information sharing are sensitive practices. With PISCES, for instance, we saw that countries were suspicious about U.S. capabilities and intent. With APIS we see what seems to be a deliberate omission of details of information sharing arrangements. With both we find sensitivity regarding the privacy of personal information of foreign citizens involved.

Second, the chapter demonstrates a variety of information sharing approaches. States can reciprocally share information or be party to an asymmetric information sharing arrangement. Also, there is a difference between sharing data, and sharing access to specific databases. The former represents a comparatively low-cost alternative in which one state can simply give another state a digital file. The latter is more complicated as it requires more attention to hardware, standardization of practices, and creating controls that restrict access (different databases are more or less sensitive).

With the U.S. PISCES program the U.S. provides hardware that enables partners to use their own watchlists which often incorporate watchlist information from other states and organizations (like INTERPOL). The program represents a strategy of pushing

capabilities and data out to partners in order to take advantage of their sensors. It demonstrates that a state (in this case the U.S.) does not need to operate its own system by its own users in order to conduct *i-veillance*. This point is critical.

The CARICOM case demonstrates more direct control, and resembles a form of trusteeship with respect to this particular exercise of *i-veillance*. The case made by the U.S. seems to be that weak states with porous borders so close to the U.S. requires a more hands-on approach.

In fact, both the U.S. and CARICOM countries expressed that U.S. assistance can benefit everyone. CARICOM countries were very excited about U.S. assistance, and from a strictly material perspective they benefited tremendously. Not only was their surveillance capabilities enhanced, but the of the Cricket World Cup had further spillover security benefits for CARICOM.

This points to one final takeaway. Surveillance has a way of spreading and linking-up with other efforts. The success of Cricket World Cup security cooperation (and APIS in particular) begat the Caribbean Basin Security Initiative. At the very least, there is fodder for justifying further cooperative efforts and connecting *i-veillance* activities together.

Chapter 5: Remote Sensors

Introduction

Remote sensors are the surveillance mechanisms states choose when direct access to a territory in which the targets live is a problem. "Access" is a function of both whether the host territory allows access (and to what extent) and whether or not the state conducting surveillance can operate a sensor in the target territory without notice.

Consider U.S. drone flights conducted in Pakistan. Why are they the sensor of choice? If Pakistan were a closer ally to the U.S. and its domestic security situation were much improved, the U.S. might actually work with and through Pakistan's intelligence and law enforcement agencies on the ground, in Pakistan. But the U.S. does not have this level of access. It does have some limited access to the air though. Pakistan has granted permission to the U.S. to conduct specific flights to conduct surveillance particularly in the Federally Administrated Tribal Regions. However, if the U.S. wanted to conduct surveillance beyond these limits, the question of access becomes a question of whether or not the U.S. could operate in Pakistani airspace without notice (or, if noticed, without repercussions). This was the case when the U.S. flew drones into Pakistan to conduct surveillance on the bin Laden compound without Pakistan's knowledge.

Unlike databased sensors which interact very directly with the information it collects (or in some cases *is* the data itself), remote sensors collect information from some distance. These sensors collect imagery, signals (e.g. cell phone communications), and other forms of data. There are two types of remote sensors—passive and active.

Passive sensors collect information from already existing signals, typically electromagnetic energy such as light (for images) and radio signals (for eavesdropping) but this includes sound waves as well. The user will point the sensor at a source of information and the sensor will receive it. Active sensors, on the other hand, project their own energy at the target and then records what happens after that. Air radar systems work this way. Radio signals are emitted into a portion of the sky, bounce off an aircraft, and return to the radar dish. The result provides information about the aircraft's position and speed.

Remote sensor platforms include satellites, aircraft (including drones), and ground and sea based sensors. These platforms operate in different environments and are deployed depending on (a) what information is being sought, (b) what area the state has access to, and (c) what resources and technology the state has at its disposal.

Despite the descriptor 'remote', the distance between the sensor and the target on which it is collecting can vary widely. Satellites orbit miles above the Earth, and aircraft fly thousands of feet overhead. Each effectively flies over the territory over which it collects. Ground stations or sea based receiving stations, on the other hand, may be dozens or thousands of miles away from its target and not require access to the target's territory. For each sensor platform one must distinguish the area of operation from the targeted area. This is, in part, what makes remote sensors special. It is possible for a state to collect information from a territory without being physically present in that territory. Nevertheless, some remote sensors require access to foreign territory.

Chapter Overview

In this chapter I focus on two types of remote sensors—satellites and aircraft—and on *one* type of information—imagery. Details on other remote sensing platforms and the information they collect—e.g. signals and communications intercepts—are very

difficult to come by. The chapter begins with an overview of satellite and drone capabilities. It closes with a case study of U.S. aerial surveillance in Africa. There are three main takeways from the U.S. experience collecting imagery on individuals abroad. First, air-based remote sensors are used where domestic state capability is weak, often in more violent contexts. Second, the U.S. often promises countries improvements in security and access to information in return for permission to fly and base its surveillance aircraft. Finally, the U.S. presence itself is often hidden or downplayed for security reasons.

Satellites

Satellites are valuable assets for any country resourceful and capable enough to put them into orbit. The startup costs are high, but the payoff for surveillance purposes can be great. Depending on the platform, satellites can collect information across the range of the electromagnetic spectrum. Cameras capture light in the visible spectrum and produce images. Antennas capture communications from radio waves. The right satellites can even detect x-rays and infrared radiation emitted from a nuclear detonation or can track ballistic missiles in flight.[251]

In addition to capturing images via the visible spectrum, satellites can be outfitted with different sensor types to capture images in other spectrum bandwidths such as ultraviolet and infrared (this imaging can provide information on vegetation, soil, and geologic features). Satellites can also put together images using radar ("synthetic aperture radar"). This approach, aggressively pursued by the US in the Cold

[251] The U.S., for instance, has a Nuclear Detonation Detection System (NDS) and the Space Based Infrared System (SBIRS)

War, has the advantage of "seeing through" cloud cover and even foliage (the US satellites are known as Lacrosse/Onyx).[252]

Space imaging comes from commercial and government satellites. The latter offer an array of products, and some of their most reliable consumers are actually governments. The first commercial satellite to offer high resolution imagery for sale was IKONOS launched in 1999. Its black and white images had a resolution of 82 cm and its color photos were at 3.2 m. Image resolution refers to the size of an object that could be detected in the image. This means the IKONOS could see missiles in black and white and larger vehicles in color.

Today's commercial satellites are more impressive, with roughly double the resolution over the technology of 1999. With an expected launch by the end of 2013, the GeoEye-2 is capable of 34cm (13.4 inch) resolution in black and white, and 1.36 m (~4.5 feet) resolution in color. The WorldView-3 satellite, scheduled to launch in 2014, is capable of 31cm (~1 foot) resolution in black and white, and 1.24 m (~4 feet) resolution in color. These satellites would be able to determine if someone (outside) were working on a laptop or not. According to Digital Globe, the satellite's manufacturer, the satellite "has an average revisit time of <1 day and is capable of collecting up to 680,000 km^2 per day." This means that the satellite can capture images of one location twice per day, and can capture imagery covering roughly the size of France per day. By the end of 2014 the imagery taken by all the satellites in operation by Digital Globe together could photograph every square kilometer of the Earth roughly three times per year.[253] (See Table 5 for more information on commercial imaging satellites.)

---

[252] See Griffiths and Baker 2007 for technical examples of how radar imaging can be used for counterterrorism.

[253] Earth has a surface area of roughly 510 million km^2. Digital Globe claims that its constellation of satellites will be able to snap shots of roughly 4.2 million km^2 per day. 4.2*365=1533 m km^2/year. 1530/510=3

Table 5. Information on select commercial optical imaging satellites					
Name	B&W Resolution	Color Resolution	Revisit Rate	Collection Capacity	Year Deployed
GeoEye-1[254]	41 cm	1.65 m	<3 days	.35 m km²/day	2008
GeoEye-2[255]	34 cm	1.36 m	3 days	.6 m km²/day	2013 (expected)
IKONOS[256]	82 cm	3.2 m	3 days	.24 m km²/day	1999
WorldView-3[257]	31 cm	1.24 m	<1 day	.68 m km²/day	2014 (expected)
WorldView-1[258]	50 cm	N/A	>1.7 days	1.3 m km²/day	2007
WorldView-2[259]	46 cm	1.85 m	>1.1 days	1 m km²/day	2009
QuickBird[260]	65 cm	2.62 m	2.5 days	.2	2001
SPOT-1 (French)[261]	10 m	20 m			1986 (defunct)
SPOT-5 (French)[262]	2.5 m	10 m			2002
More recent U.S. government spy satellites are thought to deliver imagery with a resolution of a couple inches. According to Tim Brown, a satellite expert at GlobalSecurity.org, the government "can count golf balls" with its state of the art satellites. (cite Wired)					

Personal consumers of commercial satellite images are likely most familiar with the imaging that makes online map services provided by Google, Microsoft, and the like. Some of this imagery is at sub-meter resolution. It could be better, but the U.S. Government restricts commercially available imagery to a 50cm (19.7 in) resolution. The government helps itself to the higher resolution images though, and is itself a major

[254] Digital Globe website n.d. at http://www.digitalglobe.com/sites/default/files/DG_GeoEye1_DS.pdf.
[255] Ibid. at http://launch.geoeye.com/LaunchSite/about/fact_sheet.aspx (GeoEye purchased by DigitalGlobe).
[256] Ibid. at http://www.digitalglobe.com/sites/default/files/DG_IKONOS_DS.pdf.
[257] Ibid. at https://www.digitalglobe.com/downloads/WorldView3-DS-WV3-Web.pdf.
[258] Ibid. at https://www.digitalglobe.com/downloads/WorldView1-DS-WV1-Web.pdf.
[259] Ibid. at https://www.digitalglobe.com/downloads/WorldView2-DS-WV2-Web.pdf.
[260] Ibid. at https://www.digitalglobe.com/downloads/QuickBird-DS-QB-Web.pdf.
[261] Astrium EADS 2013.
[262] Ibid. Also, Spot 5 does stereoscopic imagining.

customer of these commercial providers. For examples of what resolution translates to in practice see Table 6.

Table 6. Imagery resolutions (in meters) necessary for different levels of analysis on targets of interest to arms control [263]

TARGET	Detection [a]	General ID [b]	Precise ID [c]	Description [d]	Technical Analysis [e]
Bridges	6	4.5	1.5	1	0.3
Radar and Radio Sites	3	1-1.5	0.3	0.15	0.015
Supply Depots	1.5-3	0.6	0.3	0.03	0.03
Airfield Facilities	6	4.5	3	0.3	0.15
Rockets and Artillery	1	0.6	0.15	0.05	0.045
Aircraft	4.5	1.5	1	0.15	0.045
Missile Sites (offensive and defensive)	3	1.5	0.6	0.3	0.045
Surface Ships and Submarines	10-30	4.5-6	0.6-1.5	0.3-1	0.3-0.045
Nuclear Weapons Components	2.5	1.5	0.3	0.03	0.0015
Vehicles	1.5	0.6	0.3	0.06	0.0045
Minefields	3-9	6	1	0.03	n/a
Ports and Harbors	30	15	6	3	0.3
Railroad Yards	15-30	15	6	1.5	0.4
Roads	10-20	5	1	0.6	0.4
Urban Areas	60	30	3-5	1	0.75
Terrain	90+	30-90	4.5	1.5	0.75

a Location of a class of units, objects, or activity of military interest.
b Determination of general target type.
c Discrimination within general target type.
d Size/dimension, configuration/layout, components construction, equipment count, etc.
e Detailed analysis of specific equipment.

Government "spy" satellites are more sophisticated. U.S. President Jimmy Carter publically acknowledged the use of photoreconnaissance satellites for the first time in 1978.[264] Although some information has been declassified on older defunct satellites, the

[263] Richardson and Merz 1996.
[264] Carter 1978.

capabilities of U.S. satellites in orbit remain classified.[265] The U.S. constellation of imaging satellites is known by a 'KH' (originally "KeyHole") designation. The first reconnaissance satellite put into orbit by the US—the first of the "CORONA" satellites (KH-1 through KH-4)—had a resolution of 40 feet.[266] The first film recovered from such a satellite was in 1960. By 1963 camera resolution in the CORONA program (KH-4) had increased to 10 feet (for reference, the width of the U.S. M1 Abrams tank is ~12 feet wide).[267] According to the CIA, imagery produced by the CORONA program (from 1959-1972) "is estimated at over 2 million linear shelf feet."[268] According to NASA, "Of the 144 total Corona missions, 102 were successful. Of the 11 Argon missions, 6 were successful. Of the 3 Lanyard missions, 1 was successful."[269]

Resolution enhancements came quickly. The most recently declassified (in 2011) government satellite is the KH-9 (aka HEXAGON) operating from 1971-1986. It had a resolution of about 60cm (2 feet). Today's capabilities are highly classified, but some commentators suggest that the most recent government satellites can deliver images with resolution of a couple of inches. One analyst has suggested that the technology is good enough to "count golf balls."[270] A recent gift of two spy satellites (never been launched) from the NRO to NASA is suggestive of U.S. capabilities. The satellites are "as big and powerful as the Hubble Space Telescope" but have a much larger field of view. As an approximation of how powerful such satellites could be, "NASA official Michael Moore said that if the Hubble Space Telescope were pointed at the surface of the Earth

---

[265] See Richelson 2007 for some declassified documentation.
[266] Perry 1973, 120.
[267] Ruffner 1995, xv.
[268] Ibid., xvi.
[269] NASA Mission and Spacecraft Library n.d.
[270] Franceschi-Bicchierai 2012. Quoting Tim Brown from GlobalSecurity.org .

instead of at outer space, 'you could see a dime sitting on top of the Washington Monument.'"[271] It is not clear if such a statement takes into account atmospheric effects.

Little is known about the current status of the US spy satellite program because it is highly classified (see Table 7). Work by Jeffrey Richelson suggests there are three or four of the KH 11 type satellites still in orbit.[272] One was launched in 1988 and the others in the mid-90s. These satellites carry thermal infrared imaging systems and also integrate geolocation referencing capabilities that facilitate mapping. In addition there is the "Enhanced Imaging System" satellite program also equipped with infrared imaging sensors. Four of these are likely in orbit with the most recent placed into orbit on August 28, 2013. Finally, there is a stealth satellite known as "Misty" with similar capabilities (imaging in both visible and infrared spectrums) that is in orbit. Another program—the Future Imagery Architecture—was cancelled in 2005 before it could be fully implemented. A *New York Times* investigation on the program paints it as a spectacular failure wasting at least $4 billion.[273]

The National Reconnaissance Office (NRO), one of the "big five" U.S. intelligence organizations, is responsible for building, launching and maintaining the nation's spy satellites. Collection priorities are determined by the head of the intelligence community, the Director of National Intelligence.[274] An implication of how the U.S. collects imagery is that the Department of the Defense does not have a stream of tactical satellite imagery at the ready. This led to a program that could provide quicker and cheaper satellites and imagery when the Pentagon needed it. The program, Operationally Response Space, saw one satellite launch but was phased out in 2013.

---

[271] Achenbach 2012.
[272] Richelson 2012, 173.
[273] Taubman 2007.
[274] Erwin 2013, 7.

The NRO maintains ground stations to communicate with their satellites. Two of these are acknowledged to exist abroad—Pinegap, Australia and Menwith Hill, U.K. Both are used for SIGINT missions.

NASA posts some information for all spacecraft launched by the U.S., but for secret programs details are omitted. The most recent launch of a classified satellite was launched on December 05, 2013.

Table 7. U.S. Government Spy Satellites in Operation[275]

Satellite	**Launch Date**	**Sensors**
KH-11 (USA 33)	06.11.1988	Optical
KH-11 (USA 86)	28.11.1992	Optical, Infrared
KH-11 (USA 129, NROL 2)	20.12.1996	Optical, Infrared
Misty (USA 144)	05.22.1999	Optical, Infrared
KH-11 EIS (USA 161, NROL 14)	05.10.2001	Optical, Infrared
KH-11 EIS (USA 186, NROL 20)	19.10.2005	Optical, Infrared
KH-11 EIS (USA 224, NROL 49)	20.01.2011	Optical, Infrared
KH-11 EIS? (USA 245, NROL 65)	28.08.2013	? Optical, Infrared
LACROSSE / ONYX	03.08.1991	Radar Imaging (Active Sensor)
LACROSSE / ONYX	10.24.1997	Radar Imaging (Active Sensor)
LACROSSE / ONYX	08.17.2000	Radar Imaging (Active Sensor)
LACROSSE / ONYX	08.21.2005	Radar Imaging (Active Sensor)

Aircraft

Aircraft can be outfitted with surveillance equipment to capture imagery and signals intelligence. Acquiring imagery requires that the aircraft fly somewhat above the target, but not necessarily directly over it. Even with state-of-the-art equipment, the view an aircraft has on its target is constrained by the Earth's curvature and depends on the

[275] Data gathered from Richelson 2012; Krebs n.d. and additional scouring of news sites.

elevation of the aircraft and the distance of the aircraft from the target (two variables which together approximate the angle at which the cameras are pointed). The view, of course, is also limited by atmospheric effects, geography, vegetation and any intentional obfuscation. Taking all this in to account, it is possible for one state to conduct photo-reconnaissance against another state without flying into the latter's territory. Most imagery taken by planes however is captured from the airspace under which the target resides.

Aircraft can also collect all sorts of signals intelligence. This includes everything from communications content to different electronic signatures emitted by other instruments (e.g. an enemy's radar system). This type of collection is less limited by line of sight and geometry and is more feasible at a distance because signals propagate. As a result states can collect *some* signals well outside another state's territory. In 2001 a U.S. EP-3 aircraft was over 100km off the shore of China doing just this when Chinese pilots collided with the U.S. aircraft forcing it to land in China.

Piloted Aircraft

Piloted aircraft have long played a role in surveillance. Unlike satellites, aircraft fly in (or very close to) sovereign airspace. They also require airbases of varying degrees of proximity to their targets. For a country like the U.S., which strives for global access, basing rights in other countries are indispensable. Despite the potential barriers of territorial access, planes have at least two advantages over satellites. The first is their reusability and accessibility. Planes fly sorties and, ideally, return to base at which point they can be immediately accessed, fixed, upgraded, etc. Satellites, once launched, are physically inaccessible. The second surveillance advantage of planes is the customization of their flight routes. Territorial restrictions aside, planes can be tasked to a new flight path each time they fly.

Although "unmanned" or remotely piloted aircraft are gaining popularity for surveillance activity, piloted aircraft are far from obsolete. Two planes are emblematic of the persistent use of piloted aircraft for surveillance. The first is the iconic Cold War era U2 spy plane. It became operational in the 50s and continues to play important roles in conducting surveillance to this day. The second is a lesser known plane, the PC-12. It is a simple single engine turboprop plane most commonly used for small cargo and passenger loads. In this sense, it is completely unremarkable. The U.S., however, has been using it as a surveillance plane precisely because it is innocuous looking. The PC-12 has been used in Uganda, for example, to help hunt down the Lord's Resistance Army.

Unmanned Aerial Vehicles

The use of Unmanned Aerial Vehicles (UAVs), or drones, is of a surprisingly early vintage. Ever since "manned" flight was used in war, people have been thinking about using drones as weapons. Why not laden an aircraft with explosives and remotely fly it into a critical target? One such drone (arguably better described as a cruise missile) is the Kettering Aerial Torpedo "Bug." Designed in 1917, the aircraft had a bi-plane design. It would take off from a dolly system and its engine would shut off at a predetermined moment sending the aircraft to the ground. 50 Bugs were made but never saw combat.

The first success in testing a drone to release a munition to attack a dummy target seems to be in April 1941 when a Curtiss TG-2 flew 20 miles to release a torpedo which hit the target vessel.[276] In World War II the U.S. further experimented with drones, but saw little success. One ambitious plan—known as Operation Aphrodite—was to remotely pilot B-17s full of explosives into German targets. It was not successful.

[276] Clark 2000, 10.

The use of drones for *surveillance* came later because of technological limitations.[277] This trend reversed itself as technology and needs changed. In 1960 the U.S. Air Force began seriously looking at using drones to conduct surveillance missions. One significant result was the "Firefly" (aka "Lightning Bug") developed by Ryan Aeronautical. This type of drone would either be launched from the ground or from another aircraft, fly its route while conducting surveillance, return to safe space and deploy a parachute to land. Over 3400 reconnaissance missions were flown between 1964 and 1975 in Southeast Asia.[278]

In the Gulf War the U.S. and coalition forces used drones for surveillance, damage assessment, and targeting.[279] A Congressional report on intelligence during the 1991-2 conflict listed the use of the Pioneer drone as one of the "three most successful accomplishments of intelligence in Operation Desert Storm."[280] In the early 90s, the Predator drone made its operational debut in Bosnia.[281]

In the new millennium everything changed. It was only after September 11, 2001 that drones as we know them today were used to destroy targets. Since then the U.S. has revolutionized military aviation with the development and operation of drones.[282] The CIA was already flying drones in Afghanistan in 2000, but it wasn't until October 7 2001 that the first armed mission of a Predator drone was flown.[283] The first CIA drone attack conducted independent from any military operation was in February 2002.[284] Since then the CIA drone program has grown significantly.

---

[277] I'm not including the use of kites and balloons.
[278] Clark 2000, 14.
[279] U.S. House of Representatives Committee on Armed Services 1993, 9.
[280] Ibid., 28.
[281] Kozaryn 1996.
[282] Though the Israelis were early pioneers in developing modern drones.
[283] Tenet 2004, 15–6.
[284] Sifton 2012.

The size of the U.S. drone fleet is sometimes cited as exceeding 7000. This number is staggering, in part because it includes much smaller drones more akin to radio controlled toy planes. For instance, the U.S. military operates over 5,300 RQ-11 "Raven" drones.[285] These drones weigh around 4.5 lbs and launched by being thrown into the air by a soldier. The drones that capture headlines are more sophisticated and sometimes lethal. These include the Predator, Reaper, and Global Hawk drones.

All major drones are outfitted with sensors for surveillance.[286] The majority of drones are used for surveillance.[287] That is to say, most "flight hours" of drones are dedicated to some sort of surveillance role. So despite all the attention lethal "drones strikes" receive, far and away most drone activity is related to surveillance.

Drones can be placed into one of three categories—mini, tactical, and strategic—depending on their flight capabilities. Mini drones fly low, operate at short ranges, and typically operate for under an hour at time. Tactical drones can fly higher, for several hours, and their range is limited to line-of-sight communications (~180 miles). Strategic drones can fly at upwards of 50,000 feet for many hours and at much longer ranges due to the fact that they can communicate via satellite. Strategic drones include the well-known Predator, Reaper and Global Hawk.

Predator drones are primarily used for reconnaissance and target acquisition. It has capabilities that allow it to track moving targets and see through inclement weather. Reaper drones are more capable than the Predator. The current plan is to acquire 404 Reapers. As of mid-2013, 104 Reapers were delivered to the USAF, but only a fraction of these, around 54 perhaps are currently operational. The last five planes are scheduled to be delivered in 2021. (See Table 8.)

[285] Gertler 2012, 45.
[286] The military distinguishes between Intelligence, Surveillance and Reconnaissance (ISR). For simplicity I do not.
[287] U.S. Government Accountability Office 2012, 14.

Usage statistics for drones are hard to come by, but there are numbers on general "flight hours." According to a Government Accountability Office report, the DoD's use of UAVs have grown "from just over 10,000 UAV flight hours in 2005 to more than 550,000 in 2010."[288] To put that into context, there are almost 8766 hours in year. This means that the U.S. must have been flying an average of 63 drones 24 hours a day, every day, during 2010.

Undoubtedly most of these flight hours were logged in the hot warzones of Iraq and Afghanistan, but the numbers are suggestive of their value for surveillance. Drones are primarily used for surveillance (to include targeting) purposes. Their use in conducting lethal attacks is secondary, especially in Iraq and Afghanistan where the U.S. could use conventional aircraft without any problems. Moreover, we can infer something about the drones' value for surveillance against *individuals*. Both the wars in Iraq and Afghanistan were insurgencies and environments where terrorist organizations were much more active. In these environments knowing information about individuals is prized.

[288] Ibid.; For a yearly break down see U.S. Department of Defense 2011, 22.

Table 8. Drones operated by the U.S. Dept. of Defense

System	Vehicles (operational)	Wingspan	Endurance (hrs)	MaxAltitude (ft)	Speed (kt)	Range (nm)	Sensors
Global Hawk RQ-4A	9	131	32	65000	350	5400	E-O, IR, SAR/MTI
Global Hawk RQ-4B	16	131	28	60000	340	5400	E-O, IR, SAR/MTI, SIGINT
Reaper MQ-9	54	66	32	50,000	225	2000	E-O, IR, SAR
Grey Eagle	26	56	26	25000	120	150	E-O, IR
Predator MQ-1	161	55	24	25000	118	500	E-O, IR, SAR
Hunter MQ-5B/RQ-5A	25	29.2/34.3	12/18	15/18000	106	144	E-O, IR
Shadow RQ-7A/7B	364	14	5/7	14/15000	110/105	68	E-O, IR

Pieced together using data from CRS. Data does not include drones operated by the CIA or DHS. Drones are believed have to be flown out of: Afghanistan; Djibouti; Ethiopia; Oman; Pakistan Qatar; Seychelles; Turkey; the United Arab Emirates; and Uzbekistan.[289]

[289] Turse 2013, Ch. 3.

Drones and their surveillance capabilities will continue to grow more sophisticated. A cutting edge piece of surveillance equipment was recently showed off by DARPA. Named ARGUS, the drone-based system can operate at 20,000 feet and take video of a 25 square mile area at a resolution of roughly six inches. As the data is retrieved and processed on the ground, the result is the capability to zoom in on *any* area in the 25 mi^2 region and observe what is happening in *real time*. In addition the software can automatically spot and highlight all moving objects within the frame. As one magazine comments: "If ARGUS was hovering over New York City, it could observe half of Manhattan. Two ARGUS-equipped drones, and the US could keep an eye on the entirety of Manhattan, 24/7."[290] Again, from 20,000 feet at six inch resolution in real time.

According to the U.S. Department of Defense's 25 year "roadmap" (released in 2011), future developments will include better analysis of full-motion video and increased automation of analysis. Currently video data is "stored without being fully analyzed to exploit all information about the enemy."[291] One analytical capability that is on the DoD's wish list is face-recognition. As far as communication intelligence is concerned, "increased automation … has the potential to identify key words and even specific voices to rapidly alert operators to targets of interest."[292] Along similar lines, the roadmap suggests that so many ISR platforms are deployed it is becoming necessary to have the platform (ie. the drone) do more of the analysis. This suggests it will be the drone that alerts the operator if there is a person of interest either by identifying his face or voice.

---

[290] Anthony 2013.
[291] U.S. Department of Defense 2011, 48.
[292] Ibid., 49.

The U.S. is far from the only state using and developing drones. They are proliferating.[293] Over 70 countries have drones, but the vast majority of these are unarmed surveillance drones.[294] The UK and Italy already have purchased Reaper drones, and France recently signed on to purchase 12 of them. The Defense Security Cooperation Agency (whose responsibility it is to notify Congress of foreign military sales) explained that the "potential sale will enhance the intelligence, surveillance, and reconnaissance (ISR) capability of the French military in support of national, NATO, United Nation-mandated, and other coalition operations."[295]

There are second-order information sharing benefits that may come with the sale of drone technology to other countries with whom the U.S. has an information sharing arrangement. For instance the U.S. has an intelligence sharing relationship with Morocco,[296] and Morocco is starting to employ drones. Although their current fleet is not very sophisticated, in 2013 the U.S. demonstrated and trained Moroccan soldiers on the Raven drone.[297] As Morocco uses drones to conduct surveillance, the U.S. could benefit from that information without having to do any of the work. One U.S. Air Force general involved in the sales of drones to African countries summed up the attitude thusly: "Oh man, I'll tell you, I am so excited. [...] If they take care of the problem themselves, we don't have to worry about it."[298]

---

[293] According to the U.S. Government Accountability Office 2012 the U.S. is party to two multilateral regimes that address the proliferation of UAVs, the Missile Technology Control Regime and the Wassenaar Arrangement .
[294] Roberts 2013.
[295] Defense Security Cooperation Agency 2013.
[296] US Diplomatic Cable 2009c.
[297] The Raven drone is launched by throwing it, and is not as sophisticated as the Predator and Reaper drones.
[298] Hinshaw 2013.

The Benefits and Costs of Remote Sensing

Prima facie the benefits of remote sensing are clear—it enhances resolution through imaging and communication intercepts. A look at the surveillance behind the raid that killed Osama bin Laden in Pakistan in May of 2011 is illustrative. According to the *Washington Post* secret budget documents revealed that the "National Reconnaissance Office performed more than 387 "collects" of high-resolution and infrared images of the Abbottabad compound in the month before the raid — intelligence that was 'critical to prepare for the mission and contributed to the decision to approve execution.'"[299] But the imagery provided by satellites flying hundreds of miles above the Earth was not enough. In the months leading up to the raid the CIA also flew stealth RQ-170 Sentinel drones into Pakistan to conduct surveillance—including video—on the compound where bin Laden was hiding.[300] The same RQ-170 drone was reported flying overhead during the raid providing a live video feed.

Less furtive *i-veillance* may require states to share information and sometimes control with their partner. It has been confirmed that the U.S. shares some intelligence it collects from drones with the Pakistanis. During Congressional testimony Admiral Mike Mullen stated: "In terms of support and information, we certainly -- they have asked for that, and where they've asked for that, we've supported them."[301] There has been some reporting that the U.S. has given Pakistan a more hands on role in selecting routes and targets for surveillance (but not lethal strikes).[302]

Remote sensing can also be risky. The risks break down along two main lines: the risk of operating in another country, and the risk of disclosed cooperation. Establishing an infrastructure of remote sensors is politically challenging. The exception here is the

[299] Whitlock and Gellman 2013.
[300] Miller 2011.
[301] Mullen 2009.
[302] Barnes and Miller 2009.

use of satellites. While very expensive and technologically sophisticated, once in orbit satellites can be used unilaterally, legally, and without causing much of a stir. Establishing an international infrastructure of aircraft sensors is much more difficult. The country wishing to project its surveillance capability abroad not only has to have basing rights in another country, but also has to have the rights to fly within another country's airspace or run the run the risk of doing so clandestinely. There is also the risk of having planes shot down. Throughout 2013 Iran has scrambled jets in response to U.S. drones that were close to Iranian airspace.[303]

Case: Aerial Surveillance in Africa

While most people associate drone surveillance with U.S. operations in Iraq and Afghanistan, those cases make for a poor study of *i-veillance* primarily because much of their use has occurred under conditions of U.S. occupation and insurgency. In these locations the U.S. has effectively been operating in "uncontested" airspace that it controls with the blessing of each state. Even though al Qaeda has a presence in both states, the U.S. mission is blurred. On the one hand there are insurgent militias and on the other hand there are groups that are better described as 'terrorists'. Under these conditions, the use of U.S. drones to conduct surveillance in Iraqi or Afghan territory is not a difficult *political* decision for the U.S.

More interesting is the use of drones and other aircraft to conduct surveillance in spaces not occupied by the country operating the aircraft or when the surveillance is uninvited or massively unpopular. The U.S. began using drones to hunt al Qaeda members in Afghanistan and the first drone attacks were seen after 9/11. From

[303] Whitlock 2013.

Afghanistan and Yemen, the use of drones soon spread to Africa. That is where this case study focuses.

Africa is the latest hotspot for drone surveillance. The U.S. is increasingly interested in placing drones in African airspace in order to keep tabs on al Qaeda in the Islamic Maghreb (AQIM), the Lord's Resistance Army, al Shabaab, and Boko Haram. The demand for drones for surveillance purposes appears to be increasing. Responding to questions from the Senate Armed Services Committee the General of AFRICOM stated, "AFRICOM receives only about 7% of its total intelligence, surveillance, and reconnaissance requirements."[304] Likewise, Colonel Bill Tart the head of Air Force's Remotely Piloted Aircraft Capabilities Division has stated, "AFRICOM has a significantly underserviced ISR requirement."[305]

Niger and Mali

In 2012 extremist Islamist groups (some affiliated with al Qaeda) and a separate (non-al Qaeda) Tuareg militia took over parts of northern Mali. The rate at which Mali was succumbing to these organizations alarmed the world and eventually led to a UN Security Council Resolution 2085 authorizing an African-led military mission to help restore order. After an invitation by the Mali government the French military intervened in January 2013.

The U.S. made the decision to support the French and African forces with surveillance from drones, and in late January 2013 the U.S. signed a status of forces agreement with Niger to enable it to base drones there.[306] According to Obama, "This deployment will provide support for intelligence collection and will also facilitate intelligence sharing with French forces conducting operations in Mali, and with other

[304] Rodriguez 2013.
[305] Roston n.d.
[306] The U.S. and Niger were already negotiating a status of forces agreement for the small U.S. military contingent present there, but negotiations were hastened as events unfolded in Mali.

partners in the region."[307] The additional drone base was spurred by both the presence of extremists who were increasingly willing to flex their muscle in the area and a lack of surveillance capability in the region. In other words, the U.S. (and the French) had poor resolution on individuals acting in the Sahel.

As of March 2013 U.S. drones have provided intelligence for nearly 60 airstrikes conducted by the French.[308] By July the U.S. had flown 200 sorties.[309] The U.S. is also sharing drone surveillance information with Chad which is aiding the fight in Mali. *The Wall Street Journal* describes the nature of the cooperation as follows.

> U.S. Reapers scour the deserts and mountains using their sensors to search for so-called patterns of life--communications and movements deemed by the U.S. to be telltale signs of militant activity, officials said. The Americans then pass the raw video feeds and other real time data to French military and intelligence officers who decide if, how and when to use the information. French fighter planes or ground forces sometimes swoop in to attack. The information is also shared with African forces involved in the French-led campaign, including the Chadians, officials said.[310]

The U.S. had two concerns with respect to its assistance in Mali. The first is whether drone surveillance provided to the French makes the U.S. a co-belligerent with the French against AQIM.[311] Second, U.S. surveillance information given to other states might be used in ways the U.S. cannot control. The latter concern is not uncommon when it comes to sharing sensitive information with other countries.

U.S. drone surveillance was important here, but the operation of such drones was arguably only possible under the more exigent circumstances faced by Mali. One might object that the use of drones in this circumstance is more similar to their use under

---

[307] Obama 2013.
[308] Entous, Gauthier-Villars, and Hinshaw 2013.
[309] Schmitt 2013.
[310] Entous, Gauthier-Villars, and Hinshaw 2013.
[311] According to the Wall Street Journal, 'A senior U.S. official said the Americans ultimately decided they weren't cobelligerents because the U.S. was supporting the French rather than joining the campaign.' Ibid.

conditions of insurgency such as those found in Afghanistan. While it is true that such groups effectively took territory and control of towns, their progress was made possible by a weak Mali state. As such there was not much insurgency to speak of in such a vacuum. Moreover, and in particular regards to al Qaeda affiliated groups in the region, individuals *qua* individuals were targeted as such.

Algeria

One individual who became a major target recently was the prominent Algerian militant Mokhtar Belmokhtar. The U.S. considered sharing drone surveillance data with Algeria if the U.S. was permitted to fly in their airspace.[312] The main goal was to find Belmokhtar who also operated out of Mali. In late 2011 the U.S. Ambassador to Algeria, Henry Ensher, "proposed that the United States share what limited intelligence it had on Mali with the Algerians to encourage them to act against Mr. Belmokhtar either directly or through their contacts with the Tuaregs in northern Mali. Mr. Ensher later expanded the idea to include sharing information from unarmed drone flights."[313]

This is interesting for multiple reasons. The offer was framed as: the U.S. gives Algeria intelligence on Belmokhtar, and Algeria would try to neutralize him. Drones were offered as a way to get this intelligence. Moreover, the fact that intelligence from drones was offered later suggests that this offer was made to sweeten the pot—as if the Algerians would not be interested in or benefit from other sources of intelligence. Finally it is important, though not necessarily surprising, that the drones would be unarmed. This suggests that other states contemplating allowing U.S. drones in their airspace have varying comfort zones—surveillance maybe, but not armed drones.

---

[312] Gordon and Schmitt 2013.
[313] Ibid.

Although the 2011 offer was not accepted, Algeria allowed a Predator drone to monitor a hostage taking attack orchestrated by Belmokhtar in January 2013.[314] Afterwards, the U.S. again made an offer to the Algerians. If the Algerians allow U.S. drone surveillance, the Algerian military can use the intelligence to crack down on militants, including Belmokhtar, in their area. The U.S. has essentially been pressing for Algeria to relent since 2011. *The New York Times* reporting suggests that Algeria bight be more willing in the aftermath of the Belmokhtar attack, but as of this writing Algeria has yet to agree.

Uganda

In addition to drones the U.S. flies other spy planes that perform similar surveillance functions. The U.S. flies aircraft in central Africa, and out of Uganda in particular. As early as 2008 the U.S. was providing military advisers and intelligence to Uganda in its fight against the Lord's Reistance Army (LRA).[315] In 2009 the U.S. passed the "Lord's Resistance Army Disarmament and Northern Uganda Recovery Act"[316] in which it declared its policy to provide regional governments with intelligence support (among other forms of assistance) to fight the LRA. In October 2011 President Obama notified Congress of his intention to send in roughly 100 armed soldiers to central Africa to help counter the LRA. The forces were not to directly engage the LRA themselves, but rather play a support role—"providing information, advice, and assistance to partner nations." In addition to these troops, the U.S. flies piloted surveillance aircraft in Uganda and throughout the region. These aircraft, run by private military contractors, are equipped with sophisticated equipment similar to that used by drones.

---

[314] Ibid.
[315] The U.S. provided non-lethal support during "Operation Lightning Thunder", a regional offensive against the LRA which didn't turn out well.
[316] Public Law 111–172

In December 2009 the U.S. embassy in Uganda sent a cable to D.C. acknowledging not only that the U.S. provides Uganda with intelligence but also that Uganda uses that information to fight the Lord's Resistance Army. According to the cable, intelligence collected by the U.S. is first vetted by a "Combined Intelligence Fusion Center" stationed in Kampala. The cable refers to an intelligence sharing agreement between the U.S. and Uganda, and it refers generically to previously signed memorandums of understanding regarding information sharing.

The thesis of the cable, written by Ambassador Lanier, is that Ugandan officials have made assurances that U.S. intelligence is used responsibly and according to extant agreements, and that the he believes the Ugandan position to be "reliable and credible."[317] Information sharing is focused on routing the LRA and Kony. With such information, Uganda pledged to comply with the laws of war and to consult with the U.S. when using the information to conduct offensives in "operations not governed by the law of armed conflict." The Ambassador writes that "Uganda understands [...] that misuse of this intelligence could cause the U.S. to end this intelligence sharing relationship." The language of the cable suggests it is important for both parties to maintain the relationship. U.S. concerns are reflected in related reporting. "U.S. officials said they take care to withhold intelligence that could enable their African partners to target political opponents instead of terrorist groups, but they acknowledged that it can be difficult to know the difference."[318]

What the Uganda case suggests is that Uganda is hungry for intelligence but not eager to have U.S. drones flying in its airspace. The goal of both the U.S. and Uganda is

[317] US Diplomatic Cable 2009d.
[318] Whitlock 2012c.

not just to fight off the LRA but to find its leader, Joseph Kony.[319] Indeed the U.S. sources cited above all make reference to getting not just the LRA but Kony specifically.

In addition to Uganda, these surveillance flights cover the Congo, South Sudan and the Central African Republic.[320] At an event meant to invite proposals from private contractors to conduct aerial surveillance in Central and Northern Africa, contractors were told, "At a minimum, contractors were told that they would have to keep planes flying for 150 hours a month."[321]

It is important to emphasize that in Uganda the U.S. opted for a program (known as Tusker Sand) in which private contractors use piloted aircraft to conduct surveillance in the region. The fact that drones are not chosen as the surveillance vehicle it is illustrative. A plan to use drones and blimps was developed but scraped in favor of piloted surveillance. The U.S. apparently wanted "innocuous" aircraft that didn't stick out. According to *The Washington Post*, a U.S. federal website "warned firms bidding for the [surveillance] work that African countries would be 'uncomfortable' with activities that might look suspicious, adding: 'Don't want covert aircraft, just friendly looking aircraft.'"[322]

There are two non-competing explanations for the U.S. decision to use contractors flying inconspicuous planes to conduct surveillance. First, using private contractors buys the U.S. government some distance from the operations. Not only does it avoid committing U.S. military personnel to the region, but it makes potential accidents easier to recover from. The second explanation is more relevant to the study at hand. African countries didn't want weird looking drones flying in their airspace, the

---

[319] Kony is listed by the U.S. as a 'specially designated global terrorist'
[320] Whitlock 2012a.
[321] Ibid.
[322] Ibid.

suggestion being that their presence raises difficulties. The most obvious signal a drone sends is that "the U.S. is in your airspace."

A Senate panel, however, has pushed back a bit and directed the Pentagon to look into ways to incorporate aircraft that can loiter in the air for longer periods.[323] The suggestion here is that piloted aircraft (PC-12s) are inadequate compared to drones that can remain airborne for over 20 hours at a time. (This was in the context of manhunt for Kony.)

Burkina Faso

The U.S. operates PC-12 flights out of Burkina Faso and relies on an intelligence fusion cell (known as Aztec Archer) there to process surveillance data. In addition, Burkina Faso participates in the Trans-Sahara Counterterrorism Program—a U.S. led effort to build counterterrorism capacity (both military and civilian) in the region.

While it is unclear when the U.S. started flying surveillance flights out of Burkina Faso, some basing provisions for U.S. aircraft date back to 2006. According to a diplomatic cable, in 2006 the President of Burkina Faso, "approved the basing of a Joint Special Operations Air Detachment (JSOAD) in Ouagadougou to support U.S. Special Operations Command Europe's medical evacuation and logistics requirements [as well as] significant improvements to the JSOAD hangar and basing area at no cost to the U.S. Government."[324] This quote doesn't suggest surveillance support, but it is perhaps the genesis of cooperation that led to PC-12 flights.

What is clear is that the same desire for discreetness seen in the Uganda case is present in the Burkina Faso case. A 2009 diplomatic cable with the subject "Alternate Parking for USG Aircraft in Burkina Faso" details "Burkina Faso's objectives to maintain

---

[323] Ibid.
[324] US Diplomatic Cable 2009b.

discretion concerning the American presence."[325] U.S. aircraft were stationed at an airbase in Ouagadougou, but the precise location was problematic. The cable explains Burkina Faso's Minister of Defense's concerns: "the present location of the aircraft was in retrospect not an ideal choice in that it put the U.S. aircraft in a section of the airfield that already had too much traffic. The problem is not, he insisted, the presence of the aircraft themselves. He also commented that U.S. personnel were extremely discreet and did not attract undue attention." The language suggests simultaneously Burkina Faso's concern about U.S. aircraft and its desire to keep them in Burkina Faso. The problem is not the aircraft themselves, nor is it U.S. personnel. It is simply that the aircraft might be noticed.

The cable describes two options. One idea has the aircraft relocating to a base in Bobo Dioulasso over 200 miles away. This is described as not a viable substitute but available for short term or emergency needs. The problem with Bodo Dioulasso, the cable explains, is that it "has very little traffic, and the U.S. planes and personnel would likely draw greater attention there." This echoes the theme of discretion.

The proposed solution is simply another location in Ouagadougou. Again the Minister of Defense's concerned were explained. "He expressed a preference that they be housed in temporary hangars similar to what is being used now, because that would be discreet, clean and easiest to protect." The U.S. chargé d'affaires "explained that there was little chance of building anything permanent because the United States does not in any way want to give the impression of 'building a base.' Nor, he added, did we want to draw attention to the aircraft so as not to increase the risk of terrorist attacks."

Discretion and security are emphasized throughout this cable. Importantly they are linked. A U.S. presence might be unpopular, and this itself is a problem especially for

[325] US Diplomatic Cable 2009a.

Burkina Faso's politicians. Perhaps more important to the players involved, however, is that the U.S. presence might prompt violence. In addition, the U.S. position is emphasizing the importance not only of discretion, but also impression management. The U.S. should not be seen as establishing anything permanent. Burkina Faso's Minister of Defense "replied that this fit in well with Burkina Faso's thinking as well."[326] In later reporting, the Foreign Minister averred. "I cannot provide details [about the program], but it has been very, very helpful. [...] This cooperation should be very, very discreet. We should not show to al-Qaeda that we are now working with the Americans."[327]

Conclusion

U.S. aerial surveillance is bringing resolution to a vast area. However, there are different mission types with distinct approaches to surveillance. In Mali, for example, drone surveillance has played a significant role in supporting French combat operations. Drones were also used to search for specific known targets—Joseph Kony and Mokhtar Belmokhtar—and 'unknowns' that might be threatening by focusing on "telltale signs of militant activity."

What comes across in the broader data collection as well as the case study is that drones are used by the U.S. for surveillance in violent contexts where state power is weakly projected. The U.S. does not seem to be using drones to support an otherwise strong state with quotidian law enforcement. As far as I know, this is not occurring in world politics (the closest example of this may be U.S. drone assistance to Turkey). The people under surveillance appear to be engaged in illicit and violent activity, and the territories in which they operate are weakly covered by state power.

---

[326] Ibid.
[327] Whitlock 2012b.

The U.S. surveillance infrastructure brings resolution to these areas (and, specifically, territory), but the resolution comes with a price. The U.S. requires permission to operate these aircraft in the airspace of other countries. Moreover, the U.S. requires basing permissions. To get permission the U.S. seems to be offering security by helping eliminate bad guys in the area. Sometimes the U.S. works alone, sometimes it shares the intelligence. To what extent the U.S. takes the extra step to share is unclear. But as the cables regarding Algeria suggest, such an offer is made to sweeten a deal and is not *pro forma*.

Somewhat paradoxically, the promise of security that the U.S. presence brings, requires a discreet touch lest that same presence becomes an irritant to local populations. With the exception of U.S. assistance in Mali, the U.S. presence in the other countries reviewed is something that is both welcomed yet downplayed.

Chapter 6: Human Sensors

"The more we partner up globally—sharing information, developing strategies together, and even working side-by-side—the better off we'll all be."[328]

- Tom Fuentes, former Assistant Director of the FBI

"Criminals and terrorists don't respect borders, and neither can our efforts."[329]

- John Pistole, former Deputy Director of the FBI

Introduction

States can conduct surveillance through simple human interaction and observation. In the intelligence world this activity is known as "human intelligence," or HUMINT. The CIA, for example, fields human spies abroad (usually a well-placed foreign agent) who collect and report information back to the agency. There are, however, less obvious but more common ways in which states can conduct surveillance in general, and *i-veillance* in particular, with human sensors.

Any state official that works abroad and reports back to her government what she has seen and learned is effectively conducting surveillance. For instance a U.S. diplomat in France may learn how the French run diplomatic security and relay that information to the U.S. State Department. Surveillance doesn't have to be sneaky, and can in fact be mutually beneficial. The people that conduct *i-veillance* in this manner act as human

[328] Fuentes 2005.
[329] Quoted in Graff 2011, 20.

sensors picking up information concerning individuals whom the state deems threatening.

Chapter Overview

This chapter focuses on two ways human sensors are used in international politics. While HUMINT is an obvious case to explore, it is a secret practice, and I lack the credentials to research it. Instead I outline how liaison and educational relationships foster *i-veillance*.

Through liaison relationships officials of different states work together to share information. When officials are working abroad they observe and infer additional information. The more fruitful liaisons for *i-veillance* are between states' law enforcement and intelligence agencies. Liaison serves as a conduit for information sharing and enables joint investigative practices in which foreign partners work in domestic jurisdictions. I argue that liaison relationships are crucial for idiocentric surveillance practices, as is the mere presence of the attaché. I will also show that liaison enhances the surveillance capabilities of the partner states involved. One interesting result of the case study is that, while the U.S. maintains an enormous network of law enforcement officials abroad, *weaker states* take advantage of the U.S. network to support *their* objectives.

A second source of human sensors is training or educational relationships. The argument that these relationships result in surveillance benefits is less straightforward. Training produces a common working knowledge and vocabulary, facilitates interoperability, and lays the foundation for future cooperation. Moreover, if one state trains others, it instills within them certain priorities and ways of seeing.

As is evident by now, different sensors trigger different senstitivies and political concerns. HUMINT is conducted secretly so as to avoid political and security blowback.

However, the human sensors discussed below—those used in liaison and in educational efforts—are relatively risk free. While a foreign liaison/educator presence might be controversial in some countries, typically governments do not go to great lengths hiding the fact of such interactions.

Liaison

Official liaison relationships are typically orchestrated through embassies. Intelligence, military, and law enforcement officials often get posted to diplomatic missions for liaison purposes. For instance, the U.S. CIA "Station Chief" is typically the state's intelligence representative abroad.[330]

States post attachés to its embassies abroad. With this practice a general connection is formed between a diplomatic presence and intelligence collection, a connection which is not in any way new. As Simon Chesterman notes, "The emergence of modern diplomacy in Renaissance Italy recognized the importance of having agents to serve as negotiators with foreign powers, but a chief function of the resident ambassador soon came to be ensuring the flow of a continuous stream of foreign political news to his home government."[331]

The connection between diplomacy and intelligence is acknowledged in international law. The 1961 Vienna Convention on Diplomatic Relations states that among "the functions of a diplomatic mission" is "ascertaining by all lawful means conditions and developments in the receiving State, and reporting thereon to the Government of the sending State."[332] According Chesterman, "[t]he Convention also provides for receiving state approval of military attachés, presumably in order to

[330] Ghosh 2009.
[331] Chesterman 2011, 30.
[332] Vienna Convention on Diplomatic Relations 1961 Article 3d.

ascertain their intelligence function. This is consistent with the relatively common practice of having identified intelligence officials in certain diplomatic missions for liaison purposes."[333]

Military Liaison

Military liaisons focus on military-to-military relations. The general idea is to foster good relations and to learn about and from one another. Some liaison relationships are more involved and entail setting up training and joint exercises or even coordinating on real operations. It seems widely accepted that attachés play an intelligence role. The U.S. Defense Intelligence Agency, which runs the U.S. military's attaché efforts, explains on its website that the "objectives [of the attaché system] are twofold: to provide a more efficient system for the collection of intelligence information for DoD components and to preserve a channel for Service-to-Service and DoD representational matters of common interest worldwide."[334]

An attaché in a country struggling with terrorism or intense crime will likely be focused on how the host country's military addresses these issues. Insofar as both countries have an interest in eliminating the threats coming from these individuals, the liaison relationship will serve an *i-veillance* role shuffling relevant information back and forth between the guest and host state.

A former U.S. Army attaché to Kiev describes the "observing and reporting" role of military attachés as their "primary function."[335] "To succeed in security cooperation, policymakers and decision makers require actionable information. It is often attaché input that makes for effective security cooperation programs."[336] While "observation and reporting"—surveillance—covers conventional military issues, attachés "increasingly [...]

[333] Chesterman 2011, 30–1 See Art 7 of the Vienna Convention.
[334] U.S. Defense Intelligence Agency n.d.
[335] Shea 2005, 51.
[336] Ibid., 52.

serve as the conduit for sharing information, especially in support of the war on terror."[337]

There are more specific examples of how attachés can be used for *i-veillance*. In Africa Japan has reportedly planned to add seven attachés to the two already present.[338] The decision came after Japanese nationals were taken hostage and killed in Algeria in 2013. Japan had no liaison presence to learn what was happening (and instead had to rely on the British). The *Japan Times* explains the attachés' purpose is to "collect information from other foreign military attachés."

U.S. efforts deserve special attention. Although there are no hard numbers on U.S. defense attaché personnel abroad, it is a good bet that the U.S. has more stationed abroad than any other country.[339] Of course, some of these focus on terrorism-related threats. The U.S. defense attaché in Tanzania, for example, has worked with regional military counterparts to train special operations forces.[340]

The U.S. military recently added extra liaison capabilities, beyond the traditional defense attaché, to assist with criminal and terrorist elements abroad. In 2006 a few U.S. Special Operations troops known as "Military Liaison Elements" were deployed in "more than a dozen embassies in Africa, Southeast Asia and South America" (areas with a higher presence of terrorists).[341] According to the *New York Times*, the purpose was "to gather intelligence on terrorists in unstable parts of the world and to prepare for potential missions to disrupt, capture or kill them."[342] This activity is very close to the tip-of-the-spear of counterterrorism activity abroad. Again according to the *Times,* "Officials involved with the program said its focus is on intelligence and planning and

---

[337] Ibid.
[338] The Japan Times 2013.
[339] The U.S. "Defense Attaché System" is run by Defense Intelligence Agency (the DIA).
[340] U.S. Embassy - Tanzania 2013.
[341] Shanker and Shane 2006.
[342] Ibid.

not on conducting combat missions." The *Times* reporting is a clear example of military liaison focused on *i-veillance*.

Extra liaison capacity can also be sent for more pinpoint purposes. In 2012 for example, the U.S. sent a former Navy Seal to the Embassy in Mexico City to assist Mexico with its struggle against drug cartels.[343] This reflects the latent surveillance capability of a broader *i-veillance* assemblage mentioned in Chapter 2.

Homeland Security

The U.S. Department of Homeland Security (DHS), despite what the name suggests, has an international presence. DHS' Immigration and Customs Enforcement (ICE) has the most active DHS liaison presence abroad with a presence in 48 countries.[344] ICE focuses on terrorism and transnational crime. Among the responsibilities of ICE liaisons are "coordinating investigations with foreign law enforcement counterparts" and "referring requests from host country agencies to ICE domestic investigative offices." In January 2014, for example, ICE and foreign counterparts brought down an international on-demand child pornography ring based in the Philippines.

Participating in investigations requires receptivity to information—i.e. some amount of *i-veillance*. The language cited above also suggests that information flows both ways. ICE not only conducts *i-veillance* to pursue U.S. interests abroad, but also takes in requests and information from other states for potential follow up in the U.S.

While ICE is the mainstay of DHS' international liaison efforts, there are additional elements.[345] In 2005 the DHS decided to station a counterterrorism liaison in

---

[343] Althaus 2012.
[344] DHS Immigration and Customs Enforcement n.d.
[345] While not an example of *i-veillance*, DHS Customs and Border Protection operates in 58 cargo ports around the world to examine cargo bound for the U.S. The "Container Security

Brussels to work with EU counterparts. The Secretary of DHS explained: "This new position is not only symbolic of our commitment to increased cooperation, but, by having a direct link [...] it will allow for constant communication on an operational level. The Homeland Security attaché will enable us to make decisions faster and ramp up security more easily by working in the arena side by side, rather than across an ocean."[346] The liaison facilitates communication of information related to terrorism and crime—*i-veillance*—thereby contributing to more effective cooperation.

Law Enforcement

Law enforcement liaison not only allows states to take-in information, but push out information as well to partner countries. "In direct consequence of their relationships with law enforcement and intelligence services abroad, [legal attachés] are familiar with investigative rules, protocols, and practices that differ from country to country. They are thus well positioned to analyze and disseminate the intelligence that directly impacts U.S. national interests both domestically and abroad."[347] We saw something similar when looking at databased sensors. Surveillance is not just about sucking up information. It is about getting information where it needs to be.

A former Director of the UK's National Criminal Intelligence Service argues that *effective* law enforcement liaison requires high levels of mutual trust. To establish and maintain trust, for any given case for which cooperation is sought, there should be "full sharing of the intelligence available."[348] Sharing information also greases the wheels for

---

Initiative" is an example of surveillance more broadly, and helps the U.S. push security functions outward.

[346] Ridge 2005.

[347] U.S. Federal Bureau of Investigation 2012a, 25.

[348] Bailey 2008, 98–9.

any other international judicial processes that may be required to move forward on a case.

The case study below focuses on what is arguably the largest and most significant international presence of law enforcement officers—the U.S. Federal Bureau of Investigation (FBI).

Law enforcement liaison is not limited to the U.S. Brazil and Paraguay for instance have a strong relationship. In a 2011 interview the Brazilian ambassador to Paraguay explained the importance of the two countries' liaison for combating transnational crime. "Cooperation is very fluid, intense, and very close, especially in the border region. [...] Our cooperation has sought to focus on the exchange of information, the use of technology."[349]

Another U.S. law enforcement agency heavily involved in liaison deserves mention—the Drug Enforcment Agency (DEA). The forerunner to the DEA—Federal Bureau of Narcotics—sent agents abroad for the first time in 1949. As of 2007, the DEA had 751 employees abroad serving in 59 states.[350]

Among the DEA's international operations' five principal objectives is to "participate in bilateral investigations" and "support intelligence gathering and sharing efforts."[351] At times the DEA plays a substantial and direct role in *i-veillance* abroad. The DEA describes its international investigative activity as follows:

> DEA special agents assist their foreign counterparts by developing sources of information and interviewing witnesses. Agents work undercover and assist in surveillance efforts on cases that involve drug traffic affecting the United States. [...] In addition, when host country authorities need to know the origin of seized illicit drugs, DEA agents ship them back to DEA facilities in the United States for laboratory analysis.[352]

---

[349] Stratfor - Interfax Ukraine 2011.
[350] U.S. DOJ Office of the Inspector General 2007.
[351] Ibid., iii.
[352] The U.S. Drug Enforcement Agency n.d.

In addition to taking-in information, the DEA pushes information out to support their partners' *i-veillance* efforts (partners who, it must be emphasized, share similar objectives). The DEA "supports its foreign counterparts' investigations by providing information, such as who controls the drug trade; how drugs are distributed; how the profits are being laundered; and how the entire worldwide drug system operates at the source level, transportation level, wholesale and retail levels."[353]

According to the DEA its presence abroad is limited to locations where the drug trade affects U.S. interests. It has a list of 212 high priority organizations (as of 2006).[354] 100 of the cases involving priority organizations were inked to terrorism.[355] (See Table 9 for more on DEA involvement abroad.) This underlines the *i-veillance* impetus of DEA activity. Some DEA agents, "Special Investigative Units," are specially trained and vetted for their work abroad. For example, "in May 2006, SIUs in Colombia and Brazil, working with several other DEA domestic and foreign offices, completed a 3-year investigation that resulted in over 100 arrests."[356]

Table 9. DEA targeting of Priority Target Organizations (PTO) from 03/2002 – 06/2006[357]

Foreign Region	Total PTO Cases (active and closed)	Targets Disrupted (active and closed)	Targets Dismantled (only closed cases)
Andean	114	29	23
Caribbean	65	22	16
European	53	20	13
Far East	56	19	7
Mexico/ Cent. America	37	7	2
Middle East	43	8	4
Southern Cone	42	13	9

[353] Ibid.
[354] U.S. DOJ Office of the Inspector General 2007, vi.
[355] Ibid., viii.
[356] Ibid., xi.
[357] Ibid., vi.

i-Veillance Through Training and Education

When security officials of one state train those of another, there are potential indirect *i-veillance* benefits for the former. Training produces a common working knowledge and vocabulary, facilitates interoperability, and lays the foundation for future cooperation.[358] The state providing the training reproduces its own practices in the trainees. The result is multiple states working with the same optics. The trainees may start to "see" what they were trained to see. In this way the *i-veillance* interests of the training state get projected abroad. The argument here is **not** that the training of foreign officials is the same as *i-veillance* or that wherever one sees such training *i-veillance* will necessarily follow.

Multiple U.S. agencies train the personnel of their foreign counterparts. The principal means by which the U.S. trains foreign law enforcement officers is the State Department's International Law Enforcement Academies (ILEAs). Among the objectives of ILEAs relevant to *i-veillance* are: "Improve coordination, foster cooperation, and, as appropriate, facilitate harmonization of law enforcement activities within regions, in a manner compatible with U.S. interests;" and "Foster cooperation by foreign law enforcement authorities with U.S. law enforcement entities engaged in organized crime and other criminal investigations."[359]

The FBI provides training to local law enforcement at ILEAs located in Hungary, Thailand, Botswana, and San Salvador. The direct effects for *i-veillance* are clear. According to the FBI, through training, "the Bureau improves information sharing and collaboration with these global partners."[360]

---

[358] A dependency on this type of training is a possibility as well. For a discussion of how development assistance can paradoxically stymie institutional growth see Moss, Pettersson, and van de Walle 2006.

[359] U.S. Department of State, INL 2009.

[360] U.S. Federal Bureau of Investigation 2012a, 48.

For example, in 1995 the U.S. created the flagship ILEA in Budapest.[361] It has 27 participating countries from Central and Eastern Europe as well as Russia and Turkey. An ILEA in Thailand was established in 1998 and is meant to serve the needs of South East Asian countries. One of that region's most significant challenges is neutralizing the illegal drug trade. As of late 2008, the ILEA in Bangkok had trained over 8500 individuals from across the region including China.[362]

The DEA, which also participates in ILEAs, has been training others since 1973, and currently trains approximately 2500 foreign officers every year.[363] In addition to providing know-how, one of the objects is to "[i]ncrease cooperation and communication between foreign law enforcement personnel and DEA in international drug trafficking intelligence and operations."[364]

The Departments of State and Defense run military training abroad through the International Military Education and Training (IMET) program. IMET training focuses on military professionalization, respect for rule of law, and human rights. In many country specific programs, however, there is explicit focus on helping other militaries address terrorism and crime.[365] The goals are similar in spirit to ILEA—developing rapport, enhancing capabilities for future cooperation, *etc.* While the law enforcement centered ILEA had a $31 million budget in 2012,[366] the more muscular IMET had over $105 million.[367] In 2010 IMET trained individuals from 125 countries at over 180 schools abroad.[368]

---

[361] According to the ILEA Budapest website
[362] According to background information from the ILEA Bangkok website
[363] U.S. DOJ Office of the Inspector General 2007.
[364] The U.S. Drug Enforcement Agency n.d.
[365] U.S. Department of State 2013, 180–1.
[366] Ibid., 158, 573.
[367] Ibid., 180.
[368] U.S. Government Accountability Office 2011, 8, 4.

Case Study: FBI Liaison Abroad

The U.S. Federal Bureau of Investigation (FBI) is an example of a network of human sensors that expands abroad to conduct *i-veillance*. As the U.S.'s federal law enforcement arm the FBI is primarily a domestic institution. But the FBI has always had an international impulse. It was born in part as a reaction to the international problems of anarchist terrorists and the white slave trade. During the First World War the bureau was charged with investigating spying. Soon thereafter it briefly took on counterespionage responsibilities in South America leading up to World War II. In more recent decades the FBI has worked with international partners on terrorism cases such as the Lockerbie bombing and fight international criminal rings such as La Cosa Nostra.

Since 9/11 however, the international role of the FBI has expanded tremendously. In what follows I will show how the FBI has moved beyond quotidian international law enforcement cooperation to a real presence *in other states*. The U.S. is no longer concerned with merely facilitating extradition requests or periodically assisting in investigations. The FBI is truly a global law enforcement organization. The FBI has increasingly distributed its capabilities abroad.

A Brief History[369]

Prior to 1908 the United States had no centralized federal law enforcement agency. The Attorney General at the time, Charles Bonaparte (grandnephew to Napoleon) would have to rent Secret Service officers to conduct investigations for the Department of Justice (DOJ). After Congress prohibited federal departments from loaning out Secret Service agents in May 1908, Bonaparte took the initiative to create a small group of agents who would be responsible for most investigations under the DOJ.

[369] For some history consult U.S. Federal Bureau of Investigation 2008, and ; Kessler 2002.

In 1909 Bonaparte's successor named the small group "the Bureau of Investigation." The BI would become the FBI in 1935.

The creation of the FBI was overdetermined, but international issues were an essential part of the story. Attacks by anarchists across Europe in the second half of the 19th century were a major source of anxiety across the continent. In 1878 assassination attempts were made against the German emperor, the king of Spain and the king of Italy. Russian Tsar Alexander II was assassinated in 1881, as was the president of France in 1894, the premier of Spain in 1897, the empress of Austria in 1898 and the king of Italy in 1900.[370] By the late 19th century anarchist violence had spread to the U.S. Johann Most was pushing "Propaganda by Deed" in his publication *Freiheit*, Haymarket Square caused a furor, and Emma Goldman was agitating. The U.S. suffered an assassination as well when Leon Czolgosz shot President McKinley in 1901.

Around this time the Europeans and Russians were pressuring the U.S. to join an international effort to combat anarchism.[371] One of the reasons why the U.S. did not sign on to the 1904 St. Petersburg Protocol, which would have facilitated law enforcement cooperation and information sharing, is because the U.S. did not have a centralized police system yet.[372]

After an anarchist bombing spree in 1919, of which one bomb targeted Attorney General Palmer, a "General Intelligence Division" was set up to investigate foreign radicals. J. Edgar Hoover was assigned as its head. In 1920 the infamous "Palmer Raids" resulted in "dragnet arrests of thousands of alien residents and U.S. citizens attending

---

[370] Martin Miller Origins. 28 in Terrorism in Context (978-0-271-01014-4)
[371] Jensen (2001)
[372] Jensen (2001)

meetings of the Communist Party and the Communist Labor Party in thirty-three cities."[373] The 1919 bombings were never solved.

Beyond the growth in the Bureau spurred by anarchism, the Bureau also grew in response to the 1910 Mann Act, or the White Slave Traffic Act, which itself was motivated by an international concern for (and eventually a convention on) "the White Slave Traffic." The U.S. law prohibited the interstate trafficking of women and girls, with a particular concern for prostitution. The Bureau grew in response. "By 1915, Congress had increased Bureau personnel more than tenfold, from its original 34 to about 360 special agents and support personnel."[374]

In addition to the size of the Bureau, the *shape* of the FBI was also influenced by international events. There were border issues with Mexico. Europe broke out in war in 1914, and the FBI was in charge of enforcing the Espionage Act of 1917 and the Sabotage Act of 1918. An early and ambitious international effort of the FBI was the Bureau's "Special Intelligence Service" (SIS), created in 1940 as a counterintelligence effort against Germany's influence in Central and South America.

The origin of the FBI's international crime fighting efforts can be traced to the organization's investigation of the Mafia. Agents working to understand the Mafia in the U.S. (aka "La Cosa Nostra" – "this thing of ours") understood there was an important connection to the Sicilian Mafia. Progress on the investigations relied therefore on a relationship with Italian counterparts. Information from U.S. agents would flow to the assistant legal attaché in Rome, Special Agent Leone Flossi, who would then relay that information to Italian authorities. Eventually this information reached the Italian investigative prosecutor Giovanni Falcone. Falcone had visited the U.S. to meet with U.S.

---

[373] Kessler 2002, 15.
[374] U.S. Federal Bureau of Investigation 2008, 8 See also Jensen 2001, p 35.

officials for the first time in 1980. Overtime this relationship would grow and prove pivotal for bringing down the Mafia.

An example of how *i-veillance* worked in the Cosa Nostra case is illustrated in Garrett Graff's *The Threat Matrix*.

> In late May [of 1981, agent] Rooney and his team encountered a name they hadn't heard: Giuseppe Bono. Surveillance had shot a couple pictures of the guy at Catalano's bakery and followed him back to an enormous mansion in Pelham that he evidently owned. Rooney called the Italians: Had they ever heard of him? Falcone's team didn't believe the question at first. Bono was, according to Falcone's investigation, one of the most powerful mobsters in the world and a leader of the global heroin trade. Bono had dropped off the Italian map and was presumed to be hiding in South America. He was number one of the 162-person list of Italian organized crime figures [...] and he was just walking the streets of Queens? To a later generation of FBI agents, a find of this importance would be like discovering that Osama bin Laden had been living in a London flat.[375]

Cooperation on international criminal investigations continues today, and the relationships are tighter than ever. An example is the FBI's Eurasian Threat Focus Unit (ETFU) developed to focus on Eurasian organized crime. The ETFU relies on a broad array of what I would regard as sensors to increase its resolution on Eurasian organized crime. The sensors it pulls information from include "FBI field offices, Legal Attachés, international law enforcement and intelligence partners, and the U.S. Intelligence Community."[376] And to further support the ETFU's mission the FBI recently deployed additional Special Agents abroad "to work hand-in-hand with international law enforcement agencies and intelligence services who are committed to addressing and combating Eurasian organized crime."[377]

---

[375] Graff 2011, 91–2.
[376] U.S. Federal Bureau of Investigation 2012b, 1.8–1.9.
[377] Ibid., 1.9.

The FBI remains concerned about transnational organized crime because such illicit networks are enormous and take a real toll on civil society. In Congressional testimony regarding the FBI's 2013 budget, Director Mueller notes that "[t]oday, international criminal enterprises run multi-national, multi-billion-dollar schemes from start to finish."[378] Moreover, in the last decade there has been an increase in governments' concerns regarding the nexus of terrorism and organized crime.

FBI Legal Attachés

To prosecute its mission abroad, FBI partnerships with other governments are a practical necessity (and also a legally *necessary* condition). On the 10th anniversary of 9/11 the FBI Director testified that "Intelligence-driven investigations require a unity of effort with partners overseas, especially as global cooperation becomes increasingly necessary to combat terrorism [and] the FBI has strengthened relationships with international partners. This expanded global reach not only benefits FBI's foreign partners, but also aids FBI collection efforts and investigations."[379]

The FBI's international operations are conducted through its Legal Attaché Program. Since its inception[380] the FBI has been establishing legal attaché (aka LEGAT) offices in U.S. embassies abroad. The FBI attaché is a special agent and is present as a formal member of the diplomatic staff in the country. LEGATS form the backbone of all international FBI work, and form the distributed capacity U.S. law enforcement. In a recent budget request the FBI explains:

> LEGATs are the forward element of the FBI's international law enforcement effort and often provide the first response to crimes against the U.S. and its citizens that have an international nexus. The counterterrorism component of the LEGAT Program is comprised of SAs [Special Agents] stationed overseas who work closely with their foreign counterparts to prevent terrorism from reaching

---

[378] Mueller 2012.
[379] Mueller 2011.
[380] The first LEGAT was in Mexico City.

into the U.S., help solve crimes, and assist with the apprehension of international terrorists who violate U.S. laws.[381]

As an FBI intelligence sharing report states: "LEGATs are familiar with investigative rules, protocols, and practices that differ from country to country." They are like a beat cop who develops familiarity with the community she traverses. LEGATS "are thus well-positioned to analyze and disseminate the intelligence that directly impacts the US national interests both domestically and abroad."[382]

Although LEGATs are not new, they have not always been numerous or important. "Since its inception in the years preceding World War II, the legat program had been mostly a quiet backwater in the Bureau, its members known internally as the Mormon Mafia, because the agents selected for the program were disproportionally Mormon."[383] In 1993, there were 21 LEGATS, eight of which were outside Western Europe and North America, but none were in the Middle East or Africa.[384] By 1998, international offices had been opened in Germany, Pakistan, Poland, Saudi Arabia, Estonia, Israel, Argentina, the Ukraine, Egypt, and South Africa.[385] Despite some international growth during the mid-90s, the FBI's international mission suffered from a lack of funding and was not warmly embraced by all. Resistance came from the State Department (e.g. diplomatic concerns), Congress (e.g. budgetary concerns), the CIA (e.g. turf issues), and sometimes even the FBI itself.[386]

Early LEGATs focused on counterintelligence investigations, but when Louis Freeh took over in 1993 criminal investigations received more attention.[387] By the time

---

[381] U.S. Federal Bureau of Investigation 2013a, 4.10.
[382] U.S. Federal Bureau of Investigation 2011a, 13.
[383] Graff, Threat Matrix (212)
[384] Graff, Threat Matrix (212)
[385] Graff 2011, 253.
[386] Ibid., 253–4.
[387] Fowler 2008, 112.

the September 11 attacks happened, the FBI had LEGATs in over 40 countries.[388] Priorities quickly changed to counterterrorism, and the FBI presence overseas grew. Today the FBI has 63 offices overseas, and 76 other sub-offices, "providing coverage for more than 200 countries, territories and islands."[389] What might have been a "backwater" prior to the new millennium is now among the FBI's priorities.[390]

Counterterrorism remains a priority for the FBI. In its budget request for 2013, the FBI writes that, "Terrorism, in general, and al-Qa'ida and its affiliates in particular, continues to represent the most significant threat to the country's national security."[391] The FBI spends at least $3.3 billion a year on counterterrorism and counterintelligence (a number which does not reflect spending from the intelligence side of the FBI's work). The FBI now takes its international work seriously.

The FBI's international operations have changed since 9/11. The most obvious change is the focus on terrorism, and the shift from investigating after-the-fact incidents to also gathering intelligence to stop terrorism. Along these lines, cooperative efforts have broadened. Instead of focusing on bringing suspects to the U.S. for prosecution, the FBI offers more comprehensive assistance to support *other countries'* efforts against terrorism and transnational crime. Moreover the FBI will "routinely deploy agents and crime scene experts to assist in the investigation of attacks."[392]

Legats took on a more instrumental role in *i-veillance* after 9/11. In a 2002 memo, the U.S. Attorney General directed FBI attachés to "obtain on a regular basis the fingerprints, other identifying information, and available biographical data of all known or suspected foreign terrorists who have been identified and processed by foreign law

[388] Graff 2011, 256.
[389] See the FBI's International Operations homepage.
[390] It should also be noticed that international travel is common for the Director of the FBI. The role has taken on a diplomatic responsibility.
[391] U.S. Federal Bureau of Investigation 2013a, 1.2.
[392] U.S. Federal Bureau of Investigation 2011b.

enforcement agencies."[393] Explaining what progress has been made in international operations ten years after 9/11, the FBI underscored that this information was indeed being collected from "from cooperative international exchange programs [and] the legats."[394]

Legats are particularly empowering for *i-veillance* because all legats "are linked electronically to the FBI network and all commuications" involving legats are accessible through FBI information systems.[395] *I-veillance* by legats serve not only the FBI, but the broader intelligence community. The FBI's International Operations Division IOD "and the Legat program disseminate more intelligence information reports to the IC than the next highest producing field divisions combined."[396]

As an indication of the volume of information involved, the best proxy that is publicly available might be the number of investigative leads the attaché offices cover. In 1998 legats handled just over 20,000 leads. By 2002 that number more than doubled to over 53,000 leads.[397] This number is likely to underrepresent how much *i-veillance* the FBI conducts abroad—and there are two reasons why. First, investigative leads are requests from FBI offices back in the U.S., and therefore do not capture investigative assistance requested by countries hosting the legats. Second, the number fails to capture the unsolicited *i-veillance* that FBI attachés conduct by their mere presence abroad.

---

393 In addition it stated: 'The FBI shall also coordinate with the Department of Defense to obtain, to the extent permitted by law, on a regular basis the fingerprints, other identifying information, and available biographical data of known or suspected foreign terrorists who have been processed by the U.S. Military.' Ashcroft 2002.
394 U.S. Federal Bureau of Investigation 2011b.
395 Fowler 2008.
396 U.S. Federal Bureau of Investigation 2012a, 25.
397 U.S. Department of Justice, Office of the Inspector General 2004, 6.

LEGAT Vignettes

The FBI does some self-reporting on its LEGAT activities. Looking at press releases, interviews, and testimony (a) shows how the FBI perceives its work abroad, and (b) highlights how liaison performs an *i-veillance* role.

According to the special agent detailed in Jordan (the LEGAT was established in January 2001), the FBI tries "to meet the intelligence and law enforcement needs and requests of our host country, and we try to meet those same needs of our agents back home and our partners in the intelligence community. We serve as a conduit."[398] The quote underlines two roles of the FBI—assisting in overseas investigation and receiving information for use in U.S. investigations. "Meeting the needs of our host country" does *not* include making arrests. Rather, it entails *i-veillance* and additional investigative assistance.

An agent working in the Cambodia Legat, Laro Tan, explains "We don't have the authority to make arrests or track leads ourselves in other countries, so we go to our partners and ask for help. In return, we offer assistance in their cases with U.S. connections and encourage their agencies and officers to take advantage of the many training programs we offer." Tan further explains that the reason he is there is "to get to know my colleagues personally, to be a bridge between our countries."[399]

The language used here suggests additional *i-veillance* roles of FBI LEGATS. First, agents of the host countries are used to follow leads from FBI *i-veillance*. Second, training is highlighted. As argued above, when the FBI trains foreign officials, it helps develop a common lens for *i-veillance*. "Getting to know one's colleagues" helps grease the channels for cooperation more generally and *i-veillance* more specifically.

---

[398] FBI Press Release 2009.
[399] FBI Press Release 2007.

Other interviews highlight both the training and information sharing elements of FBI LEGATS. The Legal Attaché in Freetown, Sierra Leone said, "Being here, we can help both nations organize their police agencies to combat the most serious and pervasive threats…and they can help us better understand and stop threats that might migrate to U.S. shores."[400]

The FBI has a robust presence in Kenya. According to the attaché, if something happens in Kenya the FBI "can respond immediately with a full range of Bureau expertise." The FBI became quite involved when in 2013 al Shabaab members attacked the Westgate Mall attack in Nairobi. At the height of its investigation, the FBI had over 80 people assisting there.[401] While the FBI is assisting within investigation for purposes of prosecution, the FBI is also playing an *i-veillance* role to uncover "the entire network" involved in the attack.[402]

The FBI LEGAT in Kenya trains their counterparts in *i-veillance* methods "such as fingerprinting, cyber investigations, evidence collection, intelligence analysis, interview techniques, and major case management."[403] Again, according to their attaché, in recent years "the Bureau has conducted more than 40 training sessions in Kenya and has trained more than 800 individuals."[404]

In 2011, the FBI and Ukraine's security service busted a major cybercrime ring. Information exchange was crucial to the investigation. The FBI attaché was reportedly "directly involved in the investigative actions carried out in Ukraine."[405]

The LEGAT in Dakar works with counterparts from Senegal, Cape Verde, Bambia, Bissau-Guinea and Gabon. Like all LEGATs the office covers terrorism, but the

[400] FBI Press Release 2006.
[401] U.S. Federal Bureau of Investigation 2014b.
[402] Ibid.
[403] U.S. Federal Bureau of Investigation 2014a.
[404] Ibid.
[405] Stratfor - Interfax Ukraine 2011.

Senegal office is also heavily focused on drug trafficking. West Africa is a major stopover point for drugs from South America to Europe, and the LEGAT is active in countering Colombian drug organizations working Western Africa.[406] The LEGAT is also helping countries in the region set up "an automated fingerprint search capability."[407] This echoes the "capacity building" function of databased *i-veillance* discussed in the previous chapter.

Legal attachés can work as an *i-veillance* assemblage as they network with other attachés from their own and other countries. For example as the 2013 hostage crisis unfolded at an gas field in Algeria, the FBI mobilized "a web of partners in place to help work the case."[408] The FBI's "network extended from [the legat in] Algiers [...] to the FBI's office in Copenhagen, Denmark." While the Algerian presence was clearly relevant, the Copenhagen attaché, who is responsible for liaison throughout the region, worked closely with Norwegian authorities. Norway is home to the owner of the facility being involved in the crisis.

According to the attaché in Copenhagen: "To get a clear picture of what was happening on the ground, the FBI and Norwegian police needed to combine our respective resources. Throughout the crisis, we shared information about what we saw and heard. It's a great example of how we use our legat network to work with a partner in our area."[409] Here we see resolution effects coming into play. Combining *i-veillance* resources provides a clearer picture. The FBI write-up goes on to explain the benefits of sharing and reciprocity. "The case illustrates how relationships forged by our overseas outposts can yield unforeseen dividends. [...] If dots from a U.S. case lead to any of the

---

[406] FBI Press Release 2008.
[407] Ibid.
[408] U.S. Federal Bureau of Investigation 2013b.
[409] Ibid. These specific remarks were made by Special Agent Johannes Van Den Hoogen.

Nordic countries, the FBI can call on its partners; if the dots lead back to the U.S., agents in field offices can assist by running down leads."[410]

The FBI's own reporting on the Copenhagen liaison offers up another way in which liaison can foster *i-veillance*. In Denmark, where Legat Copenhagen was established in 1999, local police know they can rely on the FBI's extensive network if a case reaches beyond its borders. "We take advantage of your presence in different countries," said Jens Henrik Højbjerg, commissioner of the Danish National Police, which covers the country's 12 police districts as well as its intelligence service. "We can take advantage of your network, your relationships, your contacts. And this is very, very helpful."[411]

Here the head of the Danish National Police explicitly states that police in Denmark use the FBI's network and resources. The FBI's own language leading up to the commissioner's quote (i.e. the preceding sentence) apparently endorses that this is the case. This shows how complex *i-veillance* relationships can be. On the one hand it might seem that the FBI"s network is for the FBI to acquire information it needs. However we see how that same network can be tapped by trusted partners to amplify their own *i-veillance* needs. But this doesn't mean that when Denmark (or some other country) uses the FBI network that it *exclusively* serves that country's interests. The FBI can always say "no" to Danish requests. Therefore when the FBI opens up its own network it is likely to serve the *i-veillance* interests of all.

More direct information sharing links are suggested in internal communications of the global intelligence firm Stratfor leaked by Wikileaks. According to an email written by analyst (and Stratfor's Vice President of Intelligence) Fred Burton:

---

[410] Ibid.
[411] Ibid.

> The FBI Legal Attaché office in London is already helping [the UK's MI5] ([with] analysts, forensics and computer work.) There is a direct drop/dedicated line from the FBI to MI5 inside the Embassy. The suspects are being ran through the FBI's "IIIA" [intelligence database] for any links and intel gaps. Next steps are joint surveillance ops in country. Unprecedented. OSS did this during WWII. The FBI has an Assistant Director level man in charge in the UK.[412]

The quote is referring to work between the MI5 and FBI in the aftermath of a foiled UK-based plot to blow up multiple airliners. It was no secret that the FBI was working with MI5 on the investigation.[413] But cooperation comes in degrees. If the Stratfor claims are accurate, the level of cooperation outlined is deep. For *i-veillance* in particular the email suggests there is a direct line between MI5 and the FBI to check the former's intelligence against the latter's. In this case both MI5 and FBI surveillance interests are bolstered insofar as they are working on cases of mutual interest. The implication of "joint surveillance operations" for *i-veillance* is even more clear. The specific implementation cited above would involve FBI agents working in the UK to surveil terrorist suspects.

A final example of deep cooperation is the FBI involvement in the investigation of the 2008 terrorist attacks in Mumbai India. According to testimony, the FBI was on the scene in Mumbai before the attack had even ended. The FBI had "unprecedented access to evidence and intelligence" which allowed them to interview over 70 individuals and get forensics on the explosive devices used in the attack.[414] Furthermore, the FBI "collected, analyzed, and disseminated intelligence to [...] partners at home and abroad—not only to determine how these attacks were planned, and by whom, but to ensure that

---

[412] Stratfor - Fred Burton 2006.
[413] DHS Press Release 2006.
[414] McJunkin 2009.

if a second wave of attacks was planned, we had the intelligence to stop it."[415] FBI testimony about its involvement concluded with the following.

> In summary [...] as the threats to our nation and our allies become ever-more globalized, the FBI is expanding our collaboration with our international and U.S. law enforcement and intelligence partners to prevent terrorist attacks and to assist in investigating them when they do occur. We will continue to build on these relationships to advance the FBI's national security mission. And, as we have done with the Mumbai attacks, we will continue to analyze and share lessons learned from these investigations to help prevent future attacks at home or against U.S. interests abroad.[416]

Conclusion

Liaisons serve multiple functions. Representatives abroad can take advantage of information sharing arrangements, they can simply observe, they can be brought on to help with cases. Attachés abroad act as a kind of beat cop. They know the area and the "residents." Attachés "are familiar with investigative rules, protocols, and practices that differ from country to country. They are thus well-positioned to analyze and disseminate the intelligence that directly impacts the US national interests both domestically and abroad."[417]

Attachés can also push information out to foreign counterparts. This last role, which might not be an obvious surveillance function, is perhaps the most surprising takeaway from this chapter. If a state trusts another state enough it can forward information so that the partner state can act on it. This is an intriguing way for a surveillance assemblage to work. Instead of taking-in information from other agents, information is pushed out for those agents to enhance their surveillance efforts.

Furthermore, weaker states that are part of the U.S. surveillance assemblage might be able to strategically use the U.S. to serve *their* interests. As the Copenhagen

---

[415] Ibid.
[416] Ibid.
[417] U.S. Federal Bureau of Investigation 2012a, 25.

example suggests, Denmark relies on the FBI's network to pursue cases that extend beyond Denmark. This suggests that even sensitive information networks run by the U.S. can be leveraged (to some degree) by trusted partners. The U.S. *i-veillance* assemblage may not be totally within U.S. control.

States also build *i-veillance* capacity when they deploy personnel to train security officials of other states. The logic here is straightforward. A common education creates the ability for state officials to communicate with each other (and share information) and greases the wheels for cooperation. Moreover, the training state reproduces a certain way of seeing in the other state.

Chapter 7: Theoretical Implications

Having unpacked the institutional and legal conditions that underpin *i-veillance* in Chapter 3 and the material practices—the use of sensors—that actively conduct *i-veillance* in Chapters 4-6, we can begin to tease out theoretical implications. The restricted focus on U.S.-led efforts demonstrates (i) a diversity of practices (ii) that implicate many states and (iii) citizens worldwide. *I-veillance* is international, but does that matter for IR theory?

Surveillance and the state are intimately linked in three ways. First, surveillance over citizens for security purposes is a privilege that states enjoy domestically. State surveillance is a necessary component of the state's claimed monopoly of force. The state must know when, where, and what people are doing if it wishes to act. Surveillance is necessary to state administration more generally. As such surveillance is part of the internal sovereign authority of states, and that authority "stops at the water's edge." Second, surveillance is also an activity that is deeply implicated in state-society relations. Domestically, the extent of state surveillance is negotiated with a state's citizens. Just as a state limits its own violence at home, it also limits surveillance.[418] When it comes to surveillance, state and citizens balance security with privacy. Finally, while surveillance can be thought of as a tool states use to 'see', surveillance is more deeply constitutive of

[418] In political theory debates about limits to state intervention in society apply to *all* intrusive state practices, not just lethal ones.

the state's vision. States "see" through the representations which surveillance affords.[419] This is most evident in the case of drones. Commanders literally see the battlefield differently and therefore think about war differently. Examples abound.[420] An official at the Department of Homeland Security told me that in an ideal world DHS could slap a risk-assessment on every individual. He saw through risk.[421]

The fact of *international* surveillance practices may therefore have implications for what it means to be a state and what it means to be an individual subject to this form of state power. This leads to two specific questions. Is an essential state practice is being internationalized? And, are there any significant implications for the individuals on the receiving end of such surveillance? In this chapter I focus on the former question. In the concluding chapter that follows I think through the latter.

The chapter proceeds as follows. First, I describe the ideational backdrop that helps make sense of the growth of *i-veillance*. After 9/11 extant antiterrorism norms and practices were amplified and massaged into new forms. Individuals are now viewed as capable threats, and states have a responsibility to prevent any such threat from actualizing. As such *i-veillance* in particular is not only a rational security practice, but it is *appropriate*. Facilitating the pursuit of *i-veillance* are new roles of "counterterrorism partners" in international security. Taken together these ideational changes reflect an international purpose of fighting terrorism. Second, I unpack the consequences for states. I argue that structure and processes constitutive of states' security function are being internationalized. This is occurring as infrastructure gets internationalized and as processes that implicate control, society, and territory become internationalized. Finally,

---

[419] For work on the connection between visual representations and security/militarization see Campbell 2007; Campbell and Shapiro 2007; Andersen and Moller 2013.

[420] For a great read on how representations affect the way security professionals think, see Cohn 1987.

[421] Interestingly he said this while making the point that knowing a person's nationality isn't that useful for DHS. A person's origin just doesn't tell you that much whether he is a threat.

I argue that the internationalization of purpose and security mentioned above suggest an internationalization of state authority with respect to counterterrorism.

An Internationalization of Purpose

Before I explore the theoretical implications of the previous chapters, I need to articulate how norms, interests, and identities pertaining to counterterrorism have changed. Taken together these changes demonstrate that states share a common purpose in fighting terrorism through *i-veillance,* a purpose which helps give meaning to the more substantial changes I mention in the next section.

To describe the ideational changes I lean on both rationalist and constructivist insights.[422] My approach is thinly rationalist in that much of the activity outlined in the previous chapters can be partially explained as states pursuing parochial security interests in fighting terrorism. Many of these micro-decisions (e.g. the U.S. signing an information sharing agreement with France) may very well be understood as a rational decision to help prevent terrorism. But, and here is where the constructivist insights enter, it is by virtue of states simply pursuing these interests in widespread fashion that new norms and practices grow and calcify. This reflects the familiar constructivist insight that agents (re)produce structures and vice-versa.

Because I am interested in change I emphasize process to capture what Anthony Giddens refers to as 'structuration'—the ways in which actors, through acting, draw upon and reproduce structure.[423] "The structural properties of social systems exist only in so far as forms of social conduct are reproduced chronically across time and space."[424] *I-veillance* is itself a varied practice occurring in heterogeneous contexts. More specifically

---

[422] Fearon and Wendt 2002 offer a great discussion of the two approaches as they relate to one another.
[423] Giddens 1984 Ch 1 in particular.
[424] Ibid., xxi.

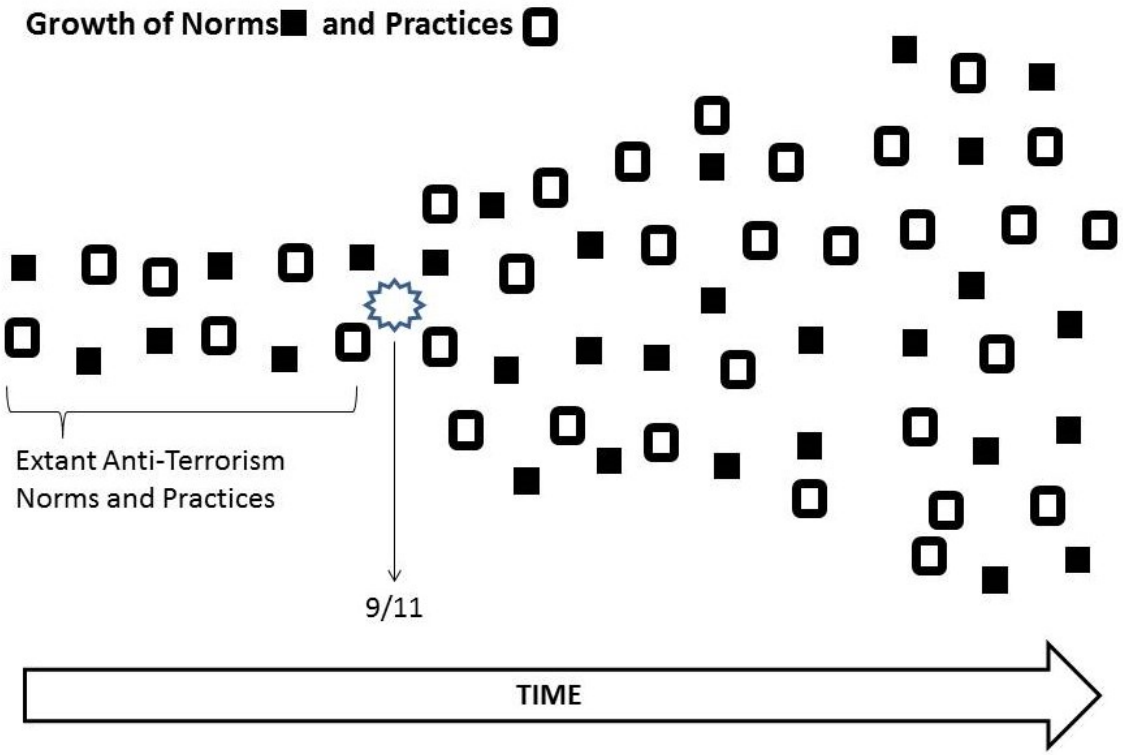
the variety of U.S. and IO practices documented in previous chapters suggest that *i-veillance* is an important international practice that structures international security. The result is that today there are strong norms which call for *i-veillance* as an appropriate response for states wishing to take terrorism seriously. *I-veillance* is not only desirable, but it is a practice befitting responsible stakeholders in international security.

What enabled the post-9/11 counterterrorism practices and norms to grow, and to make room for *i-veillance*, were (a) preexisting anti-terrorism norms and practices, and (b) the enterprising push by the U.S. to ramp up and prioritize anti-terrorism norms and practices after 9/11. Prior to 9/11 there existed international anti-terrorism norms and international counterterrorism practices. 10 universal counterterrorism legal instruments (of the current 14) had already been adopted under UN auspices. Many states had a lot of experience with violent organizations. The IRA was busy in the UK, Palestinian organizations were busy in the Levant, etc. However, in terms international security, these norms and practices were muted and certainly not prioritized. This generic anti-terrorism prior to 9/11 was not driving national security. It was a relatively inert part of the ideational underpinnings of international security.

Nevertheless, the existence of this generic anti-terrorism provided a hook, a status quo from which to build after 9/11. The al Qaeda attacks of 9/11 was, and remains, the most significant international terrorism event the world has ever seen. It catalyzed the U.S. and other key, powerful states (UK, France, Russia) to focus like never before on fighting terrorism. The U.S. built off the previously existing anti-terrorism norms and practices. As a result the U.S. could emphasize new and related norms and stress an anti-

terrorism imperative.[425] The U.S. could also ramp up previously existing practices of capacity building, information sharing, and law enforcement cooperation. Importantly, the U.S. (and other states) didn't have to do anything radically new. Many of these practices pre-dated 2001, but they were linked up *a fortiori* with the anti-terrorism emphasis. Figure 2 is a caricature of the idea.

Figure 2. The growth of anti-terrorism norms and practices



More specifically I want to highlight two ideational developments directly related to *i-veillance,* and together show that there exists common purpose in fighting terrorism. The first is the norm that effective counterterrorism requires international cooperation. The second is the internalization of interests and the development of role-identities that

[425] Cox 2001; Cox speaks of path-shaping (as opposed to path-dependency), and credits the idea to Torfing 1999.

pivot on this norm. All "responsible states" have a duty to take counterterrorism seriously. These ideational developments occurred via three routes: strategic interaction, inter-state socialization, and sub-state socialization.[426]

First, change was facilitated as states made strategic security decisions which were reliant on the extant security norms mentioned above. Because counterterrorism security discourses could draw upon entrenched state-centric security concerns, new counterterrorism practices would not encounter much resistance from security practitioners. Moreover, in something of rarity for security policy, counterterrorism policies don't come at the expense of other states' security (or their perceptions thereof). Such a security dilemma can be avoided because the targets of these practices are individuals and not states. Therefore any counterterrorism security gains by one state is not likely to be viewed as directly threatening to the security of other states, and cooperation on an anti-terrorism agenda is less controversial. Possibilities for cooperation and the development of new practices were made even more likely in the post-9/11 world in which states were not preoccupied by the prospect of interstate war.

The specific way the U.S. expanded counterterrorism policies was through bi- and multi-lateral interactions with other states. This leads to the second way in which norms, interests and identities evolved—interstate socialization. State *behavior* may change as a result of socialization,[427] but so too may their *interests* and *identities*.[428] The actual processes of socialization may be varied. States may get socialized into a pattern of action

---

[426] Social conceptions of identity can be thought of in terms of varying relationships between the Self and Other. 'Collective identity' entails identifying cognitively and empathetically with 'the Other'. (See Wendt 1999, 224-33.) Collective identity formation is fostered by certain 'intersubjective structures,' 'systemic processes' such as interdependence and sharing a common 'other', and through repeated behavioral and rhetorical practices. Wendt 1994, 388–91 Although my analysis does not trace these mechanisms outlined by Wendt, the conditions of each are favorable to the type of change I describe.

[427] Waltz 1979, Ch 4.

[428] Wendt 1992; Wendt 1999, 170, and see Ch. 7 for an evolutionary perspective.

through (asocial) internal processes of cost/benefit analysis. More *social* forms of socialization occur through social influence and persuasion.[429] Socialization—and the formation of unreflective habits—might occur through sheer "repeated exposure to how things are, and are not done."[430]

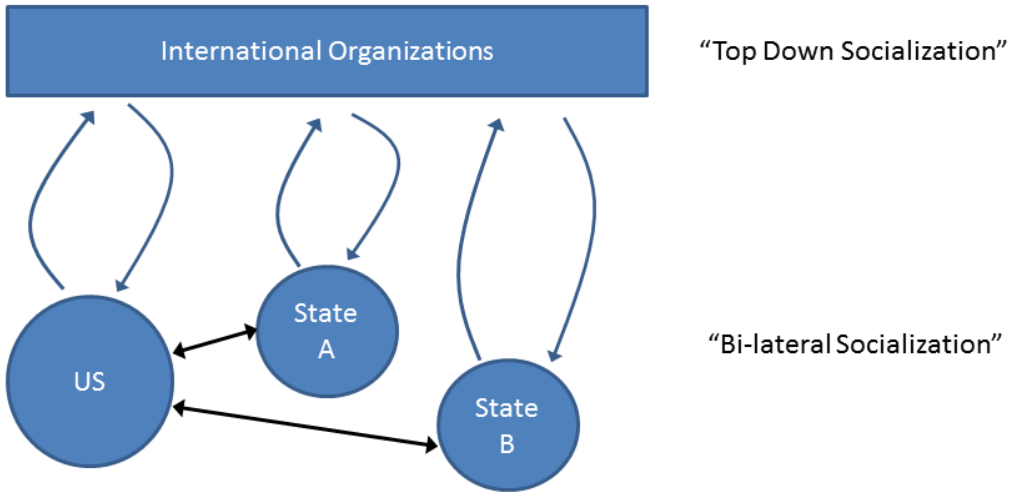
The evidence provided in this dissertation suggest that since 9/11 states have been socialized into *i-veillance* through two vectors at the international level—interactions with international organizations and bilateral interactions. (See Figure 3.) International organizations acted as "organizational platforms"[431] encouraging and requiring their members to cooperate on surveillance to fight terrorism. The G8[432] and major regional IGOs such as the EU,[433] the OSCE,[434] the African Union,[435] the Organization of American States,[436] the Asia-Pacific Economic Cooperation,[437] all address *i-veillance* in some way or another.[438] The UN in particular *requires* states to work on their counterterrorism capacity. Security Council Resolution 1373 reads that states "shall" develop counterterrorism capabilities to prevent, interdict, and prosecute terrorism. While not explicitly requiring surveillance by name, an effective CT capacity presumes an effective surveillance capacity. Resolution 1373 goes on to "call for" "intensifying and accelerating the exchange of operational information, especially regarding actions or movements of terrorist persons or networks; forged or falsified

---

[429] Johnston 2001.
[430] Which may lead to habit. Hopf 2010.
[431] Finnemore and Sikkink 1998, 899.
[432] The G8 set up a Counterterrorism Action Group (CTAG) and the Lyon-Roma Anti-Crime and Counterterrorism Group
[433] Through Europol and Eurojust in particular
[434] The OSCE Action Against Terrorism Unit
[435] The African Union Counter Terrorism Framework
[436] Inter-American Committee against Terrorism
[437] See the work of their Counterterrorism Task Force. APEC also encourages members to submit reports on progress they've made on counterterrorism reforms.
[438] At the very least, there is a common emphasis on information sharing. Capacity building assistance is also mentioned frequently. The EU is the most advanced of all of these in terms of cooperative *i-veillance*.

travel documents; traffic in arms, explosives or sensitive materials; use of communications technologies by terrorist groups."[439]

Figure 3. Socialization into *i-veillance*



The extent of bilateral socialization is clear from the previous chapters. From the myriad practices already discussed, I highlight one here. Recall the bilateral "HSPD-6 Agreements" that the U.S. has signed with over 40 countries. These agreements allow for the exchange of terrorist watchlist information. These agreements, the content of which remain secret, are the product of serious negotiation because they implicate privacy concerns. Leaked diplomatic cables regarding HSPD negotiations between U.S.-Sweden demonstrate the controversy. This suggests that growth of HSPD-6 agreements was not a *fait accompli* after 9/11, but rather required a social process of negotiation. It was an evolution of an existing norm of information sharing.

The final way in which these ideational changes occurred was through sub-state socialization between the state and networks of government officials and epistemic

[439] United Nations Security Council 2001.

communities.[440] The previous chapters were replete with examples of the former. The Intelligence Community, DHS, State Department, and most importantly the FBI worked with their counterparts abroad to facilitate information sharing on individuals. Anne Marie Slaughter describes these types of government networks as tackling important problems of global governance such as terrorism.[441] The officials that form these networks pursue similar interests (countering terrorism) with similar tools (information sharing), and the more they interact the more they align not only on the broader norm that cooperation is a must for counterterrorism, but also the specific norm that *i-veillance* is part of that cooperative package.

Working alongside these government officials has been an epistemic community of experts on information technology and business processes that influence *how* governments should share information. The turn to epistemic communities for advice is evident in how the U.S. sought new best practices for information analysis and sharing. For example the U.S. government turned to the non-profit group "the Markle Foundation" and their "Task Force on National Security in the Information Age" to help establishes practices and standards for information sharing within the Intelligence Community and with 'foreign partners.'[442]

These three processes—strategic decision making and the two forms of socialization—have given shape to the general norm that states should cooperate in counterterrorism. While the processes reflects the familiar dance of agent-structure co-constitution, insofar as there is a "norm cycle" involved, it doesn't neatly fit the pattern

[440] Haas 1992.
[441] Slaughter 2009.
[442] U.S. Government Information Sharing Environment n.d.

of: emergence-cascade-internalization.[443] Rather my story suggests a building-off from extant anti-terrorism norms (that began emerging as early as the end of the 19th century, but more thoroughly in the 60s) with a greater emphasis on international cooperation and information sharing.

The *way* in which states are being socialized suggests a more specific form of the "thou shall cooperate" norm. The *i-veillance* practices that have been cataloged in previous chapters fall into two general categories—information provision and domestic capacity. Both are frequently treated as a responsibility owed to the international community. A more specific form of the norm, therefore, would be: *States ought to (a) to share information with international partners, and (b) have the domestic capacity to accomplish that sharing, and generally keep a cap on potential threats at home.*

As mentioned above, ideational changes post-9/11 include changes in interests and identity, rather than simply behavior.[444] The evidence I've provided most clearly supports the claim that state interests have changed. Across the board states are showing an interest in developing a strong domestic counterterrorism capability which includes an *i-veillance* component (i.e. an international surveillance function). It is becoming something of a commonplace. Moreover, non-covert *i-veillance* is pursued actively by states like the U.S. with no real resistance by other states (though, not without negotiation).

Both the "content" of the anti-terrorism norms and the "actors" that promote them also suggest the internalization of interests. First, as I mentioned above, the norms in question are security norms that dovetail easily with past practices. *Prima facie* there

---

[443] Finnemore and Sikkink 1998.
[444] Wendt 1999 Ch 3.

is nothing too controversial that deviates from the status quo. I am not arguing that states have adopted these interests *de novo*. Rather the interest in cooperative *i-veillance* is a variation on other deeply held interests. Second, anti-terrorism norms are proliferating via state elites and security professionals with similar interests in preventing terrorism. Among such a group, there is little reason to think they would be employing norms strategically.[445] (They are certainly not being pressured by a third party as in the case with promotion of norms by transnational activist networks.[446]) The heavy involvement of IOs is also telling. If we see an IO promoting a norm it is a signal that the members (or at least the most powerful among them) support it. If we see multiple IOs supporting the same norm, it is even more suggestive.

The *sources* of my evidence also provide supporting evidence that *i-veillance* is a desired practice. For instance, many of my sources take the form of internal budget documents and government reports. The audience is not only domestic, but very narrow. The language is bureaucratic. All of this suggests that the belief in the appropriateness of *i-veillance* is internalized and not just mobilized rhetorically. Moreover the language of "partners," "sharing," "capacity building" are not *my* analytical categories, but rather reflect the language being used by actors themselves.

It is more difficult to make a case here that states are adopting new *identities*, but I think the evidence is on my side. The operative identities in this case would be that of "counterterrorism partner" in the international community. This is not a collective identity, but rather reflect "role identities" that pivot around normative expectations

---

[445] The reader may object strongly here suggesting that many policies (foreign and domestic) have been pursued under the guise of counterterrorism. I think this clearly applies to some policies, but not to the *i-veillance* practices I've analyzed. Most of the practices—e.g. FBI liaison abroad—aren't controversial when taken by themselves (unlike, say, the US Patriot Act). Moreover because we have elites selling ideas to elites, it is unclear why they would need to resort to rhetorical slight of hand.

[446] Keck 1998.

about how to stop terrorism.[447] As such the role identities admit of functional differentiation in that some partners are responsible for different contributions to maintaining international security. For example: stronger states tend to help weaker states build capacity; weaker states allow for that assistance and maybe even a foreign presence to help deal with a specific problem (e.g. U.S. aerial surveillance throughout central Africa); all partners should share information, though some partners (the U.S., the EU) are better equipped to process information than others. The point is, increasingly what it means to be a responsible state is to be a counterterrorism partner carrying out CT obligations. *I-veillance* is one of the requirements of a robust CT capability. The fact that such obligations are articulated in international instruments, in particular UN documents, suggests these roles are common knowledge among states (even if they are not embraced by all actors).

The norms and practices discussed above have helped construct new norms, interests, and identities pertaining to counterterrorism. *I-veillance* is now part of the warp and weft of counterterrorism. Having outlined the rough process behind this result it clears the way to thinking through the implications.

An Internationalization of Security

As I have already argued, state surveillance practices are a necessary component of the state's domestic coercive and administrative monopolies. From the state's perspective surveillance is a prerequisite for governing. From citizens' perspectives surveillance is potentially invasive. Between the state and its citizens surveillance is a negotiated practice that is of tremendous importance to domestic politics. Surveillance is part of the state's treasured internal sovereignty.

---

[447] Wendt 1999, 227–9.

However as this dissertation has documented there are myriad examples of surveillance by one state on the citizens of another. Moreover, international surveillance practices have been adopted as an *appropriate* security measure against individuals. What effect is that having on this state monopoly? Is it being internationalized?

The answer is yes. I make the argument in two ways. First state infrastructures of surveillance are being internationalized. Coercive structures that once operated primarily in the domestic realm are increasingly crisscrossing borders. Second, state *processes* of surveillance are also being internationalized. Not only is the practice of surveillance itself being internationalized, but so too are processes of territoriality and state-society interaction that accompany surveillance practices.

Before turning to my main argument I briefly review some of the extant literature on international state formation. This will help situate my argument and distinguish it from others.

International State Formation

When it comes to the international state formation (ISF) literature, there seem to be three categories of argument—economic, security, and identity. The first branch of ISF theory tends to focus on the political implications of the increasing concentration and internationalization of capital and economic processes more generally. For instance, much of the ISF debate in the late 60s and early 70s "focused on the effects of international capital on national states or on the question of whether national states will be superceded by an international state as capital loses its national form."[448] Sol Picciotto and Jim Glassman provide more recent examples of scholarship in this vein.

---

[448] Cain 1983.

Picciotto is interested in extraterritorial economic regulatory jurisdiction[449] and how the internationalization of capital affects the internationalization of state structures.[450] When Picciotto refers to the internationalization of state structures, he is referring to state structures which are increasingly oriented internationally as well as state functions which are coordinated internationally through organizations such as the IMF, World Bank, and OECD. Likewise, Jim Glassman defines the internationalization of the state as "a process in which the state apparatus becomes increasingly oriented towards facilitating capital accumulation for the most internationalized investors, regardless of their nationality."[451] The focus here is on how elites representing certain fractions of capital work within state institutions to pursue policies in the service of international, not national, capital accumulation.

Another scholar focusing on the economic role of states, but from a different angle, is Roland Paris. Paris argues that given how important collecting taxes to the development of the state, we should expect the globalization of taxation authority in order to claim revenue from electronic commerce that is currently under-taxed.[452] Here Paris is focusing primarily on the internationalization of the state in terms of its legal order as it concerns taxation, though he does make reference to international structures which would be necessary to administer such law.

The second class of ISF arguments revolve around security. Examples of this literature include the nuclear "one-worldism" of John Herz and Hans Moregenthau.[453] Herz argued that states need to be able to militarily maintain territorial 'impermeability', and that nuclear weapons made this task impossible. The modern state has thereby

---

[449] Picciotto 1983.
[450] Picciotto 1991, 47.
[451] Glassman 1999, 673.
[452] Paris 2003.
[453] As discussed in Deudney 2000.

become obsolete and political consolidation has become necessary.[454] Morgenthau agrees with the basic argument advanced by Herz but adds an additional touch of despair noting that the psychological, political and moral prerequisites for a world community are lagging the nuclear-material reality which makes such a community necessary.[455]

Christopher Chase-Dunn combines an economic and a security perspective in arguing for the necessity of a world state—not that it is developing or will develop.[456] He argues that another great power war is inevitable, and given the state of technology, such a war would be disastrous. A world state is therefore needed to contain the use of violence. Although capitalism has helped get the system this far, it is now a fetter to world-state formation (interstate systems are better for capital mobility and facilitates the manipulation of labor). Picciotto argues in a similar vein that international capital often prefers weak international state structures.[457]

Wendt's 2005 article on "Why a World State is Inevitable"[458] provides an argument that relies both on mechanisms of identity and security. His argument is that states seek recognition and can seek that recognition through violence. But as military technology becomes increasingly violent, the use of and potential for violence will be unbearable. This implies instability which can be addressed with more and more comprehensive communities of We-feeling, which culminate in a world state with a monopoly on the use of force. Following Weber, Wendt defines the state as "an

---

[454] Ibid., 19–20.
[455] Ibid., 20.
[456] Chase-Dunn 1990.
[457] Picciotto 1991.
[458] Wendt 2003.

organization possessing a monopoly on the legitimate use of organized violence within a society."[459]

Martin Shaw's *Theory of the Global State* is a large tract that, by Shaw's own account, is "ambitious in its range" and covers a lot of different ground related to ISF. Shaw argues that there exists a Western-global conglomerate of state power (not a proper World State) which exists by virtue of global layers of political power and global social relations. I cannot do justice to Shaw's work here, but it will be helpful to explain his concept of "the state" more generally. He builds off of Michael Mann's definition of the state as: "a differentiated set of institutions and personnel [...] embodying centrality [...] to cover a territorially demarcated area over which it exercises [...] some degree of authoritative, binding rule making, back up by some organized political force."[460] Shaw then notes that different types of political arrangements (for example, local municipalities) might fit this definition, so he includes an extra criteria: "to be considered a state, a particular power centre must be [...] *inclusive* and *constitutive* of other forms of layers of state power."[461] So, traditional nation-states are inclusive and constitutive of local municipalities. A global state must meet such a criteria. This particular criteria is institutional[462] (as Mann also acknowledges[463]).

The ISF work seems to lean on a conception of the state that identifies the state with structure. In the economic cases specific structures of the state are either turning outward or new international state structures are being (or will be) created, be it to facilitate the flow international capital or administer global taxation. The ISF literature tied to security likewise focuses on state structure. The focus on the monopoly on the use

---

[459] Ibid., 504.
[460] Shaw 2000, 188; Mann 2012, 55.
[461] Shaw 2000, 190.
[462] To be clear, I am *not* articulating Shaw's broader theory which itself relies on interactions between ideational and material factors.
[463] Mann 2012, 55.

of force requires a focus on institutional structure, though may also include focusing on social structures that make up authority relationships.

My approach is complimentary to other ISF scholarship, and is not meant to negate or trump other mechanisms behind ISF. I too will make an argument that relies on a state-as-structure conception, but I also make the argument via a state-as-process understanding of the state.

What is 'Internationalization'?

Before moving on, I want to be clear about what I mean by *internationalization*, and how I intend to demonstrate it. I start with a common understanding of the state in order to identify critical features widely regarded as constitutive of the state. I then look for state infrastructures and practices that underpin those features. If one state's infrastructure and practice links up with those of another state in order to perform the constitutive feature in question, then that would reflect *an* internationalization.[464] However, any one example would not really be worthy of a dissertation. What we should look for then is: multiple instances, across a variety of contexts, being sustained over time.[465]

To be clear, I am speaking of ***an*** internationalization. I am focused on a particular dimension of what the state is and does. I am not arguing that the whole state, soup to nuts, is being internationalized. And this is certainly not an argument that there exists a world state. (However, in the conclusion I suggest that there may be a dialectic

---

[464] State *A* could also extend infrastructure and practice abroad to perform the constitutive feature on behalf of State *B*. In most of the *i-veillance* examples in this dissertation, however, the infrastructure and practices of State *A* (e.g. the U.S.) and State *B* (e.g. India) link up in some way to serve the constitutive feature on behalf of both states.

[465] This reflects the relationalist search for causal mechanisms in social relations, a view in which "regularities in outcomes 'take the form of recurrent causal mechanisms which concatenate differently in various settings' and that 'recur in a wide variety of settings.'" Jackson and Nexon 2002, p5, citing Tilly 1999, 410

between security seeking states and technologically empowered rights-seeking individuals that works the system toward a more thoroughly international state.)

Defining the State

Even though "the state" is central to IR it doesn't get theorized too often. While scholars frequently note the importance of certain features of the state—they enjoy sovereignty, they seek security and prestige, they are more or less satisfied with the status quo, etc.— a tip-to-tail analysis of "the state" simply isn't necessary for most work.[466]

Because I am interested in thinking through the consequences of *i-veillance* for states (and people), I cannot avoid using conceptualization of the state. My approach will be relatively straightforward. I am not interested here in taking a stance on debates about the ontological status of the state or state agency.[467] After conceptualizing the state, I focus on two features of states that sustain such a conceptualization—process and infrastructure.

Scholars commonly connect "the state" to coercive capacity, territory, and sovereignty/authority. Michael Barnett writes that "State, territory, and authority are forever married in IR theory."[468] Biersteker avers in analyzing state, territory and sovereignty together.[469] Michael Desch writes, "Most scholars agree that the state is (1) a set of institutions, (2) placed in a geographically bounded territory, that (3) has a monopoly of rule within that area."[470] David Lake writes: "States are authoritative actors whose duly enacted policies are binding on their citizens and thus regulate how

---

[466] Though many constructivist and critical theory scholars would quickly point out that we should be watchful for how tacit assumptions regarding 'the state' lead to one analysis rather than others.

[467] See the "State as Person" discussion in the April 2004, issue 2, volume 30 of the *Review of International Studies*

[468] Barnett 2001, 49.

[469] Biersteker 2005.

[470] Desch 1996, 240.

individuals and the collective interact with other similarly bound societies. As sovereign entities, states possess ultimate or final authority over delimited territories and their inhabitants."[471] It is not uncommon, for example, for scholars to lean on a Weberian understanding of the state:

> [A] state is a human community that (successfully) claims the monopoly of the legitimate use of physical force within a given territory. Note that 'territory' is one of the characteristics of the state. Specifically, at the present time, the right to use physical force is ascribed to other institutions or to individuals only to the extent to which the state permits it. The state is considered the sole source of the 'right' to use violence.[472]

For the analysis that follows I start with Wendt's definition of the "essential state" (the state shorn of its socially constructed content) as "an organizational actor embedded in an institutional-legal order that constitutes it with sovereignty and a monopoly on the legitimate use of organized violence over a society in a territory."[473] This definition is, by design, fairly empty of specifics. It is a sort of plug-and-play conception of the state that gives the scholar flexibility to study the meaning of sovereignty, violence and territory in whatever way is appropriate to her object of study.

Our understandings of the state is made possible because states have infrastructures and processes that are common and important enough to be included in a skeletal definition like Wendt's. In what follows I look at the specific processes and infrastructure of *i-veillance* to gauge the consequences for the state. In as much as these infrastructures and processes are international—that is, shared and exercised by multiple states, then they represent an internationalization of that essential state feature.

---

[471] Lake 2008, 43.
[472] Weber and Owen 2004, 33.
[473] Wendt 1999, 213; For another interesting break down of how to conceptualize the state see Benjamin and Duvall 1985, 22–29.

State Infrastructure

State processes are often reliant on material features. The state has courts, police stations, ports of exit and entry, etc. These things you can actually point to.[474] This is infrastructure that helps shape the state and facilitate state practices. As state infrastructures penetrate throughout the state's territory, it results in what Michael Mann calls 'infrastructural power'—"the institutional capacity of a central state [...] to penetrate its territories and logistically implement decisions. This is collective power, "power through" society, coordinating social life through state infrastructures."[475] This is a power unique to states.

Not all *i-veillance* is infrastructural (e.g. like the *practice* of sharing information), and not all *i-veillance* infrastructure exists abroad (e.g. databases in the U.S.). However much of the sensors outlined in previous chapters are examples of U.S. infrastructure penetrating territory abroad. These are all infrastructures of control, deployed by the U.S., that surveil individuals in other states.

The infrastructures involved are very diverse and widespread. There are different modalities of *i*-veillance (for example remote sensing instruments and databases) that surveil different types of activity (movement of people within and between borders). Remote sensing aircraft are stationed abroad cover dozens of countries. FBI agents are housed in embassies in roughly 64 states giving the FBI nearly global coverage. Information systems, such as border control systems, are deployed abroad, again in dozens of countries. Domestic versions of this infrastructure would unproblematically be described as essential aspects of the state's internal coercive monopoly. But, of course, this infrastructure exists all over the world.

---

474 Even if we might not point to a police car driving down the street and say 'there goes the state!' Wendt 2010.

475 Mann 2012, 59; Mann 1989, 113; Soifer 2008.

The infrastructures are not *ad hoc*. Not only are the infrastructures being sustained over time, they are growing. And, most of the infrastructures I have examined in some sense "link up" with the similar-infrastructures of the other state. In these examples U.S. is not unilaterally conducting surveillance. It has required infrastructural support. (Clearly there are example of unilateral surveillance—such as recently disclosed NSA practices—but for the argument I make here this is an example of an international practice, not an internationalization of a state practice.)

Process

The intersubjective meanings of what-makes-a-state depend on a broader constellation of ideas which themselves depend on state practices. While one can do a strictly constitutive analysis, one can also focus on what states *do*. In this vein Patrick Thaddeus Jackson notes the importance of process in undergirding conceptualizations of the state. Comparing the state to a house he writes: "The snapshot from which a theorist might derive the constitutive properties of a house purposely abstracts from these processes of maintenance so that the analyst can focus on the purely conceptual and definitional aspects of the house as an entity."[476]

Here I want to focus on three elements of the definition (my snapshot) of the state. The state has:

- A monopoly on the legitimate use of organized violence
- over a society
- in a territory

For each of these elements, there are corresponding practices that make them intelligible as belonging to the state. If a state departed too drastically from these processes, it is unclear whether or not we would call it a state. Or, perhaps, we would simply have to redraw where that state exists. For instance if tomorrow the U.S. stopped

[476] Jackson 2004, 282.

exercising authority in Texas (something some Texans would like), and if this absence of authority persisted, we might redraw the map of the U.S. to exclude Texas.

I focus now on the *i-veillance* processes relevant to each of the three state-elements noted above: coercion, within a territory, over a people.

Process: Coercion

As I've already argued, the ability of the state to make any coercive interventions against individuals within its territory *presupposes* a surveillance capability. The state must know who is committing what infraction where before it can take further action. Moreover, just as the state has a claim to the monopoly of legitimate force, the state has a similar claim on the monopoly on the legitimate use of surveillance. Not only does the state *need* its own surveillance capabilities to carry out interventions (and any substantial act of administration), the state also legislates related matters of privacy.

The process of surveillance of individuals has been internationalized, although not completely and definitely unevenly. The previous chapters have demonstrated myriad practices—mostly driven by the U.S.—where multiple states cooperate in some fashion to conduct surveillance on individuals. The U.S. has: major information sharing arrangements with dozens of other countries; human liaisons funneling information back and forth; and physical infrastructure strewn abroad for the purposes of collecting information on individuals. Beyond the U.S. and its partners, states are increasingly sharing information via international organizations such as INTERPOL and FATF.

The variety and frequency of *i-veillance* practices suggest that the surveillance aspect of the state's domestic monopoly of force is being internationalized. However, it is not fully international, and the practices themselves are unevenly spread, revolving as they seem to around centers of power. A stronger internationalization will likely require

a moment when actors "yoke" together *i-veillance* practices to more explicitly rationalize them as an international project.[477]

Now, whether the *claim* to a surveillance monopoly has been internationalized is another story. One could pose the question: has any state alienated its sovereign right to determine whether other states can conduct surveillance in its territory? I don't imagine any head of state would answer "yes" to this question. However, one could also ask: Has another state (or institution) made a competing claim to contest the very idea of such a monopoly? Here I think the answer is "yes." Both the U.S. and the UN push norms, the content of which clearly refer to *some* surveillance activity as an obligation owed to the international community.

Process: Territory

Processes of *i-veillance* also have a significant effect on territory, and territory is inextricably linked with stateness. IR theory was once very susceptible to the "territorial trap" of assuming that states' rule is always territorial and fixed, demarcating zones of total mutual exclusion.[478] Recent IR, however, seems to be thinking about territory in more sophisticated and variegated ways. [479] On the one hand there is the common view is that states have "territorial rights" that bear on legal jurisdiction, access to resources, taxation and property, movement across borders.[480] In international politics Westphalian sovereignty suggests that a state's territory represents a zone of non-intervention in which other states must stay out of one another's internal business.[481] On

---

[477] Jackson and Nexon 1999; Abbott 1995.
[478] Agnew 1994.
[479] For a recent discussion on territory see the symposium in Issue 01, Volume 6 if International Theory. Banai et al. 2014.
[480] Simmons 2001, page 306 in particular; For more recent discussions of territorial rights see Banai 2014; Dietrich 2014.
[481] Krasner 2004.

the other hand there is a sense in which state practices help *produce* territory (not land, but territory).

To demonstrate how the state-territory security relationship is internationalized through *i-veillance* I make two arguments. The first focuses on the norms implied by *i-veillance* practices, and the second argument looks at how states produce territory through security practices.

In a narrow way, the use of drones and satellite surveillance by the U.S. suggests that the U.S. tacitly supports the following norm: if state X cannot monitor its territory in order to check threats against state X, then state X is justified in taking steps to monitor that territory. On the single dimension of surveillance for security purposes, this represents an internationalization of territorial authority. That the U.S. holds this view is evident in the way it justifies drone strikes. The U.S. argues that if a state that harbors a threat to the U.S. is unwilling or unable to do something about the threat, the U.S. is allowed to take action. This logic is borrowed from neutrality rules in the law of war which outline the circumstances in which one party to a conflict can attack another threatening party within a neutral's territory if the neutral state is unwilling or unable to deal with the threat itself.[482]

The fact that the UN, the U.S. and other international fora encourage states to beef up their surveillance capacity suggests another version the norm just mentioned: the international community has a stake in each state's ability to conduct surveillance at home, and can therefore make authoritative requests that states meet minimum security (surveillance) requirements domestically. (The most extreme version of such a norm—which I don't think obtains today—would be: insofar as a state cannot project power throughout its own territory, that territory becomes *res communis* (held in common by

[482] Deeks 2012.

all states) for purposes of security.[483]) Both the U.S.-specific norm and the broader norm suggest a coupling between internationalized security practices and territory, and both cut against the idea that territory marks a state's sovereign zone of exclusivity.

Moving from an analysis of norms to practice allow us to think through not only how territory is established, but what meaning states attribute to territory. Work by geographer Stuart Elden argues that it was the development of territory that led to borders, not vice versa.[484] "Territory is a political technology: it comprises techniques for measuring land and techniques for controlling terrain."[485] For instance, it was advances in science and technology—e.g. land surveying, geometry, cartography—that enabled rulers to gain dominion over larger tracts of land. Elden, working in a Foucaultian tradition, argues that "[t]erritory and population emerge at a similar historical moment as new ways of rendering, understanding and governing the people and the land."[486] The point here is not that territory is simply an outcome of state practices. Territory is also a lens through which states "conceive" the world, and as such it is an ongoing process.[487]

Surveillance is another technology that helps constitutes territory. It is a technology of visibility, also a technique for controlling terrain. Historically the space that could be territory was partially a function of the state's calculative reach. There was (and remains) a relationship between calculation and control. But *visibility* is important to calculation and control. Surveillance helps states know the land and what transpires on it. Another way to get at the point is to recognize that the "problem" to which surveillance is a solution is, in part, territorial.

---

[483] Simmons 2001, 304, citing Brownlie 2008.
[484] Elden 2010; Elden 2013b.
[485] Elden 2013a, 14.
[486] Ibid., 17.
[487] Elden 2013b, 16–17.

If territorial techniques are internationalized, so too are the ways in which states control land. If I am right—that state surveillance is partially constitutive of territory *qua* political technology—then *i-veillance* abroad represents an internationalization of certain territorial (i.e. state) practices. As states jointly surveil a given territory they simultaneously operate state control over land which under conventional sovereignty is exclusively ruled. They jointly inscribe their power over the land resulting in a space territorialized through *i-veillance* producing new opportunities for administration and rule.

This is not to suggest a de-territorialization of the state, but rather a reterritorialization. Seeing territory as a political technical process mirrors the analysis in John Ruggie's well-known article "Territoriality and Beyond."[488] As the modern state grew each state applied its own territorial practices to establish its own rule. "Political space came to be defined as it appeared from a single fixed viewpoint," reflecting through territory (and through "sovereignty" as Ruggie emphasizes) "the application of single-point perspectival forms to the spatial organization of politics."[489] Multiple states operating technologies of visibilities over space, however, reflect a "multiperspectival" operation of power. There is an increasing amount of earth over which multiple countries exercise power via surveillance. The point is *not* that more than one state has its eyes on a single patch of land. Rather, the way in which certain land is *effectively ruled* is made possible by cooperative *i-veillance*.

It is worth mentioning that *i-veillance* also operates on non-territorial spaces of flows and databases.[490] By "non-territorial" I mean that the relevant information being collected is not anchored to territory. The clear example is internet traffic. But another,

---

[488] Ruggie 1993.
[489] Ibid., 159.
[490] Ruggie 1993.

less obvious, example is the surveillance of the very databases that get created through massive amounts of data collection. Consider the sheer amount of abstraction that occurs as personal data of specific individuals joins up with massive datasets full of similar and other types of entries. The databases[491] of "data doubles"[492] of people and all their associations and transactions is itself an object of surveillance. As multiple states contribute to this weird non-territorial form of surveillance, we see yet another way in which surveillance *qua* state security practice is being internationalized.

Process: Society

Just as surveillance is tightly coupled to coercion and territory, it is tied to society as well. In particular, surveillance is heavily implicated in administrative control over people. Surveillance is the way that states "see" their people. Recurrent acts of state administration in some sense helps constitute the very people over whom the state wields authority as a citizenry. This is true from the state's perspective. Whether or not the people view themselves as such is another story, and I address that in the next chapter.

States not only "bind society"[493] in the legal sense, but they also "cage social relations"[494] through administrative and coercive acts of control. Modern state practices coordinate a good deal of social life. A prerequisite of this coordination is—no surprise here—surveillance. As an administrative and security practice, surveillance cages social relations bringing individuals and their interactions within the state's grasp.

While *conceptually* it seems that states "presuppose their societies,"[495] during state formation or state growth (both are process) a state forges new state-society

---

[491] Teboho Ansorge 2011.
[492] Haggerty and Ericson 2000; Lyon 2007, 55, 114.
[493] Lake 2008, 44.
[494] Mann 2012, 61.
[495] Wendt 1999, 209.

relationships with a new people. The question is, does one state's *i-veillance* activity likewise cage social relations within *other* states? "The notion of 'society' as a self-contained unit is itself an historical product of the state project,"[496] so there is no *a priori* reason why not. The answer must be determined empirically. Two conditions would have to be met before considering answering "yes" with respect to *i-veillance*. First, there needs to be an abundance of data collected, not just on a few 100 individuals, but on a more recognizably "social" scale. Second, the i-*veillance* must feed into some state action that affects those being surveilled. Otherwise, there is no real caging to speak of. A watchful Big Brother that never intervened might as well not exist. Things change, however, if the population being surveilled becomes acutely aware of the fact, if for no other reason that they may change their behavior as a result. I'll speak to this a bit more in the next chapter.

Does U.S. *i-veillance* meet these two criteria? It is hard to know just how much data the U.S. has on which groups of people. Data troves, however, will likely keep growing. Likewise, the number of interventions based on this data will also grow. Given this, I think we can say that the U.S. is in the process of caging more and more social relations outside of its borders, but it is a far cry from what occurs domestically. Regardless, because a state has sovereign prerogative over its own society, as social relations become implicated through international processes, we see another way in which the security feature of states is being internationalized.

---

[496] Jackson and Nexon 1999, 309.

An Internationalization of Authority

Given the transformations above, what is the implication for authority? Political authority results from "a fusion of power with legitimate social purpose."[497] This idea of authority as "legitimate power" is not uncommon and is even reflected in a common understanding of state authority entailing a monopoly of legitimate force. The legitimacy that underpins authority can differ in degree and kind.[498] There is also variation in the work performed by "power" and "purpose." Authority is typically thought of as present in the domestic context, but absent in the international context where anarchy rules. It is not uncommon, however, for scholars to look for authority (and therefore hierarchy) in the international realm.[499]

If the "legitimate social purpose" of a political activity and the power that underpins it becomes internationalized, then authority with respect to that activity will be internationalized. The articulation of power suggests the *form* of authority, whereas the social purpose gives authority its *content*.[500] The two sections above shed light on each of these elements of authority and suggests that there is an internationalization of political authority with respect to counterterrorism.

The legitimate social purpose of *i-veillance* has developed in tandem with norms, interests and identities that all prescribe international cooperation in the fight against terrorism. *I-veillance* is a critical counterterrorism practice that is at times not simply recommended but flatly mandated. The purpose is clear: fight terrorism. Moreover, the purposes behind *i-veillance* (and other counterterrorism practices) are articulated by myriad states and international institutions making it clear that this purpose is held in

---

[497] Ruggie 1982, 382.
[498] For discussions of legitimacy and authority in IR see Hurd 1999; Milner 1991; For a more specific discussion pertaining to international organizations see Barnett and Finnemore 2004.
[499] For some examples see Lake 2010; Dunne 2003; Wendt and Friedheim 1995.
[500] Ruggie 1982, 382.

common by multiple states. The purpose is *social* among states in the system (not necessarily with respect to their publics).

The power underpinning authority can be thought of a collective capacity to execute the purpose and "sanction actors who disrupt the performance of that function."[501] The security practice of *i-veillance,* as argued above, is internationalized. In this case the relevant capacity—the infrastructures and processes that enact *i-veillance*—is pooled internationally. It is however skewed toward powerful states, especially the U.S. The knowledge underpinning the capacity is likewise held disproportionately by powerful states, thereby lending those states additional (epistemic) authority.

Authority with respect to counterterrorism is therefore internationalized. This does not mean that it is *completely* internationalized, and it certainly does not mean that the authority is evenly distributed. As to the former point, it is clear that states could resist cooperating and some do. Nevertheless such resistance is marginal and within the tolerances we might expect given the relevant normative backdrop. As to the second point, some actors seem to have more authority than others in these matters. Specifically the U.S. and the United Nations. On the one hand the U.S. has been a source of capacity and a change agent promoting relevant counterterrorism norms. On the other hand the UN has been an active promoter of counterterrorism (and *i-veillance*) norms, most notably through UNSC Resolution 1373 and the UN Counterterrorism Strategy.

One question remains untouched—what of sovereignty? While that venerable institution has changed over time, contemporary sovereignty involves the following. States are supposed to have final authority with respect to their internal affairs, enjoy the luxury of non-interference in their internal affairs, and be recognized by international

---

[501] Wendt 1994, 392.

law as juridically independent.[502] But if we look at what states *do*, it is clear that sovereignty gets fudged in different ways all the time. Nevertheless, scholars cannot seem to pin down some new meaning of sovereignty or some final determination of the fate of sovereignty.[503]

Because *i-veillance* reflects an internationalization of some state security functions and authority on such matters, the temptation is to come to some conclusion about sovereignty in the abstract. I think this is mistaken.[504] We cannot look at a sliver of what states do and conclude that sovereignty *per se* has changed. However, insofar as authority is tied to sovereignty, and authority with respect to a given domain is being internationalized, observations can be made regarding how sovereignty *in that domain* is being *exercised*. For example we might observe how states are changing domestic law to enhance surveillance capabilities in light of demands placed on them by the U.S. and the UN. We could see the international authority at play, and we might conclude that those states are, in that moment, not exercising sovereignty in a domain in which we might expect it (i.e. concerning important domestic laws). That's fine. But that doesn't mean we can conclude that sovereignty has changed. Authority is much more corrigible than sovereignty. One cannot infer from changes in former that there are necessarily changes in the latter. What we need is a longer track record of evidence, and to see if more significant institutional changes take place regarding *i-veillance*.

---

[502] Krasner 2004.
[503] There are also arguments that some aspects of sovereignty be shared or otherwise held contingent on state behavior. Ibid.; International Commission on Intervention and State Sovereignty and International Development Research Centre (Canada) 2001.
[504] Moreover it distracts from the real and important ideational, infrastructural, and processual changes described in the dissertation.

Conclusion

Surveillance itself is a practice near and dear to what it means to be and act as a state. Since 9/11, surveillance infrastructure and practice has articulated itself internationally. The result are norms, interests and identities that implicate *i-veillance*. A significant presence of *i-veillance* infrastructure internationally suggests an incipient internationalization of security related surveillance. Moreover, because surveillance is tightly coupled with authoritative processes unique to states—coercion, territory, and society—the growth of *i-veillance* entails the internationalization of those same essential state processes. The result is an internationalization of the surveillance dimension of the state's security prerogative. And as purpose and power have internationalized, so too has authority on the matter. To be clear, "[i]nternationalization is a way of reorganizing and redeploying state power [and does not necessarily entail] a withering away of the state."[505] However if this process continues, it is compatible with two outcomes. A form of neo-medievalism,[506] or increased centralized authority at the international level (a world state at the extreme end of this spectrum).

[505] Wendt 1994, 393.
[506] Friedrichs 2001.

Chapter 8: Conclusion

The dissertation opened with the observation that states sometimes cooperate on the surveillance of individuals. The question posed was, to what extent is this a unique practice of international security and how extensive is it? With a clear conceptualization of surveillance it became clear that surveillance is really important to states and that it comes in many different forms. When one state engages in the surveillance of citizens of another state, I call this *i-veillance*. The empirical chapters demonstrated a significant involvement of international organizations and the myriad ways in which the U.S. conducts *i-veillance* abroad through different sensors. The conclusion is that *i-veillance* is an important international practice that underpins international security.

The penultimate chapter made three arguments. First, changes in norms, interests, and identity suggest a common international purpose in fighting terrorism—a task for which *i-veillance* is an indispensable tool. Second, there is an incipient internationalization of the state's surveillance function, itself a critical part of what it means to be a state. Finally, the internationalization of both purpose and power suggests an internationalization of authority with respect to *i-veillance*.

In this concluding chapter I think about how *i-veillance* might continue to grow, and what the implications of that growth will be for the people over whom surveillance is exercised. I make two arguments. First the growth of *i-veillance* is inevitable. Second the growth of *i-veillance* will be a contributing factor in the creation of global citizenship. I then think through some of the normative implications of *i-veillance* more generally and the claims of inevitable growth more specifically. I close the chapter with a discussion of

the limits of what has been written in the dissertation and by outlining future lines of research.

The Inevitable Growth of I-Veillance

The recent growth in *i-veillance* was, in part, a reaction to 9/11. That attack showed how a few individuals could do a lot of damage to the state. States paid attention. Today we are all keenly aware of how globalization, technology, and vulnerable complex systems conspire to empower individuals. What it means to be an individual in the 21st century is to be empowered through technology and freedom to move and communicate. As a result we live in an age of "complex terrorism"[507] in which individuals can more easily exact costs from states.[508] Individuals, the narrative goes, are threats to keep an eye on.

There are two dynamics that will work together to propel the growth of *i-veillance*. The first is the ratcheting effect of significant events. In the face of successful terrorist attacks or the increasing threat of such attacks, states will increase their surveillance efforts. The second is an "information security dilemma." As states seek information on individuals for security purposes, it necessarily reduces individuals' information security (and privacy). As people seek technological redress, states look for new ways to acquire information, and an information "arms" spiral ensues.

Before addressing these two dynamics, I need to put one assumption on the table: technology will continue to develop and become more accessible to individuals. While technological growth may be humanity's undoing (and therefore stop 'prematurely'),[509] many futurists are sanguine about continued development on into the future. Renown

---

[507] Homer-Dixon 2002.
[508] Though states exaggerate the risks. Mueller and Stewart 2012.
[509] Bostrom 2013, 15–16; Apparently scholars who think about these issues see a disturbingly high risk of near-term extinction. In an informal poll at the Global Catastrophic Risk Conference in Oxford, the median risk estimate of human extinction prior to 2100 was 19%. See Sandberg and Bostrom 2008.

futurist Ray Kurzweil (now Google's Director of Engineering), for one, argues that machines will surpass human language capabilities in 2029. Today it is not uncommon for futurists to predict machine consciousness.[510]

As technology writ large evolves, so too will surveillance technology more specifically. The most direct example is the co-evolution of computing technology and en/decryption technology. Technological development also provides new ways for the state to collect and categorize information. States will naturally explore surveillance technologies to counter the illicit behavior of individuals.

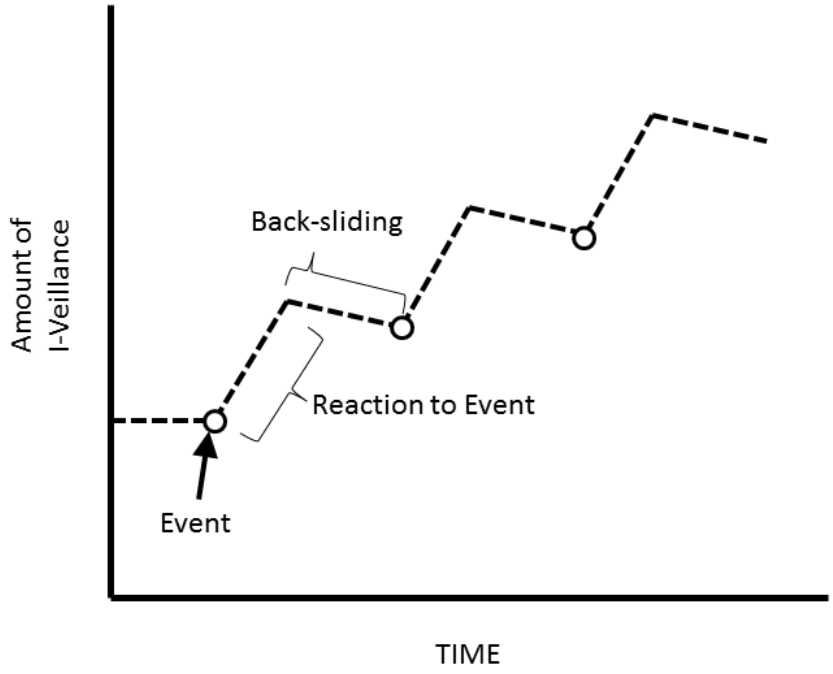
The first dynamic of change I refer to as "the ratcheting effect of significant events." After a significant terrorist or criminal incident the affected states will reflect on what they can do to stop similar events in the future. They will move to paper over gaps of knowledge with surveillance. Insofar as states are driven by a "phenetic fix"[511] to know and classify information about individuals, this will be most heightened after a major event. This is what occurred after 9/11. (Surveillance Studies as a discipline really took off over the past 14 years. The discipline's leading journal *Surveillance & Society* was started in 2002.) Over time, as publics push back a bit and the memory of significant events fade, states may dial back some of their surveillance activity. But they are unlikely to roll back all developments in surveillance capability. The growth of technology and the inevitable events that spur states to increase surveillance will result in a gradual increase of surveillance—and cooperative *i-veillance*—over time. Figure 4 illustrates the process.

The second dynamic reflects what I call an "information security dilemma." This is based off of IR's "security dilemma" concept which captures the idea that one state's

[510] George Dvorsky is an example here.
[511] Lyon 2002.

pursuit of security makes other states less secure (intentionally or not).[512] My riff on the idea suggests that as states take measures to protect themselves from *individuals,* some of those measures might be perceived as decreasing the freedom (security?) of those individuals. The state's security gains through *i-veillance* can be provocative to individuals, giving them an incentive to develop and adopt means to defeat surveillance. The result is an information arms spiral in which states and people pursue means to capture and protect information respectively.

Figure 4. The ratcheting effect of significant events



Such an information arms spiral occurs domestically but is muted due to the authority and legitimacy of the state. That is to say, *ceteris paribus*, there is already some understanding among citizens that their state requires some surveillance capability, and the state is in a better position to legislate limits on the use of technology to defeat state

[512] For a traditional statement of the security dilemma see Herz 1950; Jervis 1978.

surveillance. But *i-veillance* is an international phenomenon bereft of accountability and transparency mechanisms, and states are less able to make demands on people outside their borders. International publics will therefore be more likely and capable to push back against *i-veillance*.

The information security dilemma and spiral suggest that *i-veillance* will increase over time. However, it may be dialectical in the general sense that there are two opposing tendencies at play that may eventually find resolution. As I mentioned above, there is likely to be more resistance against international forms of surveillance than domestic forms. This is because states enjoy more legitimacy with their own publics than they do with citizens of other countries. *Legitimacy* in the eyes of other publics is the key. If states want to pursue *i-veillance* without resistance, then they need to adopt more transparent and accountable practices. The information security dilemma can be resolved if states can overcome this democratic deficit.[513] For this to happen, however, there needs to be enough pressure on states by the people affected. This pressure might come from transnational movements anchored in discourses of global citizenship.

The Contribution to Global Citizenship

The rhetoric of *i-veillance* and the practices themselves construct individuals as potential threats beyond their borders. Individuals are treated as global subjects who need monitoring. The mere fact that individuals are subject to *i-veillance* is, by itself, not enough to lead to a public that exercises agency for a common purpose.[514] Whether or not individuals subject to surveillance (a) are aware of that fact and (b) mobilize in light of that fact is another story.

---

[513] For some thoughtful work on the 'democratic deficit' see issue 2 of the 2004 volume of Government and Opposition. In particular Held 2004; Moravcsik 2004.
[514] Williams 2009, 42.

Individuals may respond to *i-veillance* in at least three ways. First, individuals may associate themselves with their fellow citizens nationally and petition their own government with their concerns of *i-veillance*. Second, individuals may again associate themselves nationally and petition the U.S. (or whichever outside state is involved in *i-veillance*). Third, individuals may associate themselves *transnationally* and petition multiple the governments involved. Each response is more unlikely than the former. The more invasive surveillance becomes, and the more it comes from a recognizable entity (like the U.S., the EU, or even "the West"), the more likely we will see the second and third responses.

As *i-veillance* increases, as I argue it inevitably will, the chance of an organized transnational public response increases. The response itself would likely revolve around privacy concerns and a perceived democratic deficit. But the *impetus* behind such a countermovement is likely to spring from a deeper sense of what it means to be a political agent. Because *i-veillance* implicates state-society relations the response of transnational actors may be explicitly political in a way that, say, environmental concerns are not. Moreover, if left unchecked *i-veillance* jeopardizes the foundation of global civil society[515] and transnational public spheres more broadly. Actors in global civil society may not feel free to pursue their agendas if they suspect states are closely monitoring them. The effect could be chilling for certain groups.

For these reasons, transnational actors pushing back against *i-veillance* are likely to adopt discourses of global citizenship. These are "discourses of 'citizenship' that exceed the boundaries of territorial states"[516] which are "focused not on status [of 'citizenship' in national contexts] but on role, on the exercise of new forms of political

---

[515] See Chapter 1, 'Five Meanings of Civil Society,' in Kaldor 2013; Kaldor 2003.
[516] Williams and Warren 2014, 31.

agency."[517] And it is *this* discourse—not simply a discourse about privacy and accountability—that global civil society will draw upon.[518]

The specific demands will likely reflect the human condition in the information age. Simon Chesterman writes that in the information age "we are witnessing [...] the emergence of a new social contract, in which individuals give the state (and, frequently, many other actors) power over information in exchange for security and the conveniences of living in a modern world."[519] Chesterman's observation concerns the U.S. domestic context, and he therefore doesn't consider surveillance as a form of power like I do. Nevertheless the social contract angle is suggestive.

Social contract theory typically focuses on the state's coercive power over individuals, and today information (and therefore surveillance capacity) is a determinant of power. The implication is that surveillance can be teased out as a pillar of state power and be subject to negotiation. Empirically we are in fact seeing an enormous growth in the digital world and systems that can record this data. Information is more and more an enabler of government intervention (i.e. of coercive power) and is becoming a distinct power resource of the state (and of other actors). So while transnational actors may speak of privacy and accountability, they will also be negotiating over a new dimension of state power.

Normative Implications

The practice of *i-veillance* raises two strands of normative implications. One concerns how states interact with people, and the other concerns how states interact with each other. I begin with the former. As the discussion above makes clear, there are normative implications for the individuals over whom *i-veillance* is wielded. As

---

[517] Williams 2009, 38.
[518] Castells 2008.
[519] Chesterman 2011, 11–12.

mentioned above there are likely to be concerns about a democratic deficit brought about by unaccountable and non-transparent state power. Because I already touched on these issues, in this section I want to focus on a less obvious implication for *liberty*.

Political Theorists distinguish between different types of liberty. The most well-known is the standard liberal idea that individuals are free insofar as the state does not interfere in their affairs. This is freedom as non-intervention.[520] Republican theorists have a slightly different notion of freedom. They argue that individuals are free insofar as no other entity has the capacity to arbitrarily interfere in their lives.[521] This is freedom as non-domination. To illustrate the difference between the two, consider the case of a slaveholder who is very hands-off on the conduct of his slaves. The slaves might not experience much intervention (and therefore be free in the first sense mentioned above), but we would certainly not regard them as enjoying liberty (in the Republican sense).

The upshot for *i-veillance* is that any country gathering volumes of data on people outside its territory may be negatively affecting their liberty *even if there is no direct intervention in their lives*. The U.S. NSA, for example, monitored telephony metadata of Spanish citizens, but is not (to my knowledge) intervening in the lives of Spanish citizens.[522] Nevertheless, surveillance represents a latent capacity for more intrusive interventions against people. Remember, for a state to intervene in the lives of individuals (either administratively or more coercively), it requires some surveillance capability. In practice, U.S. surveillance of individuals in Northwest Pakistan enable arbitrary interference in their lives in the form of drone attacks. In the Spanish case, the

---

[520] This is also referred to as 'negative liberty.' For the canonical statement see Isaiah Berlin's 'Two Concepts of Liberty.' Berlin 1969; For a more foundational expression see Mill 1863, 27–29.

[521] Pettit 1996.

[522] *El Mundo* reported that the NSA spied on 60 million calls in Spain during a one month period. Greenwald and Aranda 2013.

U.S. *could* take action against an individual under surveillance (for example, freezing assets or blocking travel), even if we have trouble imagining such a situation.

This discussion suggests that any and all substantial applications of *i-veillance* negatively affect the liberty of those individuals being targeted. The solutions to this normative concern are similar to that of the democratic deficit. There needs to be either less i-veillance or mechanisms that increase the control of individuals being affected by *i-veillance*.

The second set of normative implications concern interstate relations. There are interstate practices of *i-veillance* wherein stronger states wield influence over weaker ones. Throughout the dissertation I have spoken of "cooperative" *i-veillance*, but like most interactions in global politics, *i-veillance* is often a product of asymmetrical power relations. What are we to make of this?

Reflexively we might consider the relations through the lens of empire. This, however, is not fruitful. The fact that stronger states have more levers of power than weaker states does not equate to empire. Empires are "relationships of political control imposed by some political societies over the effective sovereignty of other political societies."[523] This imposed control entails a strong state systematically exercising its will over time, typically in the form of control over some policy domain, over a weaker state. A necessary condition of empire is an asymmetrical distribution in military power[524] and authority relations which flow 'downhill', as it were, from stronger states to weaker states. Imperial relationships are also dyadic. The "core" power dominates states on the "periphery", and states in the periphery are segmented from each other.[525] The result is a

[523] Doyle 1986, 19.
[524] Wendt and Friedheim 1995, 696–7.
[525] Nexon and Wright 2007, 257–8.

hub and spoke type network structure, but with no political ties connecting states on the rim.

Formal empire entails a more direct presence of and obtrusive control by the stronger power. *Informal* empire is a structure "of transnational political authority that combine an egalitarian principle of *de jure* sovereignty with a hierarchical principle of *de facto* control."[526] *De jure* sovereignty is respected, and there is no *direct* administration. In informal empire control is achieved through one of two routes. The stronger state can get buy-in from key local elites through incentives (e.g. via the "controlling influence of economic means"[527]). Second, through effects of the third dimension of power the interests and identities of relevant elites in weaker states change, and control becomes accepted. But even in informal empire, there is an *expectation* of violence on behalf of the weaker state if it deviates from the imperial state's rules or expectations.[528]

Theoretically, *i-veillance* need not be imperial. The practice can be conducted by co-equals and be viewed as a mutually beneficial coordination problem.[529] The structure may be bi-lateral or thoroughly orchestrated by multilateral institutions. Finally there is not necessarily an expectation of force to keep "partners" in line.

Empirically, *i-veillance* is not imperial. True, the U.S. is stronger than all its *i-veillance* partners. But this is not a necessary part of the relationships. Co-equal countries conduct *i-veillance* as well (here I am thinking of the different regional organizations that facilitate information exchange). Although some *i-veillance* is dyadic—underwritten by bilateral treaties for instance—other examples involve multiple actors (including IOs) sharing processes or actual infrastructures. The European Union

---

[526] Wendt and Friedheim 1995, 695.
[527] Doyle 1986, 23.
[528] Wendt and Friedheim 1995, 697.
[529] Maybe a coordination problem (akin to adopting the same weights and measures standards) in which states need to be able to speak the same language to exchange information easily.

is the most obvious example here. Finally, there is nothing to suggest in my research that stronger states are willing to use force to get other states to join in the surveillance game. (Though, this is not to say that there is no asymmetry of power behind any *quid pro quo*.)

While empire is too strong to apply here, elements of informal empire are suggestive for thinking through the normative implications of state interactions behind *i-veillance*. Empirically we see a strong state (the U.S.) pursuing an agenda (counterterrorism broadly and *i-veillance* more specifically) that requires the participation of weaker states. Cooperation appears to occur without any expectation of violence. If a state rebuffs U.S. requests for cooperation there may be costs, but nothing too out of the ordinary for typical foreign relations.

We might see the U.S. leaning-in on some countries to secure cooperation here and there, but not to a greater extent than other quotidian foreign policy issues that happen all the time but never make headlines. This is to say that looking at the interaction of specific actors (the U.S. and state *A*, the U.S. and state *B*, etc.) is not going to be too interesting. As with the general phenomena of *i-veillance,* looking at any one example may be underwhelming.

Instead of looking at how power works through specific interactions, we should be attentive to how power works through "relations of constitution." This perspective focuses on how "power works through social relations that analytically precede the social or subject positions of actors and that constitute them as social beings with their respective capacities and interests."[530] This approach helps make sense of widespread cooperation and the seemingly common attitude that states *ought* to play a part in combating terrorism (and serious crime). As I suggested in the previous chapter, part of

[530] Barnett and Duvall 2005, 47.

what it means to be a responsible state with respect to international security is to manage terrorism problems at home and contribute to solving the problem internationally. There is, as it were, a counterterrorism role-identity. Moreover there is functional differentiation among such roles. Weaker states furnish information to stronger states or allow stronger states to conduct surveillance on their citizens. Stronger states also take a more active role in storing and analyzing information. Strong states, the U.S. in particular, also have more epistemic authority due to advantages in technology and expertise.[531] The roles help *shape* state interests, sets expectations and lends legitimacy to *i-veillance* practices.

Being attuned to these power dynamics helps us understand the background conditions that facilitate *i-veillance* cooperation. It draws attention to how the legitimacy of any one practice is a product of a larger normative context that implicates security discourses and a broader constellation of similar practices that together normalize *i-veillance*.

Having thought through these implications we can ask the broader question, is *i-veillance* desirable? After all, it may increase security by decreasing the chance of large scale terrorist attacks. So long as *i-veillance* is not kept in the shadows, there might be a sweet spot in which states can conduct *i-veillance* in a way and to an extent that doesn't bother global publics much. Anne Marie Slaughter has remarked about similar "government networks" of agencies and national officials that they meet serious needs (in this case, security), are quite capable, and the agents involved are identifiable (and

[531] The recent disappearance of Malaysian Airlines Flight 370 is telling. The news coverage suggested surprise that the U.S. didn't have the surveillance capability to know what happened. Moreover, the U.S. sent aviation experts to aid in the investigation.

therefore maybe accountable). While not a perfect form of governance, such an approach may be the "least worst" option.[532]

However, I have argued that both the growth of *i-veillance* and related public discontent are inevitable. If I am right the question becomes how to best steer the development of *i-veillance*. The answer must be found in more accountable global governance that is responsive to a global civil society that can effectively channel concerns percolating in the public sphere.

The Dissertation's Limits

The broader claim of the dissertation is that *i-veillance* is a significant, *sui generis*, practice critical to international security. The argument was made first conceptualizing surveillance and then throwing tons of information about U.S. led practices at the reader. Nevertheless, the main limits of the arguments and research of the dissertation are the unavailability and secrecy of information. States don't advertise their surveillance activity, and no one else is systematically collecting information on *i-veillance* activity. This has led to a scattered research approach in which I looked far and wide for morsels of data. Though scattered, there ended up being quite a lot of information out there to demonstrate the broader claim.

That being said, three more specific claims have been more difficult to demonstrate.

1. *I-veillance* is heavily networked.
2. The returns of the whole *i-veillance* apparatus are greater than the sum of the individual inputs.
3. I-veillance has been critical to specific counterterrorism and anti-crime interventions against individuals.

Evidence for the first claim is strong for the U.S. case. For instance, U.S. policy requires information sharing between its agencies that operate different sensors.[533] The

[532] Slaughter 2004, 162 with the hat-tip to Churchill. See also Slaughter 2009.

claim, however, might be unique to U.S. led practices if only because U.S. efforts are so developed. It is also difficult to know how much surveillance information the U.S. pushes out to its partner countries.

There is no *direct* empirical evidence for the second claim. The truth of the claim, however, is heavily suggested facts of the matter and the dynamics of surveillance in the digital age. As multiple inputs of data get put together in databases there are increasing returns to knowledge. Consider the following simplistic example. One sensor connects person *A* to *B*, a second connects *B* to *C,* and a third *C* to *D*. Analysis of this data leads to an inference that is not given by any one sensor—*A* might be connected to *D*. The more data one has the greater the inferential capability.

The third claim is difficult to substantiate due to a lack of information. States are not eager to provide details of how they acquire information that led to arrests or counterterror operations. This is the familiar "sources and methods" that intelligence agencies go to great lengths to protect. However, again I think the truth of the claim is implicit in the nature of state interventions. States require surveillance prior to making interventions.

The theoretical claims I made in the previous chapter have limits as well. The claim is that a key security function of the state is being internationalized. Some might resist the claim arguing that (a) surveillance isn't essential in the way I have claimed, or (b) the "internationalization" I point to is too weak to sustain any argument about international state formation. I look at each in turn.

First, there are other processes related to states' security functions that are international, but we wouldn't say that security itself is internationalized. The global

---

533 The existence of the National Counterterrorism Center (NCTC) is illustrative of how networked counterterrorism information flows are. All CT intelligence flows into NCTC for analysis. The NCTC then disseminates that information back out to U.S. intelligence agencies.

arms trade, for instance, is in some sense a cooperative international practice, and many states rely on foreign military purchases to build up their security forces. So my argument hinges on convincing the reader that surveillance of individuals for security purposes is essential to what it means to be a state. The nub of the argument I made in the previous chapter is that surveillance *is* a security practice and *necessary* for state interventions. If a state decides to buy a better helicopter from the U.S., that is a choice about *how* to improve security infrastructure and is not the infrastructure (or practice) *per se*. Readers, however, might not be satisfied with this, and there might very well be other counterexamples I need to consider.

The argument that surveillance internationalization is too thin to be meaningful is more difficult to dismiss. Compared to domestic state surveillance, *i-veillance* is thin indeed. However the whole purpose of the empirical chapters was to show just how much activity there actually is. Moreover this international *i-veillance* activity is often emphasized by state practitioners as very important. So, even though *i-veillance* is thin in comparison to domestic surveillance, there is still a lot of it and it is highly valued. Again, if readers are not convinced by the preceding chapters, I am convinced that there will be increased evidence in the future.

Future Avenues of Research

The dissertation covers a lot of ground and opens up many different lines for future research. While I will continue to look for and keep track of examples of *i-veillance*, there are five projects I have in mind.

The first project would be to dig deeper into one of the cases in the dissertation—either the role of the FBI in surveillance or the role of the U.S. Department of Homeland Security. There are opportunities for me to do extensive interviews with current and former officials from each agency. The FBI even has a point person to work with

academics. The goal of the project would be to get a more fine grained understanding of what surveillance exists, how it works, and the self-understandings of the practitioners.

The second project would focus on the recent publically disclosed NSA activity. There has not been much academic treatment of the revelations and the relevant documentation. There remains a lot of confusion about what has been released, and documents continue to get leaked. At this point I am not sure what specific question to ask, but I would limit my inquiry to the international aspects of the NSA data gathering. How are other states implicated in U.S. efforts (as "partners" or as unknowing targets)? What do the targeting patterns (of individuals) tell us about how the U.S. understands security? What does the language in the documents say (if anything) about U.S. threat perceptions?

Third, how does *i-veillance* work in cyberspace? I believe that security and cyberspace will garner more and more attention from practitioners and scholars alike. It will be nice to keep up with this trend and focus on the surveillance angle. While the dissertation did not address the matter much, there is cooperative *i-veillance* among cybersecurity practitioners (from both the public and private sectors). This activity needs documenting and is worthy of more in depth study.

The final two projects would focus on discourses of surveillance. One is from states' perspectives, the other from that of individuals. First would be to study the perceptions of citizens who are on the receiving end of *i-veillance*. How are privacy advocates of other countries responding to U.S. international surveillance technology, and to what extent do these advocates work together transnationally? I would limit my inquiry to two groups of countries—those which have been targeted by publicly disclosed NSA surveillance and those that have received U.S. drone technology. For each of those countries I would study how their privacy-focused

NGOs are reacting. To begin, I would do a discourse analysis of their relevant publications and public statements and further analysis on how the relevant NGOs work together transnationally.

The last project would examine how states talk about surveillance in the aftermath of crises. Under the presumption that states will expand surveillance after a crisis, what is the discourse that underlies and makes possible increases in surveillance. Is it about minimizing risk, or maximizing knowledge? Is it about fixing mistakes, or staying ahead of adversaries? Is there a role for IOs to play? The most obvious case to examine would be 9/11. Other possible cases include the London and Madrid plots, and even the recent disappearance/hijacking(?) of Malaysian Airlines flight 370.

Final Thoughts

The dissertation has been one long case for taking the surveillance of individuals in international politics seriously. My hope is that the reader will now have a heightened awareness of how states are extending tendrils of power to touch the lives of individuals globally. There are a lot of little practices going on that constitute a fairly significant infrastructure of international surveillance. The practices reflect interests in securing the state from individuals. The practices also suggest a growing norm that containing individuals *qua* international-threat is a responsibility states owe each other.

As states cooperate in *i-veillance,* they share infrastructure and processes that are near and dear to what it means to be a state. Today, I have argued, we see an internationalization of surveillance that partly constitutes states' core security functions. Further development of this, which in this last chapter I have argued is inevitable, will trigger an information security dilemma of sorts. As the dialectic of security seeking states and privacy/liberty seeking individuals plays out, the result will likely be transnational movements demanding more transparency and accountability. The growth

of *i-veillance* and the push to overcome the resulting democratic deficit could result in a more recognizable form of international state formation.

Bibliography

Abbott, Andrew. 1995. Things of boundaries. *Social Research* 62 (4): 857–882.

Achenbach, Joel. 2012. NASA gets two military spy telescopes for astronomy. *The Washington Post*. Available from <http://www.washingtonpost.com/national/health-science/nasa-gets-military-spy-telescopes-for-astronomy/2012/06/04/gJQAsT6UDV_story.html>. . Accessed3 October 2013.

Adler, Emanuel, and Vincent Pouliot. 2011a. International practices. *International Theory* 3 (01): 1–36.

Adler, Emanuel, and Vincent Pouliot. 2011b. *International practices*. Cambridge; New York: Cambridge University Press.

Agnew, John. 1994. The Territorial Trap: The Geographical Assumptions of International Relations Theory. *Review of International Political Economy* 1 (1): 53–80.

Althaus, Dudely. 2012. U.S. Navy Seal becomes military attaché to Mexico. *Houston Chronicle*. Available from <http://www.chron.com/news/houston-texas/article/U-S-Navy-Seal-becomes-military-attach-to-Mexico-3400982.php#src=fb>. . Accessed16 January 2014.

Ambrosio, Thomas. 2008. Catching the 'Shanghai Spirit': How the Shanghai Cooperation Organization Promotes Authoritarian Norms in Central Asia. *Europe-Asia Studies* 60 (8): 1321–1344.

American Civil Liberties Union. 2013. *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*. American Civil Liberties Union. Available from <http://www.aclu.org/technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record>. . Accessed22 July 2013.

Andersen, R. S., and F. Moller. 2013. Engaging the limits of visibility: Photography, security and surveillance. *Security Dialogue* 44 (3): 203–221.

Andreas, Peter, and Ethan Avram Nadelmann. 2006. *Policing the globe: criminalization and crime control in international relations*. Oxford ; New York: Oxford University Press.

Andreas, Peter, and Richard Price. 2001. From War Fighting to Crime Fighting: Transforming the American National Security State. *International Studies Review* 3 (3): 31–52.

Anthony, Sebastian. 2013. DARPA shows off 1.8-gigapixel surveillance drone, can spot a terrorist from 20,000 feet. *ExtremeTech*. Available from <http://www.extremetech.com/extreme/146909-darpa-shows-off-1-8-gigapixel-surveillance-drone-can-spot-a-terrorist-from-20000-feet>. . Accessed14 November 2013.

Aris, Stephen. 2009. The Shanghai Cooperation Organisation: 'Tackling the Three Evils'. A Regional Response to Non-traditional Security Challenges or an Anti-Western Bloc? *Europe-Asia Studies* 61 (3): 457–482.

Ashcroft, John. 2002. Memorandum on the Coordination of Information Relating to Terrorism. Office of the Attorney General.
Astrium EADS. 2013. Spot Satellite Technical Data. Available from <http://www2.astrium-geo.com/files/pmedia/public/r329_9_spotsatellitetechnicaldata_en_sept2010.pdf>.
Bailey, Neil. 2008. Overseas Liaison Officers. In *Combating International Crime: The Longer Arm of the Law*, edited by Steven David Brown, 96–102. Routledge.
Banai, Ayelet. 2014. The territorial rights of legitimate states: a pluralist interpretation. *International Theory* 6 (01): 140–157.
Banai, Ayelet, Margaret Moore, David Miller, Cara Nine, and Frank Dietrich. 2014. Symposium 'Theories of Territory beyond Westphalia'. *International Theory* 6 (01): 98–104.
Barnes, Julian E., and Greg Miller. 2009. Pakistan gets a say in drone attacks on militants. *Los Angeles Times*. Available from <http://articles.latimes.com/2009/may/13/world/fg-predator13>. . Accessed16 October 2013.
Barnett, Michael. 2001. Authority, Intervention, and IR Theory. In *Intervention and transnationalism in Africa: global-local networks of power*, edited by Thomas M. Callaghy, Ronald Kassimir, and Robert Latham, 47–65. Cambridge ; New York: Cambridge University Press.
Barnett, Michael, and Liv Coleman. 2005. Designing Police: Interpol and the Study of Change in International Organizations. *International Studies Quarterly* 49 (4): 593–619.
Barnett, Michael, and Raymond Duvall. 2005. Power in International Politics. *International Organization* 59 (01): 39–75.
Barnett, Michael, and Martha Finnemore. 2004. *Rules for the World: International Organizations in Global Politics*. 1 edition. Cornell University Press.
Benjamin, Daniel. 2012. Countering Violent Extremism (Remarks), Near East South Asia Center for Strategic Studies. Washington, DC. Available from <http://www.state.gov/j/ct/rls/rm/2012/182716.htm>.
Benjamin, Roger, and Raymond Duvall. 1985. The Capitalist State in Context. In *The Democratic State*, edited by Roger W. Benjamin and Stephen Lloyd Elkin. University Press of Kansas.
Berlin, Isaiah. 1969. *Four essays on liberty*. London; New York [etc.: Oxford University P.
Biersteker, Thomas. 2005. State, Sovereignty and Territory. In *Handbook of international relations*, edited by Walter Carlsnaes, Thomas Risse-Kappen, and Beth A Simmons. London; Thousand Oaks, Calif.: SAGE Publications.
Bostrom, Nick. 2013. Existential Risk Prevention as Global Priority. *Global Policy* 4 (1): 15–31.
Brownfield, William R. 2012. *Statement on Security Challenges in Latin America*. Washington D.C. Available from <http://m.state.gov/md187097.htm>.
Brownlie, Ian. 2008. *Principles of public international law*. Oxford University Press.
Bureau of Investigative Journalism. 2013. *Covert War on Terror: The Data*. Available from <http://www.thebureauinvestigates.com/category/projects/drone-data/>.
Bush, George. 2002. State of the Union Address.
Bush, George W. 2003. Homeland Security Presidential Directive / HSPD-6. Available from <https://www.fas.org/irp/offdocs/nspd/hspd-6.html>.

Cain, Maureen. 1983. Introduction: Towards an Understanding of the International State. *International Journal of the Sociology of Law* 11: 1–10.
Campbell, David. 2007. Geopolitics and visuality: Sighting the Darfur conflict. *Political Geography* 26 (4): 357–382.
Campbell, David, and Michael J. Shapiro. 2007. Guest Editors' Introduction. *Security Dialogue* 38 (2): 131–137.
CARICOM IMPACS. 2013. *2013 CARICOM Crime and Security Strategy: Securin The Region*. Port-Au-Prince, Haiti: Conference of Heads of Government of CARICOM. Available from <http://www.state.gov/documents/organization/210844.pdf>. . Accessed1 January 2014.
CARICOM IMPACS. 2007. One Team, One Space, One Caribbean. ISBN: 978-976-8212-10-8. Available from <http://caricomimpacs.org/impacs/pdf/07.pdf>.
CARICOM Press Release. 2007. Communique Issued at the Conclusion of the Twenty-Eighth Meeting of the Conference of Heads of Government of the Caribbean Community.
CARICOM Secretariat. 2008. Statement Issued by the Conference of Heads of Government of the Caribbean Community at its Thirteenth Special Meeting. Available from <http://www.state.gov/p/wha/rls/107741.htm>.
Carrington, Edwin W. 2007. Statement on the Occasion of the Inauguration of the CARICOM Single Domestic Space.
Carter, Jimmy. 1978. Remarks at the Congressional Space Medal of Honor Awards Ceremony, Kennedy Space Center, Florida.
Castel, Robert. 1991. From Dangerousness to Risk. In *The Foucault Effect: Studies in Governmentality*, edited by Graham Burchell and Colin Gordon, 281–298. University of Chicago Press.
Castells, Manuel. 2008. The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance. *The ANNALS of the American Academy of Political and Social Science* 616 (1): 78–93.
Chairman of the Joint Chiefs of Staff. 2011. Instruction: Information Assurance (IA) and Support to Computer Network Defense (CND) - CJCSI 6510.01F. Joint Chiefs of Staff. Available from <http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf>.
Chase-Dunn, Christopher. 1990. World-state formation: historical processes and emergent necessity. *Political Geography Quarterly* 9 (2): 108–130.
Chesterman, Simon. 2011. *One nation under surveillance: a new social contract to defend freedom without sacrificing liberty*. Oxford ; New York: Oxford University Press.
Clark, Richard M. 2000. *Uninhabited Combat Aerial Vehicles*. Cadre Papers. Air University. College of Aerospace Doctrine, Research and Education.
Cohn, Carol. 1987. Sex and Death in the Rational World of Defense Intellectuals. *Signs* 12 (4): 687–718.
Cox, Robert Henry. 2001. The Social Construction of an Imperative: Why Welfare Reform Happened in Denmark and the Netherlands but Not in Germany. *World Politics* 53 (3): 463–498.
Dandeker, Christopher. 1994. *Surveillance, power and modernity : bureaucracy and discipline from 1700 to the present day*. Cambridge: Polity.
Dean, Mitchell. 2010. *Governmentality: Power and Rule in Modern Society*. SAGE Publications.

Deeks, Ashley S. 2012. 'Unwilling or Unable': Toward a Normative Framework for Extraterritorial Self-Defense. *Virginia Journal of International Law* 52 (3): 483–550.
Defense Information Systems Agency. 2012. Multinational Information Sharing.
Defense Security Cooperation Agency. 2013. News Release: France -MQ-9 Reapers. Available from <http://www.dsca.mil/pressreleases/36-b/2013/France_13-40.pdf>. . Accessed19 July 2013.
Desch, Michael C. 1996. War and strong states, peace and weak states? *International Organization* 50 (2): 237–268.
Deudney, Daniel. 2000. Geopolitics as Theory: Historical Security Materialism. *European Journal of International Relations* 6 (1): 77–107.
DHS Immigration and Customs Enforcement. n.d. ICE - International Affairs. *About ICE*. Available from <http://www.ice.gov/about/offices/homeland-security-investigations/oia/>. . Accessed18 January 2014.
DHS Press Release. 2006. Press Conference with Michael Chertoff, Alberto Gonzales, Robert Mueller and Kip Hawley.
Dietrich, Frank. 2014. Territorial rights and demographic change. *International Theory* 6 (01): 174–190.
Digital Globe website. n.d. DigitalGlobe - Satellite Imagery and Geospatial Information Products. *DigitalGlobe - Satellite Imagery and Geospatial Information Products*. Available from <http://digitalglobe.com/resources/satellite-information>. . Accessed3 March 2013.
Douglas, Richard. 2007. DOD Briefing wiht Deputy Assistant Secretary Douglas, Pentagon. Available from <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=3947>.
Doyle, Michael W. 1986. *Empires*. Cornell University Press.
Dray, William. 1964. *Philosophy of History*. Englewood Cliffs, N.J.: Prentice Hall.
Dunne, Tim. 2003. Society and Hierarchy in International Relations. *International Relations* 17 (3): 303–320.
Duvall, Raymond, and Chowdhury. 2011. Practices of theory. In *International practices*, edited by Emanuel Adler and Vincent Pouliot, 335–354. Cambridge; New York: Cambridge University Press.
Elden, Stuart. 2013a. How Should We Do the History of Territory? *Territory, Politics, Governance* 1 (1): 5–20.
Elden, Stuart. 2010. Land, terrain, territory. *Progress in Human Geography*. Available from <http://phg.sagepub.com/content/early/2010/04/21/0309132510362603>. . Accessed7 December 2012.
Elden, Stuart. 2013b. *The Birth of Territory*. University of Chicago Press.
Enders, Walter, and Todd Sandler. 2011. Who adopts MIND/FIND in INTERPOL's fight against international crime and terrorism? *Public Choice* 149 (3-4): 263–280.
Entous, Adam, David Gauthier-Villars, and Drew Hinshaw. 2013. U.S. Boosts War Role in Africa; American Drones Help French Target Militants in Mali, as Chad Claims Killings. *Wall Street Journal (Online)*. New York, N.Y., United States, sec. World.
Ereli, Adam, and U.S. Department of State. 2004. Joint Statement by the United States of America, the Caribbean Community (CARICOM) and the Dominican Republic on the Third Border Initiative. Available from <http://2001-2009.state.gov/r/pa/prs/ps/2004/28136.htm>. . Accessed6 January 2014.
Ericson, Richard Victor, and Kevin D. Haggerty. 1997. *Policing the risk society*. Toronto ; Buffalo: University of Toronto Press.

Erwin, Marshall Curtis. 2013. *Intelligence, Surveillance, and Reconnaissance (ISR) Acquisition: Issues for Congress*. Congressional Research Service. Congressional Research Service.
European Union, and United States of America. 2011. *Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security*. *L 215, 11/08/2012, p. 5*.
Farrell, Theo, Terriff Terry, and Osinga Frans. 2010. *A Transformation Gap: American Innovations and European Military Change*. Stanford University Press.
FBI Press Release. 2006. FBI Opens Office in Sierra Leone. *FBI*. Available from <http://www.fbi.gov/news/stories/2006/december/freetown_legat120106>. . Accessed14 April 2014.
FBI Press Release. 2009. Legat Building Relationships in Jordan. *FBI*. Available from <http://www.fbi.gov/news/stories/2009/september/jordan_091009>. . Accessed14 April 2014.
FBI Press Release. 2007. Our Legal Attache in Cambodia. *FBI*. Available from <http://www.fbi.gov/news/stories/2007/august/cambodia080207>. . Accessed14 April 2014.
FBI Press Release. 2008. Our Legal Attache in Dakar, Senegal. *FBI*. Available from <http://www.fbi.gov/news/stories/2008/july/dakar_071408>. . Accessed14 April 2014.
Fearon, James, and Alexander Wendt. 2002. Rationalism v. Constructivism: A Skeptical View. In *Handbook of International Relations*, edited by Walter Carlsnaes, Thomas Risse-Kappen, Thomas Risse, and Beth A. Simmons, 52–72. SAGE.
Finnemore, Martha, and Kathryn Sikkink. 1998. International norm dynamics and political change. *International Organization* 52 (4): 887–917.
Forget, Louis, International Monetary Fund, and World Bank. 2004. *Financial intelligence units: an overview*. Washington, D.C: International Monetary Fund : World Bank Group.
Foucault, Michel. 1995. *Discipline & Punish: The Birth of the Prison*. Random House Digital, Inc.
Foucault, Michel. 2007. *Security, territory, population: lectures at the Collège de France, 1977-78*. Basingstoke ; New York: Palgrave Macmillan : République Française.
Foucault, Michel, Graham Burchell, and Colin Gordon. 1991. *The Foucault Effect: Studies in Governmentality*. University of Chicago Press.
Fowler, Sandra L. 2008. Legal Attaches and Liaison: The FBI. In *Combating International Crime: The Longer Arm of the Law*, edited by Steven David Brown, 110–121. Routledge.
Franceschi-Bicchierai, Lorenzo. 2012. Spy-Satellite Merger Fizzles, Preventing Space Monopoly. *Wired (online)*. Available from <http://www.wired.com/dangerroom/2012/06/spysat-smackdown/>.
Friedrichs, Jörg. 2001. The Meaning of New Medievalism. *European Journal of International Relations* 7 (4): 475–501.
Frydl, Kathleen J. 2006. Kidnapping and State Development in the United States. *Studies in American Political Development* 20 (01): 18–44.
Fuentes, Tom. 2005. An Interview with the FBI's International Operations. Available from <http://www.fbi.gov/news/stories/2005/september/fuentes_091205>. . Accessed14 April 2014.

Gambler, Rebecca, and Michael J. Courts. 2012. *Visa Waiver Program: Additional Actions Needed to Mitigate Risks and Strengthen Overstay Enforcement*.
Gantz, John, and David Reinsel. 2012. *The Digital Universe in 2020*. IDC, sposnored by EMC Corporation. Available from <http://www.emc.com/collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf>.
Gaventa, John. 1982. *Power and powerlessness: quiescence and rebellion in an Appalachian valley*. Urbana: University of Illinois Press.
Gerring, John. 2012. Mere Description. *British Journal of Political Science* 42 (04): 721–746.
Gertler, Jeremiah. 2012. *U.S. Unmanned Aerial Systems*. Congressional Research Service.
Ghosh, Bobby. 2009. Overseas Turf War Between the CIA and DNI Won't Die. *Time*. Available from <http://content.time.com/time/nation/article/0,8599,1936129,00.html>. . Accessed15 January 2014.
Giddens, Anthony. 1985. *A Contemporary Critique of Historical Materialism. Vol. 2: The Nation-State and Violence*. University of California Press.
Giddens, Anthony. 1981. *A Contemporary Critique of Historical Materialism: Power, Property and the State*. University of California Press.
Giddens, Anthony. 1984. *The Constitution of Society: Outline of the Theory of Structuration*. University of California Press.
Glassman, Jim. 1999. State power beyond the `territorial trap': the internationalization of the state. *Political Geography* 18 (6): 669–696.
Gordon, Michael R., and Eric Schmitt. 2013. U.S. Officials Propose Sharing Drone Surveillance Data With Algerian Forces. *The New York Times*, sec. World / Middle East. Available from <http://www.nytimes.com/2013/02/27/world/middleeast/john-kerry-diplomatic-trip.html>. . Accessed17 July 2013.
Graff, Garrett M. 2011. *The threat matrix: the FBI at war in the age of terror*. New York: Little, Brown and Company.
Greenwald, Glenn, and Germán Aranda. 2013. La NSA espió 60 millones de llamadas en España en sólo un mes. *El Mundo*. Available from <http://www.elmundo.es/espana/2013/10/28/526dcbad61fd3d07678b456b.html>.
Greenwald, Glenn, and Ewen MacAskill. 2013a. Boundless Informant: the NSA's secret tool to track global surveillance data. *The Guardian*, sec. World news. Available from <http://www.guardian.co.uk/world/2013/jun/08/nsa-boundless-informant-global-datamining#zoomed-picture>. . Accessed17 July 2013.
Greenwald, Glenn, and Ewen MacAskill. 2013b. NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*, sec. World news. Available from <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. . Accessed2 March 2014.
Griffiths, Hugh, and Chris Baker. 2007. Radar imaging for combatting terrorism. In *Imaging for detection and identification [proceedings of the NATO Advanced Study Institute on Imaging for Detection and Identification, Il Ciocco, Italy, 23 July-5 August 2006]*, 29–48. Dordrecht; [London]: Springer. Available from <http://dx.doi.org/10.1007/978-1-4020-5620-8>. . Accessed21 May 2013.
Haas, Peter M. 1992. Introduction: Epistemic Communities and International Policy Coordination. *International Organization* 46 (1): 1–35.

Haggerty, KD, and A Gazso. 2005. Seeing beyond the ruins: Surveillance as a response to terrorist threats. *The Canadian Journal of Sociology* 30 (2): 169–187.
Haggerty, Kevin D., and Richard V. Ericson. 2000. The surveillant assemblage. *The British Journal of Sociology* 51 (4): 605–622.
Hayward, Clarissa Rile. 2000. *De-facing power*. Cambridge; New York: Cambridge University Press.
Healy, Timothy. 2009. The Terrorist Screening Center and Its Role in Combating Terrorist Travel. Available from <http://www.fbi.gov/news/testimony/the-terrorist-screening-center-and-its-role-in-combating-terrorist-travel>. . Accessed12 July 2013.
Held, David. 2004. Democratic Accountability and Political Effectiveness from a Cosmopolitan Perspective. *Government and Opposition* 39 (2): 364–391.
Herz, John H. 1950. Idealist Internationalism and the Security Dilemma. *World Politics* 2 (02): 157–180.
Heyman, David. 2011. *The United States Visa Waiver Program*. Rayburn House Office Building.
Hinshaw, Drew. 2013. For African Generals, Drones Are The Latest Thing; Aircraft Are Being Used to Track Militants, Poachers and Drug Traffickers. *Wall Street Journal (Online)*. New York, N.Y., United States, sec. World.
Homer-Dixon, Thomas. 2002. The Rise of Complex Terrorism. *Foreign Policy*.
Hopf, Ted. 2010. The logic of habit in International Relations. *European Journal of International Relations* 16 (4): 539–561.
Hulnick, Arthur S. 1991. Intelligence cooperation in the post-cold war era: A new game plan? *International Journal of Intelligence and CounterIntelligence* 5 (4): 455–465.
Hurd, Ian. 1999. Legitimacy and Authority in International Politics. *International Organization* 53 (2): 379–408.
Imtiaz, Saba. 2011. Pakistan to Replace 'Insecure' US Border Watch Software. *The Express Tribune*. Pakistan. Available from <http://tribune.com.pk/story/184568/pakistan-to-replace-insecure-us-border-watch-software/>.
International Commission on Intervention and State Sovereignty, and International Development Research Centre (Canada). 2001. *The responsibility to protect: report of the International Commission on Intervention and State Sovereignty*. Ottawa: International Development Research Centre. Available from <http://responsibilitytoprotect.org/ICISS%20Report.pdf>.
INTERPOL. 2009. Cooperation Agreement Between ICPO-INTERPOL and CARICOM. Available from <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCsQFjAA&url=http%3A%2F%2Fwww.interpol.int%2Fcontent%2Fdownload%2F9286%2F68580%2Fversion%2F1%2Ffile%2FINTERPOL_CARICOM.pdf&ei=iq7RUtblAu7NsQSMn4KoCw&usg=AFQjCNG7YVl96yD2A9QIjktlomYoTp8a_g&bvm=bv.59026428,d.cWc>.
INTERPOL. 2014. Data Exchange: I-24/7.
ISE Program Manager. 2009. *Information Sharing Environment Annual Report 2009*. Available from <http://www.ise.gov/sites/default/files/ISE_2009-Annual-Report_FINAL_2009-06-30_0.pdf>. . Accessed11 July 2013.
ISE Program Manager. 2012. *Information Sharing Environment Annual Report 2012*. Available from

<http://ise.gov/sites/default/files/ISE_Annual_Report_to_Congress_2012.pdf >. . Accessed11 July 2013.
ISE Program Manager. 2006. *Information Sharing Environment Implementation Plan*. Available from <http://ise.gov/sites/default/files/ise-impplan-200611_0.pdf>.
Jackson, Patrick Thaddeus. 2004. Hegel's House, or 'People are states too'. *Review of International Studies* 30 (2): 281–287.
Jackson, Patrick Thaddeus, and Daniel Nexon. 2002. Whence Causal Mechanisms? A Comment on Legro. *Dialogue IO* 1 (01): 81–102.
Jackson, Patrick Thaddeus, and Daniel H. Nexon. 1999. Relations Before States: Substance, Process and the Study of World Politics. *European Journal of International Relations* 5 (3): 291–332.
Jensen, R. 2001. The United States, International Policing and the War against Anarchist Terrorism, 1900-1914. *Terrorism and Political Violence* 13 (1): 15–46.
Jensen, Richard Bach. 2013. The First Global Wave of Terrorism and International Counter-Terrorism. In *An international history of terrorism: Western and non-Western experiences*, 16–34. Political violence. Abingdon, Oxon ; New York, NY: Routledge.
Jervis, Robert. 1978. Cooperation under the Security Dilemma. *World Politics* 30 (02): 167–214.
Johnston, Alastair Iain. 2001. Treating International Institutions as Social Environments. *International Studies Quarterly* 45 (4): 487–515.
Johnstone, Ian. 2008. Legislation and Adjudication in the Un Security Council: Bringing down the Deliberative Deficit. *The American Journal of International Law* 102 (2): 275–308.
Kahler, Miles, and David A. Lake. 2003. Globalization and Governance. In *Governance in a Global Economy: Political Authority in Transition*. Princeton University Press.
Kaldor, Mary. 2013. *Global Civil Society: An Answer to War*. John Wiley & Sons.
Kaldor, Mary. 2003. The idea of global civil society. *International Affairs* 79 (3): 583–593.
Kaplan, David, and Kevin Whitelaw. 2006. Remaking U.S. Intelligence - Part I: Introduction. *U.S. News and World Report*. Available from <http://www.usnews.com/usnews/news/articles/061103/3dni.intro.htm>. . Accessed20 May 2013.
Karp, D.J. 2013. The location of international practices: What is human rights practice? *Review of International Studies* 39 (4): 969–992.
Keck, Margaret E. 1998. *Activists Beyond Borders: Advocacy Networks in International Politics*. Cornell University Press.
Keohane, Robert O. 2005. *After Hegemony: Cooperation and Discord in the World Political Economy (Princeton Classic Editions)*. 1st Princeton Classic Ed edition. Princeton University Press.
Keohane, Robert O., and Joseph S. Nye. 2000. Introduction. In *Governance in a Globalizing World*, edited by Joseph S. Nye and John D. Donahue. Brookings Institution Press.
Kessler, Ronald. 2002. *The bureau: the secret history of the FBI*. New York: St. Martin's Press.
King, Gary, Robert O. Keohane, and Sidney Verba. 1994. *Designing social inquiry: scientific inference in qualitative research*. Princeton, N.J: Princeton University Press.

Kozaryn, Linda. 1996. Predators Bound for Bosnia. *American Forces Press Services*. Available from <http://www.defense.gov/News/NewsArticle.aspx?ID=40516>. . Accessed15 November 2013.
Krasner, S. D. 2004. Sharing sovereignty: new institutions for collapsed and failing states. *International Security* 29 (2): 85–120.
Krebs, Gunter. n.d. KH-11 / Kennen / Crystal Satellites. *Gunter's Space Page*. Available from <http://space.skyrocket.de/doc_sdat/kh-11.htm>. . Accessed3 October 2013.
Kronstadt, K. Alan. 2003. *Pakistan-U.S. Anti-Terrorism Cooperation*. Congressional Research Service. Congressional Research Service. Available from <http://www.fas.org/man/crs/RL31624.pdf>.
Lake, David. 2008. The State and International Relations. In *The Oxford handbook of international relations*, edited by Christian Reus-Smit and Duncan Snidal. Oxford; New York: Oxford University Press.
Lake, David A. 2010. Rightful Rules: Authority, Order, and the Foundations of Global Governance. *International Studies Quarterly* 54 (3): 587–613.
Li, Tania Murray. 2005. Beyond 'the State' and Failed Schemes. *American Anthropologist* 107 (3): 383–394.
Lukes, Steven. 2005. *Power, Second Edition: A Radical View*. Palgrave Macmillan.
Luna, David M. 2013. Leveraging Partnerships to Combat Corruption, Money Laundering, and Illicit Networks. U.S. Department of State. Available from <http://www.state.gov/j/inl/rls/rm/2013/205899.htm>.
Lyon, David. 2006. 9/11, Synopticon, and Scopophilia: Watching and Being Watched. In *The new politics of surveillance and visibility*, edited by Richard V. Ericson and Kevin D. Haggerty. Green College thematic lecture series. Toronto: University of Toronto Press.
Lyon, David. 2003. Surveillance as Social Sorting: Computer Codes and Mobile Bodies. In *Surveillance as social sorting: privacy, risk, and digital discrimination*, edited by David Lyon, 13–29. London ; New York: Routledge.
Lyon, David. 2007. *Surveillance studies : an overview*. Cambridge, UK; Malden, MA: Polity.
Lyon, David. 2002. Surveillance Studies: Understanding visibility, mobility and the phenetic fix (editorial). *Surveillance and Society* 1 (1): 1–7.
Mann, Michael. 2008. Infrastructural Power Revisited. *Studies in Comparative International Development* 43 (3-4): 355–365.
Mann, Michael. 1984. The autonomous power of the state: its origins, mechanisms and results. *European Journal of Sociology / Archives Européennes de Sociologie* 25 (02): 185–213.
Mann, Michael. 1989. The Autonomous Power of the State: Its Origins, Mechanisms and Results. In *States in History*, edited by John A Hall, 109–136. Oxford: Basil Blackwell. Available from <http://www.sscnet.ucla.edu/soc/faculty/mann/Doc1.pdf>.
Mann, Michael. 1993. *The Sources of Social Power: Volume 2, The Rise of Classes and Nation States 1760-1914*. Cambridge [u.a.]: Cambridge Univ. Press.
Mann, Michael. 2012. *The Sources of Social Power: Volume 2, The Rise of Classes and Nation-States, 1760-1914*. Cambridge University Press.
Marquis, Greg. 2003. Private Security and Surveillance: Fromthe 'Dossier Society' to Database Networks. In *Surveillance as social sorting: privacy, risk, and digital discrimination*, edited by Lyon David, 226–248.

Mathiesen, T. 1997. The Viewer Society: Michel Foucault's `Panopticon' Revisited. *Theoretical Criminology* 1 (2): 215–234.
McJunkin, James W. 2009. *FBI Role and Lessons Learned in Mumbai Investigation*. Was. Available from <http://www.fbi.gov/news/testimony/fbi-role-and-lessons-learned-in-mumbai-investigation>.
Mill, John Stuart. 1863. *On Liberty*. Ticknor and Fields.
Miller, Greg. 2011. CIA flew stealth drones into Pakistan to monitor bin Laden house. *The Washington Post*, sec. World. Available from <http://www.washingtonpost.com/world/national-security/cia-flew-stealth-drones-into-pakistan-to-monitor-bin-laden-house/2011/05/13/AF5dW55G_story.html>. . Accessed16 October 2013.
Miller, Greg, Julie Tate, and Barton Gellman. 2013. Documents reveal NSA's extensive involvement in targeted killing program. *The Washington Post*, sec. World. Available from <http://www.washingtonpost.com/world/national-security/documents-reveal-nsas-extensive-involvement-in-targeted-killing-program/2013/10/16/29775278-3674-11e3-8a0e-4e2cf80831fc_story.html?hpid=z3>. . Accessed17 October 2013.
Miller, Martin. 1995. The Intellectual Origins of Terrorism in Modern Europe. In *Terrorism in Context*, edited by Martha Crenshaw, 27–62. University Park, Pa: Pennsylvania State University Press.
Milner, Helen. 1991. The assumption of anarchy in international relations theory: a critique. *Review of International Studies* 17 (01).
Mitchell, Paul T. 2009. *Network Centric Warfare and Coalition Operations: The New Military Operating System*. Routledge.
Mitzen, Jennifer. 2013. *Power in concert: the nineteenth-century origins of global governance*. Chicago: The University of Chicago Press.
Moravcsik, Andrew. 2004. Is there a 'Democratic Deficit' in World Politics? A Framework for Analysis. *Government and Opposition* 39 (2): 336–363.
Moss, Todd, Gunilla Pettersson, and Nicolas van de Walle. 2006. *An Aid-Institutions Paradox? A Review Essay on Aid Dependency and State Building in Sub-Saharan Africa- Working Paper 74*. The Center for Global Development. Available from <http://www.cgdev.org/publication/aid-institutions-paradox-review-essay-aid-dependency-and-state-building-sub-saharan>. . Accessed14 March 2014.
Mueller, John. 2009. *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them*. Free Press.
Mueller, John, and Mark G. Stewart. 2010. Hardly Existential. *Foreign Affairs*. Available from <http://www.foreignaffairs.com/articles/66186/john-mueller-and-mark-g-stewart/hardly-existential>. . Accessed24 January 2013.
Mueller, John, and Mark G. Stewart. 2012. The Terrorism Delusion America's Overwrought Response to September 11. *INTERNATIONAL SECURITY* 37 (1): 81+.
Mueller, Robert S. 2012. *FBI Budget Request for Fiscal Year 2013*. Washington D.C. Available from <http://www.fbi.gov/news/testimony/fbi-budget-request-for-fiscal-year-2013-1>.
Mueller, Robert S. 2011. *Ten Years After 9/11: Are We Safer?* Washington D.C. Available from <http://www.fbi.gov/news/testimony/ten-years-after-9-11-are-we-safer>.
Mullen, Mike. 2009. *Senate Armed Service Committee Testimony Regarding FY 2010 Budget Request*. Dirksen Senate Office Building, Room 106, Washington, D.C.

Available from <http://www.jcs.mil/speech.aspx?ID=1182>. . Accessed17 July 2013.
Napolitano, Janet. 2011. Remarks for DHS Secretary Janet Napolitano: CBSI Dialogue, Nassau, Bahamas. Available from <http://photos.state.gov/libraries/bahamas/8325/pdf/napolitanoremarks.pdf>.
NASA Mission and Spacecraft Library. n.d. Corona Program. *Corona Program*. Available from <http://space.jpl.nasa.gov/msl/Programs/corona.html>. . Accessed3 October 2013.
NCTC. 2013. NCTC: About Us. Available from <http://www.nctc.gov/about_us/about_nctc.html>. . Accessed4 September 2013.
New America Foundation. 2013. *The Year of the Drone*. Available from <http://counterterrorism.newamerica.net/drones>. . Accessed2 March 2013.
Nexon, Daniel H., and Thomas Wright. 2007. What's at Stake in the American Empire Debate. *American Political Science Review* 101 (02): 253–271.
Obama, Barack. 2013. Letter from the President -- Concerning Niger. Available from <http://www.whitehouse.gov/the-press-office/2013/02/22/letter-president-concerning-niger>. . Accessed17 July 2013.
Office of the Director of National Intelligence. 2011. *ODNI Congressional Budget Justification for FY 2012 (redacted)*. Available from <http://www.fas.org/irp/dni/cbjb-2012.pdf>. . Accessed11 July 2013.
Office of the Director of National Intelligence. n.d. Partner Engagement. U.S. Government. *ODNI, About the Organizataion*. Available from <http://www.odni.gov/index.php/about/organization/partner-engagement-partnerships>. . Accessed11 April 2014.
Ogata, Kenji. 2013. Japan, U.S. agree to allow joint access to fingerprint databases. *AJW by The Asahi Shimbun*. Available from <http://ajw.asahi.com/article/behind_news/social_affairs/AJ201309060070>. . Accessed31 December 2013.
Paris, Roland. 2003. The Globalization of Taxation? Electronic Commerce and the Transformation of the State. *International Studies Quarterly* 47 (2): 153–182.
Perry, Robert. 1973. *A History of Satellite Reconnaissance: Vol 1*. Declassified May 2012. National Reconnaissance Office. Available from <http://www.nro.gov/foia/docs/hosr/hosr-vol1.pdf>.
Pettit, Philip. 1996. Freedom as Antipower. *Ethics* 106 (3): 576–604.
Phillips, Andrew. 2013. The wars on terror, duelling internationalisms and the clash of purposes in a post-unipolar world. *International Politics* 50 (1): 77–96.
Picciotto, Sol. 1983. Jurisdictional Conflicts, International Law and the International State System. *International Journal of the Sociology of Law* 11: 11–40.
Picciotto, Sol. 1991. The Internationalisation of the State. *Capital and Class* 43.
Pontius, Ronald. 2011. Coalition C2/Multinational Information Sharing: Current Capabilities and Challenges presented at the 16th International Command and Control Research and Technology Symposium.
Pouliot, Vincent. 2010. *International security in practice: the politics of NATO-Russia diplomacy*. Cambridge studies in international relations 113. Cambridge, UK ; New York: Cambridge University Press.
Powell, C.H. 2012. The United Nations Security Council, terrorism and the rule of law. In *Global anti-terrorism law and policy*, edited by Victor Vridar Ramraj, 19–43. 2nd ed. Cambridge ; New York: Cambridge University Press.

Priest, Dana. 2013. NSA growth fueled by need to target terrorists. *The Washington Post*, sec. World. Available from <http://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html?tid=pm_world_pop>. . Accessed23 July 2013.
Ramotowski, Edward. 2012. *Eleven Years Later: Preventing Terrorists from Coming to America*.
Richardson, Graham T., and Robert N. Merz. 1996. *High-Resolution Commercial Imagery and Open-Source Information: Implications for Arms Control*. Intelligence Brief. U.S. Arms Control and Disarmament Agency, Bureau of Intelligence, Verification and Information Management. Intelligence, Technology, and Analysis Division. Available from <http://www.fas.org/irp/offdocs/acda.htm>.
Richelson, Jeffrey. 2007. *Declassifying the 'Fact of' Satellite Reconnaissance*. National Security Archive Electronic Briefing Book. George Washington University, National Security Archives. Available from <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB231/>.
Richelson, Jeffrey. 2012. *The U.S. intelligence community*. 6th ed. Boulder, CO: Westview Press.
Ridge, Tom. 2005. U.S., EU Security Depends on Collective Fight Against Terrorism, European Policy Centre in Brussels. Available from <http://iipdigital.usembassy.gov/st/english/texttrans/2005/01/20050113180043 1cjsamoht0.2542078.html#axzz2qaI3JA6j>.
Ringmar, Erik. 2014. The search for dialogue as a hindrance to understanding: practices as inter-paradigmatic research program. *International Theory* 6 (01): 1–27.
Risse, Thomas. 2004. Global Governance and Communicative Action. *Government and Opposition* 39 (2): 288–313.
Roach, Kent, Michael Hor, Victor Ramraj, and George Williams. 2012. Introduction. In *Global anti-terrorism law and policy*, edited by Victor Vridar Ramraj. 2nd ed. Cambridge ; New York: Cambridge University Press.
Roberts, Kristin. 2013. When the Whole World Has Drones. *National Journal*. Available from <http://www.nationaljournal.com/magazine/when-the-whole-world-has-drones-20130321>. . Accessed19 July 2013.
Rodriguez, David. 2013. *Advance Policy Questions for General David M. Rodriguez, U.S. Army Nominee for Commander, U.S. Africa Command*. Available from <http://www.armed-services.senate.gov/statemnt/2013/02%20February/Rodriguez%2002-14-13.pdf>.
Rosenau, James N, and Ernst Otto Czempiel. 1992. *Governance without government: order and change in world politics*. Cambridge [England]; New York: Cambridge University Press.
Roston, Aram. n.d. Whither The Hunter-Killers? USAF Ponders Post-Afghan Glut of Reapers, Predators. *Defense News*. Available from <http://www.defensenews.com/article/20130402/C4ISR02/304020012/Whither-Hunter-Killers-USAF-Ponders-Post-Afghan-Glut-Reapers-Predators>. . Accessed15 November 2013.
Ruffner, Kevin, ed. 1995. *Corona: America's First Satellite Program*. CIA Cold War Records. CIA Center for the Study of Intelligence. Available from <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/corona.pdf>. . Accessed16 May 2013.

Ruggie, J. G. 1993. Territoriality and beyond: problematizing modernity in international relations. *International Organization*: 139–174.
Ruggie, John Gerard. 1982. International Regimes, Transactions, and Change: Embedded Liberalism in the Postwar Economic Order. *International Organization* 36 (2): 379–415.
Rule, James. 1974. *Private lives and public surveillance: social control in the computer age*. Schocken Books.
Sandberg, A., and N. Bostrom. 2008. *Global Catastrophic Risks Survey*. Future of Humanity Institute, Oxford University.
Sandrolini, Christopher. 2012. APIS Border Security Training, Barbados. Available from <http://barbados.usembassy.gov/dcm08212012a.html>.
Schatzki, Theodore R. 2001. Introduction: practice theory. In *The Practice Turn in Contemporary Theory*, edited by Theodore R. Schatzki, Karin Knorr Cetina, and Eike von Savigny, 10–23. Routledge.
Scheppele, Kim Lane. 2010. The International Standardization of National Security Law. *Journal of National Security Law & Policy* 4: 437.
Schmitt, Eric. 2013. Drones in Niger Reflect New U.S. Tack on Terrorism. *The New York Times*, sec. World / Africa. Available from <http://www.nytimes.com/2013/07/11/world/africa/drones-in-niger-reflect-new-us-approach-in-terror-fight.html>. . Accessed25 November 2013.
Schweller, Randall L. 1994. Bandwagoning for Profit: Bringing the Revisionist State Back In. *International Security* 19 (1): 72–107.
Schweller, Randall L. 2010. Entropy and the trajectory of world politics: why polarity has become less meaningful. *Cambridge Review of International Affairs* 23 (1): 145–163.
Scott, James C. 1998. *Seeing like a state : how certain schemes to improve the human condition have failed*. New Haven: Yale University Press.
Scott, James C. 1995. State Simplifications: Nature, Space and People. *Journal of Political Philosophy* 3 (3): 191–233.
Scott, James C. 2010. The Trouble with the View from Above. *CATO Unbound*. Available from <http://www.cato-unbound.org/2010/09/08/james-c-scott/the-trouble-with-the-view-from-above/>.
Shanker, Thom, and Scott Shane. 2006. Elite Troops Get Expanded Role on Intelligence. *The New York Times*, sec. International / Americas. Available from <http://www.nytimes.com/2006/03/08/international/americas/08forces.html>. . Accessed15 January 2014.
Shaw, Martin. 2000. *Theory of the Global State: Globality as an Unfinished Revolution*. Cambridge University Press.
Shea, Timothy C. 2005. Transforming Military Diplomacy. *Joint Force Quarterly* (38): 49–52.
Sifton, John. 2012. A Brief History of Drones. *The Nation*. Available from <http://www.thenation.com/article/166124/brief-history-drones#>. . Accessed15 November 2013.
Simmons, A. John. 2001. On the Territorial Rights of States. *Philosophical Issues* 11: 300–326.
Slaughter, Anne-Marie. 2009. *A New World Order*. Princeton University Press.
Slaughter, Anne-Marie. 2004. Disaggregated Sovereignty: Towards the Public Accountability of Global Government Networks. *Government and Opposition* 39 (2): 159–190.

Soifer, Hillel. 2008. State Infrastructural Power: Approaches to Conceptualization and Measurement. *Studies in Comparative International Development* 43 (3-4): 231–251.
Stratfor - Fred Burton. 2006. *UK Plot - A few points to ponder*. Stratfor Internal Email. WikiLeaks Global Intelligence Files. Available from <http://search.wikileaks.org/gifiles/?viewemailid=3488779>.
Stratfor - Interfax Ukraine. 2011. *Ukraine's security service, FBI bust cybercrime ring (Story #100)*. Stratfor Internal Email. WikiLeaks Global Intelligence Files. Available from <http://search.wikileaks.org/gifiles/?viewemailid=814122>.
Stuart, Freundel J. 2010. Press Release: Caribbean Basin Security Initiative Inaugural Caribbean- United States Security Cooperation Dialogue. Caribbean Community Secretariat. Available from <http://www.caricom.org/jsp/speeches/caribbean_us_security_cooperation_dialogue_stuart.jsp?null&prnf=1>.
Susman, Tina, and Richard A. Serrano. 2010. Times Square bomb suspect admits involvement in failed attack. *Los Angeles Times*. Available from <http://articles.latimes.com/2010/may/04/nation/la-na-ny-bomb-20100505>. . Accessed11 April 2014.
Swiss Federal Department of Foreign Affairs. 2012. Negotiations Successful - Switzerland to Remain in the U.S. Visa Waiver Program. *News of the FDFA (Switzerland)*. Available from <http://www.eda.admin.ch/eda/en/home/recent/media/single.html?id=45147> . . Accessed31 December 2013.
Szasz, Paul C. 2002. The Security Council Starts Legislating. *The American Journal of International Law* 96 (4): 901–905.
Taubman, Philip. 2007. Failure to Launch: In Death of Spy Satellite Program, Lofty Plans and Unrealistic Bids. *The New York Times*, sec. U.S. - Washington. Available from <http://www.nytimes.com/2007/11/11/washington/11satellite.html>.
Teboho Ansorge, J. 2011. Digital Power in World Politics: Databases, Panopticons and Erwin Cuntz. *Millennium - Journal of International Studies* 40 (1): 65–83.
Tenet, George. 2004. *Written Statement for the Record of the Director of Central Intelligence Before the National Commission on Terrorist Attacks Upon the United States*. Available from <http://www.9-11commission.gov/hearings/hearing8/tenet_statement.pdf>.
The Financial Action Task Force. n.d. Who We Are. *About Us*. Available from <http://www.fatf-gafi.org/pages/aboutus/>.
The Global Counterterrorism Forum. 2011. Political Declaration. Available from <http://www.thegctf.org/documents/10162/13878/Political+Declaration.pdf>.
The Japan Times. 2013. Defense Ministry to expand military attaches in Africa to nine. *The Japan Times Online*. Available from <http://www.japantimes.co.jp/news/2013/10/27/national/defense-ministry-to-expand-military-attaches-in-africa-to-nine/>. . Accessed16 January 2014.
The U.S. Drug Enforcement Agency. n.d. International Training. *DEA Operations*. Available from <http://www.justice.gov/dea/ops/Training/IntTraining.shtml>. . Accessed20 January 2014.
The United States, and CARICOM IMPACS. 2010. Caribbean-U.S. Plan of Action on Security Cooperation.
The White House. 2003. U.S. National Strategy for Combating Terrorism.

The White House. 2006. U.S. National Strategy for Combating Terrorism. Available from <http://www.cfr.org/counterterrorism/national-strategy-combating-terrorism-2006/p11389>. . Accessed14 July 2013.
The White House. 2011. U.S. National Strategy for Counterterrorism.
Tilly, Charles. 1999. Epilogue: Now Where? In *State/culture: State-formation After the Cultural Turn*, edited by George Steinmetz, 407–20. Cornell University Press.
Torfing, Jacob. 1999. Towards a Schumpeterian workfare postnational regime: path-shaping and path-dependency in Danish welfare state reform. *Economy and Society* 28 (3): 369–402.
Turse, Nick. 2013. *The Changing Face of Empire: Special Ops, Drones, Spies, Proxy Fighters, Secret Bases, and Cyberwarfare*. Haymarket Books.
U.S. Defense Intelligence Agency. n.d. DIA Locations. *Defense Intelligence Agency*. Available from <http://www.dia.mil/About/Organization/Locations.aspx>. . Accessed18 January 2014.
U.S. Department of Defense. 2011. *Unmanned Systems Integrated Roadmap FY2011-2036*. U.S. Department of Defense.
U.S. Department of Homeland Security. 2008. Privacy Impact Assessment for the Advance Passenger Information System. Available from <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_apisfinalrule.pdf>.
U.S. Department of Homeland Security. 2013. Privacy Impact Assessment Update for the Advance Passenger Information System. Available from <https://www.dhs.gov/sites/default/files/publications/privacy-pia-apis-update-20130605.pdf>.
U.S. Department of Homeland Security, Director of Information Security Policy. 2011. DHS Sensitive Systems Policy Directive 4300A v.8. Available from <http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf>.
U.S. Department of Justice, Office of the Inspector General. 2004. Federal Bureau of Investigation Legal Attache Program: Audit Report 04-18. OIG Audit Dvisiion.
U.S. Department of State. 2010a. Caribbean-U.S. Plan of Action on Security Cooperation. Available from <http://www.state.gov/p/wha/rls/142440.htm>.
U.S. Department of State. 2011. *Country Reports on Terrorism: Chapter 2*. Available from <http://www.state.gov/j/ct/rls/crt/2010/170259.htm>.
U.S. Department of State. 2010b. Fact Sheet: The Caribbean Basin Security Initiative: A Shared Regional Security Partnership. Available from <http://www.state.gov/r/pa/scp/fs/2010/142088.htm>.
U.S. Department of State. 2010c. Joint Caribbean-United States Framework for Security Cooperation Engagement. Available from <http://www.state.gov/p/wha/rls/142442.htm>.
U.S. Department of State. 2007. *The Fiscal Year 2008 Performance Summary*. Washington D.C.
U.S. Department of State. 2013. *U.S. Department of State Congressional Budget Justification: Foreign Operations. Vol 2. FY14*.
U.S. Department of State and the Office of Inspector General. 2012. *Evaluation of the Antiterrorism Assistance Program for Countries Under the Bureaus of Near Eastern Affairs and South and Central Asian Affairs*. Office of Audits Middle East Region Operations.
U.S. Department Of State, Bureau of Counterterrorism. 2012. *Annual Report on Assistance Related to International Terrorism: Fiscal Year 2011*. Report.

Department Of State. The Office of Website Management, Bureau of Public Affairs. Available from <http://www.state.gov/j/ct/rls/other/rpt/206686.htm>. . Accessed17 December 2013.
U.S. Department Of State, Bureau of Counterterrorism. 2013. *Annual Report on Assistance Related to International Terrorism: Fiscal Year 2012*. Report. Department Of State. The Office of Website Management, Bureau of Public Affairs. Available from <http://www.state.gov/j/ct/rls/other/rpt/206686.htm>. . Accessed17 December 2013.
U.S. Department of State, Bureau of Diplomatic Security. 2009. *Diplomatic Security: Regional Security Office*.
U.S. Department of State, Bureau of Diplomatic Security. 2012. *Office of Antiterrorism Assistance: 2011 Fiscal Year in Review*. Available from <http://www.state.gov/documents/organization/195222.pdf>.
U.S. Department Of State, Bureau of Public Affairs. 2002. Terrorist Interdiction Program (TIP). Available from <http://2001-2009.state.gov/s/ct/rls/fs/2002/12676.htm>. . Accessed17 December 2013.
U.S. Department of State, INL. 2009. ILEA Statement of Purpose. Available from <http://www.state.gov/j/inl/c/crime/ilea/c11242.htm>. . Accessed20 January 2014.
U.S. DOJ Office of the Inspector General. 2007. *The Drug Enfrocement Administration's International Operations*. Audit Report. Available from <http://www.justice.gov/oig/reports/DEA/a0719/final.pdf>.
U.S. Embassy - Tanzania. 2013. *East African Security Forces Host Inaugural Special Operations Conference*. Press Release. Zanzibar, Tanzania. Available from <http://tanzania.usembassy.gov/pr_02112013.html>. . Accessed13 January 2014.
U.S. FBI, Criminal Justice Information Services Division. 2013. *Criminal Justice Information Services Law Enforcement National Data Exchange: Policy and Operating Manual*. v.3. U.S. Department of Justice. Available from <http://www.fbi.gov/about-us/cjis/n-dex/policy-and-operating-manual.pdf>.
U.S. FBI, Criminal Justice Information Services Division. 2010. Law Enforcement Records Management Systems as They Pertain to FBI Programs and Systems. Available from <http://www.fbi.gov/about-us/cjis/law-enforcement-records-management-system>. . Accessed27 December 2013.
U.S. Federal Bureau of Investigation. 2014a. A Conversation with Our Legal Attaché in Nairobi, Part 1. *FBI News Stories*. Available from <http://www.fbi.gov/news/stories/2014/january/a-conversation-with-our-legal-attache-in-nairobi-part-1/a-conversation-with-our-legal-attache-in-nairobi-part-1>. . Accessed30 January 2014.
U.S. Federal Bureau of Investigation. 2014b. A Conversation with Our Legal Attaché in Nairobi, Part 2. *FBI News Stories*. Available from <http://www.fbi.gov/news/stories/2014/january/a-conversation-with-our-legal-attache-in-nairobi-part-2/a-conversation-with-our-legal-attache-in-nairobi-part-2>. . Accessed30 January 2014.
U.S. Federal Bureau of Investigation. 2012a. *FBI Information Sharing & Safeguarding Report*. Available from <http://www.fbi.gov/stats-services/publications/national-information-sharing-strategy-1/fbi-information-sharing-and-safeguarding-report-2012>.
U.S. Federal Bureau of Investigation. 2011a. *FBI Information Sharing Report*.

U.S. Federal Bureau of Investigation. 2012b. FY 2013 Authorization and Budget Request to Congress. Available from <http://www.justice.gov/jmd/2013justification/pdf/fy13-fbi-justification.pdf>. . Accessed30 January 2014.
U.S. Federal Bureau of Investigation. 2013a. FY 2014 Authorization and Budget Request to Congress. Available from <http://www.justice.gov/jmd/2014justification/pdf/fbi-justification.pdf>. . Accessed30 January 2014.
U.S. Federal Bureau of Investigation. 2011b. International Operations - Ten Years After: The FBI Since 9/11. *FBI*. Available from <http://www.fbi.gov/about-us/ten-years-after-the-fbi-since-9-11/just-the-facts-1/international-operations>. . Accessed26 January 2014.
U.S. Federal Bureau of Investigation. 2013b. Partnerships Pay Dividends at Copenhagen Legal Attaché. *FBI New*. Available from <http://www.fbi.gov/news/stories/2013/december/partnerships-pay-dividends-at-copenhagen-legal-attache/partnerships-pay-dividends-at-copenhagen-legal-attache>. . Accessed30 January 2014.
U.S. Federal Bureau of Investigation. 2008. *The FBI: a centennial history, 1908-2008*. Washington, D.C.: U.S. Dept. of Justice, Federal Bureau of Investigation : For sale by the Supt. of Docs., U.S. G.P.O.
U.S. Government Accountability Office. 2011. *International Military Education and Training: Agencies Should Enhance Human Rights Training and Improve Evaluations*. Available from <http://www.gao.gov/new.items/d12123.pdf>. . Accessed17 July 2013.
U.S. Government Accountability Office. 2012. *Nonproliferation: Agencies Could Improve Information Sharing and End-Use Monitoring on Unmanned Aerial Vehicle Exports*. A report to the Ranking Member, Subcommittee on National Security, Homeland Defense, and Foreign Operations, Committee on Oversight and Government Reform, House of Representatives. Available from <http://www.gao.gov/products/GAO-12-536>. . Accessed17 July 2013.
U.S. Government and CARICOM. 2006. Memorandum of Intent Between the Government of the United States of American and Member States of the Caribbean Community on Co-operation Regarding the Development of an Advance Passenger Information System. Available from <http://www.caricom.org/jsp/secretariat/legal_instruments/moi_us_caricom_apis.pdf>.
U.S. Government Information Sharing Environment. n.d. A Brief History of the Information Sharing Environment (ISE). Available from <http://ise.gov/sites/default/files/Brief_History_of_the_ISE.pdf>. . Accessed3 March 2014.
U.S. House of Representatives Committee on Armed Services. 1993. *Intelligence Successes and Failures in Operations Desert Storm/Shield*.
United Nations Security Council. 2001. S/RES/1373 (2001).
US Diplomatic Cable. 2009a. *Alternate Parking for USG Aircraft in Burkina Faso*. WikiLeaks Cable. Available from <http://www.cablegatesearch.net/cable.php?id=09OUAGADOUGOU574>.
US Diplomatic Cable. 2006. *Delegation Discusses Cricket World Cup Security Issues with Jamaican Minister of National Security Peter Phillips*. WikiLeaks Cable. Available from <http://wikileaks.org/cable/2006/06/06BEIJING11758.html>.

US Diplomatic Cable. 2008. *HSPD-6 Team Visits to Discuss Terrorist Screening Information Exchange with Sweden*. WikiLeaks Cable. Available from <http://www.wikileaks.org/plusd/cables/08STOCKHOLM748_a.html>.
US Diplomatic Cable. 2009b. *Request for Establishment of a Department of Defense Position in Ouagadougou, Burkina Faso*. WikiLeaks Cable. Available from <http://www.cablegatesearch.net/cable.php?id=09OUAGADOUGOU298>.
US Diplomatic Cable. 2009c. *U.S.-Morocco Security dialogues*. WikiLeaks Cable. Available from <http://cablegatesearch.wikileaks.org/cable.php?id=09RABAT904&q=intelligence-sharing-agreement>.
US Diplomatic Cable. 2009d. *Uganda: Intelligence Sharing Agreement*. WikiLeaks Cable. Available from <http://www.cablegatesearch.net/cable.php?id=09OUAGADOUGOU298>.
Vella, Matthew. 2004. FBI May Have Its Bugs on Malta's Arrivals and Departures. *Malta Today*. Available from <http://www.maltatoday.com.mt/2004/06/27/t12.html>. . Accessed18 December 2013.
Vienna Convention on Diplomatic Relations. 1961. Entered into Force 24 April 1964.
Walsh, William H. 1951. *Introduction to Philosophy of History*. London, New York: Hutchinson's University Library.
Waltz, Kenneth. 1979. *Theory of International Politics*. McGraw-Hill.
Weber, Max, and David S. Owen. 2004. *The Vocation Lectures*. Hackett Publishing.
Weitz, Richard. 2007. Shanghai Cooperation Organization: The Primakov Vision and Central Asian Realities, The. *Fletcher Forum of World Affairs* 31: 103.
Wendt, Alexander. 1992. Anarchy is what states make of it - the social construction of power-politics. *International Organization* 46 (2): 391–425.
Wendt, Alexander. 1994. Collective Identity Formation and the International State. *The American Political Science Review* 88 (2): 384–396.
Wendt, Alexander. 2010. Flatland: quantum mind and the international system. In *New systems theories of world politics*, edited by Mathias Albert, Lars-Erik Cederman, and Alexander Wendt. Palgrave studies in international relations series. Basingstoke [England] ; New York: Palgrave Macmillan.
Wendt, Alexander. 1999. *Social theory of international politics*. Cambridge University Press.
Wendt, Alexander. 2003. Why a world state is inevitable. *European Journal of International Relations* 9 (4): 491.
Wendt, Alexander, and Daniel Friedheim. 1995. Hierarchy under Anarchy: Informal Empire and the East German State. *International Organization* 49 (4): 689–721.
White House, Office of the Press Secretary. 2001. Fact Sheet President's Speech at the Summit of the Americas. Available from <http://georgewbush-whitehouse.archives.gov/news/releases/2001/04/20010423-1.html>.
Whitlock, Craig. 2012a. Contractors run U.S. spying missions in Africa. *The Washington Post*. Available from <http://articles.washingtonpost.com/2012-06-14/world/35462335_1_contractors-missions-central-african-republic>. . Accessed19 July 2013.
Whitlock, Craig. 2012b. U.S. expands secret intelligence operations in Africa. *The Washington Post*. Available from <http://articles.washingtonpost.com/2012-06-13/world/35462541_1_burkina-faso-air-bases-sahara>. . Accessed19 July 2013.
Whitlock, Craig. 2013. U.S. military drone surveillance is expanding to hot spots beyond declared combat zones. *The Washington Post*, sec. World. Available from

<http://www.washingtonpost.com/world/national-security/us-military-drone-surveillance-is-expanding-to-hot-spots-beyond-declared-combat-zones/2013/07/20/0a57fbda-ef1c-11e2-8163-2c7021381a75_story.html?hpid=z1>. . Accessed21 July 2013.

Whitlock, Craig. 2012c. U.S. shares fruit of spy missions. *The Washington Post*. Available from <http://articles.washingtonpost.com/2012-06-14/world/35459893_1_intelligence-ugandan-joseph-kony>. . Accessed19 July 2013.

Whitlock, Craig, and Barton Gellman. 2013. To hunt Osama bin Laden, satellites watched over Abbottabad, Pakistan, and Navy SEALs. *The Washington Post*, sec. World. Available from <http://www.washingtonpost.com/world/national-security/to-hunt-osama-bin-laden-satellites-watched-over-abbottabad-pakistan-and-navy-seals/2013/08/29/8d32c1d6-10d5-11e3-b4cb-fd7ce041d814_story.html>. . Accessed16 October 2013.

Williams, Melissa S. 2009. Citizenship as Agency within Communities of Shared Fate. In *Unsettled Legitimacy: Political Community, Power, and Authority in a Global Era*, edited by Steven Bernstein and William D. Coleman, 33–52. UBC Press.

Williams, Melissa S., and Mark E. Warren. 2014. A Democratic Case for Comparative Political Theory. *Political Theory* 42 (1): 26–57.

Wintour, Patrick. 2013. David Cameron puts Algeria and Mali crises ahead of EU speech. *The Guardian*, Online edition. Available from <http://www.guardian.co.uk/politics/2013/jan/18/david-cameron-algeria-mali-eu>.

Zureik, Elia. 2003. Theorizing Surveillance. In *Surveillance as social sorting: privacy, risk, and digital discrimination*, edited by Lyon David.