Surveillance & Society

Article | Surveillance Hegemony

Jason Keiber

Otterbein University, US.
jkeiber@otterbein.edu

Abstract

The National Security Agency activity disclosed by Edward Snowden plugs into a larger information ecology made possible by US surveillance hegemony. While the revelations of the NSA's international spying ambitions have astonished, there is more to US surveillance than secretive programs carried out by its intelligence community. The US also assiduously conducts surveillance on individuals abroad through public programs negotiated with other states. These more public efforts are made possible by institutions and hortatory norms that support international surveillance. This triad of capabilities, norms, and institutions reflect US surveillance hegemony. Hegemony greases the wheels of US-led international surveillance and fosters an information ecology that feeds, and is fed by, secretive programs like those of the NSA and more public surveillance alike. This article unpacks elements of US surveillance hegemony and situates the NSA activity within the resulting information ecology.

Introduction

In 2013 Edward Snowden began revealing how busy the US National Security Agency (NSA) has been scooping up information on individuals worldwide. The capacity—and, frankly, the boldness—of the NSA makes very clear the seriousness with which the US conducts surveillance on individuals abroad. In dragnet style the NSA scoops up information and communications content from large swaths of the world's population.

In order to situate the NSA activity within the broader context of US surveillance abroad, the paper makes two claims. First, the US exercises surveillance hegemony. Hegemony requires material power (e.g. *technological* capability) and a normative and institutional framework that supports and provides legitimacy to that power. Since 9/11 strong anti-terrorism norms have evolved calling on states to develop domestic capacity to keep track of "bad guys" and share information with other states. There are institutions that promulgate this norm—such as the United Nations—and many more that facilitate information sharing on suspected terrorists more generally.

Surveillance hegemony is the reason why the US can rely on myriad avenues for surveillance.[1] The hegemonic triad of material power, legitimizing norms, and supporting international institutions greases the wheels of US efforts to get information on suspected and known terrorists throughout the world. In

[1] I do not intend to claim that any one form of surveillance is hegemonic. This is not true (Murakami Wood 2012).

Keiber, J. 2015. Surveillance Hegemony. *Surveillance & Society* 13(2): 168-181. http://www.surveillance-and-society.org | ISSN: 1477-7487

addition to secretive efforts like the NSA's, hegemony is reflected in surveillance programs with other states conducted more above board. I review two of these programs in this paper.

This leads to the second claim. US surveillance hegemony fosters an information ecology that connects secret and public surveillance efforts. Information gains in one part of the ecology has effects for other programs in the system. NSA activity cannot be fully understood without understanding how the information with which it works interacts within this information ecology.

In fleshing out US surveillance hegemony, the paper brings an International Relations (IR) perspective to Surveillance Studies to emphasize the interaction of states and the role of international norms and organizations. IR is well suited to note the ways in which states cooperate, clash, and project power abroad to collect information on individuals living in other sovereign states. In addition, focusing on the US's surveillance hegemony acts as a corrective to the obsession with NSA power. While the NSA disclosures display US technology and willingness to go-it-alone, much of the US surveillance apparatus is actually a product of cooperation and negotiation with other states and is fostered by norms and institutions.

The paper begins by looking at what we learn from Snowden's trove of documents about the US's *international* surveillance ambitions. After Snowden, we need to wipe our lenses clean and look again at how the US practices surveillance abroad. In the next section the paper explains the concept of hegemony and argues that the US is a surveillance hegemon. I then introduce two *non*-secret surveillance programs to illustrate other significant ventures that help constitute and are made possible by surveillance hegemony. In the final section of the paper I illustrate how these programs, along with the NSA, are part of an information ecology. When viewed through the hegemony lens, we see how NSA activity fits in the broader context of US surveillance activity abroad and international politics more broadly.

Surveillance and International Politics

As the interests and problems of governments have gone global, so too has "the opportunity for surveillance to appear as one of a range of solutions at that scale" (Murakami Wood 2012: 335). Recently disclosed NSA activity is a perfect example of this. States, it seems, are increasingly interested in conducting surveillance not only on their own populations but also on individuals living abroad. Global surveillance reflects and is affected by dynamics of globalization that fundamentally change how individuals interact in space and time. "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" (Lyon 2007: 125). As governments (and the private sector) seek to comprehend and influence these global social relationships forms of surveillance and information infrastructures have become globalized (Lyon 2004).

Documents provided by Edward Snowden testify to the depth of international surveillance practices. Security surveillance is no longer a domestic centered practice. Moreover, when powerful states (the US in particular) conduct international surveillance, they are often gathering information on ordinary individuals. The monitoring of millions of telephone calls in Spain (Greenwald and Aranda 2013; Gonzáles 2013) and the actual *recording* of calls in the Bahamas (Devereaux, Greenwald and Poitras 2014) are but two examples. States used to be preoccupied with learning about the behavior of other *states*. The NSA disclosures powerfully illustrate how the US has dedicated itself to the surveillance of individuals outside of its borders as well as those within.

This paper focuses on *international* surveillance by *states* that occurs when one state (working alone or with others) collects, stores, or disseminates information about people (their activity and environments) who live in foreign jurisdictions for the purposes of influence, intervention, or further surveillance. This

conceptualization of surveillance draws our attention to how states interact in the conduct of surveillance. It shifts attention to the international *politics* of surveillance and opens up questions concerning the strategic interaction of states and the role of norms and international organizations.

To better understand this particular dimension of surveillance, it will pay dividends to draw from International Relations (IR). Surveillance Studies has demonstrated a particular interest in the genealogy of the methods, concepts, and technologies of surveillance in the global context (Mattelart 2010 is a particularly good example) and often draws attention to how global surveillance facilitates neoliberalism (Murakami Wood 2013). My goal in this article is to supplement this understanding of the international dimension of surveillance with a more explicit focus on international *politics*—how states interact to achieve surveillance objectives. The intersection of Surveillance Studies and IR has already proven productive (work on the implications for borders is particularly interesting: Bigo 2008; Vaughan-Williams 2009). But more can be done.

The state centrism of IR (which can be problematic for the field) can be leveraged in an analysis of state-led global surveillance practices. Today's forms of surveillance are often networked and "rhizomatic"—interconnected and rootlike. Today's surveillance systems act as an "assemblage"—a "multiplicity of heterogeneous" sources and flows of information on individuals that are not necessarily connected or unified by design, but rather *can* connect up and function together to powerful effect. There is no concrete surveillant assemblage that one could point to as it were. Rather, "to the extent that the surveillant assemblage exists, it does so as a potentiality, one that resides at the intersections of various media that can be connected for diverse purposes" (Haggerty and Ericson 2000: 609). Rhizomatic surveillance assemblages tend to be discussed as less central and less hierarchical. As such, the interaction of states (hulking, centralized, hierarchical powers) is often neglected as surveillance scholars instead focus on more diffuse, hidden, capillary forms of surveillance power. But states still matter tremendously in international politics.

International politics is fundamentally different than domestic politics. States enjoy sovereignty and are not legally bound to an overarching authority the same way citizens are bound to their states. This makes it difficult for any one state to conduct surveillance on the citizens of a different state. Secret programs like those run by intelligence services offer one way to mitigate such difficulties. States can also try to work together. After all, there are incentives for states to cooperate on transnational issues such as terrorism and crime (Andreas and Nadelmann 2006; on the benefits of working through institutions see Keohane 2005).

Cooperation on surveillance matters, however, does not come easy. States tend to take their domestic sovereign prerogatives seriously. We shouldn't expect any state to wantonly share information about its citizens with other states. One way the US has been able to get other states and institutions to cooperate on surveillance, is through its hegemonic position in world politics.

Hegemony

Many IR scholars pay close attention to how many "great powers" there are in the world as a parsimonious way to understand how countries get along. The Cold War era was a bi-polar world dominated by the US and the Soviet Union. After the dissolution of the Soviet Union in 1991, the US remained atop in a uni-polar system. Some IR scholars see bi-polarity as very stable because it facilitates a balancing of power (Waltz 1979; for contrast, see Hopf 1991). Today, the expectation of some is that other states will eventually balance against the US by either forming alliances or shoring up their own power (Waltz 2000; Mearsheimer 1990).

Others scholars argue that a single dominant power can provide order to the system through *hegemony*.[2] Hegemony does not simply mean dominance in material power. It refers also to a dominance in the way things are done. Hegemony is reflected in a particular constellation of power, ideas and institutions which together produce stability (Cox 1981). A materially powerful actor by itself is not a hegemon. Hegemony also requires a foundation in ideas (e.g. norms and social images) that provide at least a veneer of legitimacy to the dominant actor's power and influence. Institutions, in turn, provide transmission belts for the proliferation of ideas and venues for other actors to participate in—and not resist—the social order.

Whereas in an imperial system, the dominant power sets the rules for subordinates to follow, in a hegemonic system, the dominant power sets up the rules for all—including itself, though with exceptions—to follow. Hegemony offers a "negotiated" order that benefits (or purports to benefit) states that don't go against the grain. Hegemony is still hierarchical. It is, however, hierarchy softened by legitimizing norms and (often merely quasi-) inclusive institutions.

The leading power of a hegemonic order is the prime mover in creating and protecting the major rules and institutions of international politics. IR scholar John Ikenberry explains:

> Compliance and participation within the order is ultimately ensured by a range of power capabilities available to the hegemon—military power, financial capital, market access, technology and so forth. Direct coercion is always an option in the enforcement of order, but less direct 'carrots and sticks' are also mechanisms to maintain hegemonic control.
>
> (Ikenberry 2004: 616)[3]

Today it is the US which exercises global hegemony. It runs a "political order built on 'liberal hegemonic' bargains […] public goods provision, and an unprecedented array of intergovernmental institutions and working relationships" (Ikenberry 2004: 611). The seeds of US hegemony were sown after World War II with the creation of the United Nations, the IMF, the World Bank, and GATT/WTO. The latter three institutions helped underpin an international liberal financial and trading regime. After the fall of the Soviet Union, the US with its preponderance of power became the unchallengeable supporter and protector of this liberal order (for more on the military dimension of hegemony see Posen 2003).

As a result of this broader hegemonic political order, the US has been able to establish what I call "surveillance hegemony." It is useful to make this distinction between *surveillance* hegemony from hegemony broadly construed for at least two reasons. First, the type of power at play—surveillance—cuts to the core of statehood. Everything that a state does from mere administration to the most lethal acts of coercion relies on surveillance. Second, as will be discussed further below, the ideas that support the expansion of international surveillance are more specifically reliant on security discourses, rather than the (neo)liberal discourses that underpin the broader US led hegemonic order. This last point is important because in order for the West's anti-terrorism discourse and its related security practices to spread, there needs to be a discursive fit between the agenda of the US and the norms held by the security and intelligence elites of other states. Indeed, the anti-terrorism discourse and the related counterterrorism surveillance measures it calls for is readily intelligible because it speaks the security vernacular shared by these elites. More importantly, there is good reason to believe that such a discourse is also viewed as legitimate, and *this* is where hegemony achieves a firm grip. (For a great discussion on discursive fit and hegemony see Hopf 2013: 321–323.)

---

[2] These views do not exhaust IR's understanding of international order. Complementing views that focus on the distribution of power, are those (more social) accounts that focus on ideas, interest, and identity (for a canonical statement see Wendt 1999).

[3] See also Gilpin (1983).

Surveillance Hegemony: Power, Norms and Institutions

The extraordinary material surveillance capabilities of the US is perhaps most easily "measured" by its exorbitant funding. Nearly a third of the US's $52.6 billion intelligence budget is dedicated to fighting terrorism (Gellman and Miller 2013).[4] The NSA in particular gets one fifth of the overall budget. This money sustains a talented workforce and produces cutting edge surveillance techniques. These capabilities are often put to use covertly and unilaterally. The US, however, can also influence others to participate in its broader, strategic surveillance efforts. One of the more striking examples of secret cooperation is the recently disclosed RAMPART-A program in which over a dozen countries allow the US to install equipment to "congested" cables so that the US can intercept phone and internet traffic (Gallagher 2014). With some caveats, *both* the US and the host country reportedly get access to the fruits of that surveillance. In general there are 37 states that are "approved SIGINT partners" (Greenwald 2014).

This highlights the fact that other states accept (to varying degrees) core premises of how surveillance should work on an international scale. This acceptance, in turn, rests on a broader set of norms that emphasize the threat of terrorism and the necessity of counterterrorism measures. On the normative side of the ledger, a modicum of international surveillance in the form of information sharing has become not just tolerated, but held up as a *responsibility* states owe each other. Finally there is an array of international institutions that support surveillance activities. The US has been able to use its influential position within these institutions—the UN in particular—to establish an array of information sharing practices, all of which benefit US surveillance goals.

Anti-terrorism norms existed prior to 9/11, but the attacks on that day in 2001 vaulted anti-terrorism business to the top of the agenda. Terrorism moved from *a* threat to *the predominant* threat. Pre-9/11 norms began emerging as early as the end of the 19th century as a response to anarchism (Jensen 2013), but developed more thoroughly in the 1970s (see Rapoport 2002 for more on the international dimensions of terrorism over time). The general emphasis was that states should refrain from supporting international terrorism. After 9/11 this changed into a norm urging states to actively intervene to stop international terrorism. This requires shoring up their own surveillance capacity at home and sharing information with others abroad.

For scholars and policy makers accustomed to seeing the world through a geopolitical lens, it might seem unusual (or surprising) that security norms would shift to prioritize terrorism. After all, the actual threat of terrorism to the West is marginal (Mueller and Stewart 2012; Mueller 2009). Normative change has been facilitated by several factors. First, there is a strong fit between international security discourses obsessed with terrorism and the more parochial security discourses which reference traditional state security concerns. On this score, the portrayal of terrorism as a threat to the security of all states (not just the US) is readily digestible by other governments. Second, because the targets of anti-terrorism practices are individuals and not states, any security gains by one state is not likely to be viewed as directly threatening to the security of other states. States don't perceive much of a threat to their security interests by cooperating on an anti-terrorism agenda. In IR parlance, there is no security dilemma in which the gains in security by one state threatens (inadvertently or not) the security of other states (Herz 1950; Jervis 1978). Finally, the post-9/11 world has been one where states are not preoccupied by the prospect of significant interstate war. There is geopolitical slack that allows states to focus on other issue areas.

The normative change is most clearly seen in how the US and the UN speak of counterterrorism (CT). Clearly, 9/11 had a major impact on how the US views international security. The US views CT as an international *responsibility* all states share. Among the US objectives in its earliest "National Strategy for Combating Terrorism" was to "[e]stablish and maintain an international standard of accountability with

[4] The figures represent the President's request. After sequester cuts the budget ended up being $49 billion.

regard to combating terrorism" (The White House 2003: 18). It further argued that "[s]tates that have sovereign rights also have sovereign responsibilities" that revolve around counterterrorism.

Even though the Bush administration was known for its go-it-alone attitude, international cooperation was integral to the US's CT strategy. The initial CT strategy document broke up the world up into four different types of states.

> 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.
>
> (The White House 2003: 12)

The hegemonic position of the US is evident in its CT strategies. First, the US offers carrots to "weak" states, promising 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" (The White House 2006: 16). Only a powerful state could offer (and sometimes foist upon other states) such assistance.

Second, over time the US shifts from unilateral bluster (which is implicitly backed by direct coercion) to a more international approach (which relies on US diplomatic strengths and advantages in international fora). In the 2006 CT strategy, the language of "willing and able" states persists, but the stark language from 2003 is absent. Instead, for those states "reluctant to fulfill their sovereign responsibilities to combat terrorist-related activities within their borders" the US 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" (The White House 2006: 16). This is the approach of a hegemon relying on less coercive modes of influence.

There are two watchwords throughout these documents—capacity and partnership. Both reflect US hegemony, and 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 (The White House 2011). References to "partnerships" occurred 25, 41, and 59 times in the respective years. The US sees its CT relationship with other "willing" states as that of a partnership. Partnerships with "able" states are exercised through more joint efforts. In its partnerships with weaker states the US would help build their capacity to fight terrorism—a capacity that includes surveillance. The expectation is that the US approach to surveillance would be dominated by cooperative efforts with more capable states and assistance for weaker states to shore up their domestic surveillance capability.

The United Nations (UN), often through US initiative, has also been instrumental in fostering US surveillance hegemony. Although the UN does not itself conduct surveillance it has passed significant Security Council Resolutions which have shaped international counterterrorism practices, including surveillance. 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 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 has two elements. First, states ought to develop

capacity that respects certain liberal norms but cracks down on terrorism. Second states ought to share relevant information with foreign partners. The later suggests that terrorism is a community problem, as does the very fact that the UN has tasked itself to address terrorism.

Resolution 1373 is binding on UN member states because it was passed by the Security Council (under its Chapter 7 authority). Its measures are meant 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, and prohibit 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.
>
> (Szasz 2002)[5]

Of particular interest to surveillance are the mandatory provisions in 1373 relating to sharing of information. 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.*[6]

Both provisions require, or at the very least imply, a domestic surveillance capability and an ability to convey that information to other states thereby effectively expanding surveillance across borders.

As a result of Resolution 1373 states have made changes. 1373 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 […] 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" (Scheppele 2010: 442).

The US has leaned on these UN resolutions to get other states to take CT and related surveillance seriously. According to the 2003 strategy document, the US promised to "use 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" (The

[5] See also Scheppele (2010: 440); Roach et al. (2012: 4); Johnstone (2008).

[6] Implicit in the other requirements set forth by resolution 1373, such as stopping terrorism finance and movement, is a requisite surveillance capability that enables the state to know these very things.

White House 2003: 19). Here again we see the language of "responsibility." On the one hand the US 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 establishes. For instance, the same 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." This line suggests that the legitimacy of CT norms—including information sharing between states—pre-exists the international instruments mentioned, as if the norms are justified by the simple fact that terrorism exists.

The broader counterterrorism norm is that states should cooperate in counterterrorism, and effective counterterrorism entails cooperative international surveillance of individuals. Looking at actual international surveillance practice we see two trends—the growth of information sharing and an emphasis on increasing 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 one's own bad guys. The norms are part of a shared representation of what it means to be a good steward of international security and a responsible sovereign state at home.

Other international organizations 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 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. All of the institutions enjoy buy-in from the US. Indeed, it could be argued that without the US they would be impotent.

Hegemonic Surveillance Capabilities

There are two sides to American surveillance power. One is secret and exemplified by the NSA. This surveillance hides and dissembles. The other is a more public (though not necessarily *publicized*) surveillance. Both piggyback on the general hegemonic position of the US and rely on the warp and weft of US interactions with other states and institutions. The public side of surveillance is often semi-consensual. This is not meant to suggest the absence of power (there is always power at play), but rather to highlight the more negotiated way of approaching surveillance. Without knowing more about the NSA programs, it is hard to know to what extent the US is strong arming states into partnerships.

Regardless, both forms of surveillance—the hidden and the public—are part of a broader information ecology. They feed each other. Their synergy works to feed not only the US information, but partner countries' information as well. Some surveillance programs play a more central role in this ecology. I discuss two of these below. One involves information sharing between countries. The other involves the distribution hardware to other countries for use in their surveillance activity. Both implicate and benefit from NSA activity.

Information Sharing

The US has hundreds of information sharing agreements with foreign countries,[7] many of which are minor, but one set of agreements is of particular importance. 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 individuals known or suspected to be involved in

[7] The ODNI's "Foreign Intelligence Relationship Enterprise" (FIRES) system is purported to list over 400 such agreements.

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" (Bush 2003). 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 […] to establish appropriate access to terrorism screening information of the participating governments" (Bush 2003). The result has been the proliferation of "HSPD 6 agreements" that deal with the bilateral exchange of "terrorism screening information." The US ingests the data provided by other countries adding some of it to the watchlist, and some foreign partners receive a subset of the watchlist data for their own screening purposes. The FBI has referred to the watchlist as "the world's most comprehensive and widely shared database of terrorist identities" (Healy 2009).

The watchlist is a product of hegemony. The US uses its leverage but does not command by fiat.[8] For instance, the US requires all countries participating in its Visa Waiver Program (which allows foreign citizens to travel to the US for a temporary time without a visa) to sign an HSPD 6 agreement. This is a *quid pro quo* arrangement, wherein the US gets data and the citizens of participating countries get travel benefits. It should also be noted that the US has good relationships with these countries, a product broader US hegemony.

But the benefits of participation for "partner countries" don't stop there. The US is in a position to share watchlist data—known as the Foreign Partner Extract—with its partners (some, presumably the core allies like the UK, get more routine access). Importantly, as more countries funnel their datasets of "bad guys" to the US, the US not only learns about new persons of interest, but can also triangulate across multiple sources to make better inferences about threatening individuals. As of September 2012, the US had signed over 40 of these with partner countries (Ramotowski 2012). This accounts for roughly 20 per cent of states in the world representing nearly 700 million people.[9] All this data flows to the surveillance hegemon, enabling the US to act as an international terrorism data broker—a global NCTC as it were. This feat of surveillance is described by the FBI as follows: "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" (Healy 2009).

Providing Information Systems

A second example of a public practice supporting US surveillance hegemony is a program known as PISCES. Run by the US Department of State, PISCES is a screening/watch-listing system meant to assist other countries with border security. By providing countries with the necessary hard- and software, the US intends to bolster the recipients' surveillance capacity. PISCES also provides the US an opportunity to give datasets to other countries to use on the provided system, thereby effectively outsourcing surveillance. The NSA, as we will see, is also implicated in this program.

Surveillance hegemony empowers the US to proliferate and maintain PISCES systems. Through April 2012, the system was working at 184 ports of entry across 18 states. 53 of these, across 11 states, had biometric capabilities (US Department Of State, Bureau of Counterterrorism 2013).The participating countries are considered by the US as suffering from a higher risk of terrorist transit and lacking the

[8] For an interesting window into the negotiation process, see the leaked diplomatic cable regarding US negotiations with Sweden (US Diplomatic Cable 2008).

[9] The US does not publish information about HSPD 6 agreements—the signatories or the content. However, of the "over 40" agreements, we know that all Visa Waiver participants (38 states) have signed HSPD 6 agreements.

infrastructure to address that problem.[10] States with the twin burdens of weak domestic capacity and a domestic terrorism problem are likely to be interested in accepting assistance from other states. The US, in turn, has both the technological capability and the security interests to make such an offer. Finally, because it provides training and system maintenance, the US is able to foster a dependency on its wares.

It is unclear whether or not the US has direct access to the data that gets entered into PISCES systems worldwide (or even what "direct access" would amount to). PISCES is deployed in Pakistan, but the country recently considered scrapping the system partially out of fear that US had direct access to the data. However, both Pakistani and US officials denied that this was true. In 2011 a former Pakistani Interior Minister said that the data "was never available to [the US] and was solely for the FIA's [Pakistan's FBI] use" (Imtiaz 2011). A representative from the US 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" (Imtiaz 2011). After a similar concern was raised in Malta, the US embassy clarified how PISCES is used.

> 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.
>
> (Vella 2004)

While the US might not have a direct line in or out of these systems, there are at least two ways in which the system serves a surveillance function. First, if the US wants information regarding specific individuals or travel patterns, it can make a request (Imtiaz 2011). Similarly during check-up visits, the US can make inquiries about data collection and analysis conducted by the host country.

Second, the US *provides* data to the PISCES systems to facilitate checks that would benefit US interests. A 2003 Congressional Research Service report describing US-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" (Kronstadt 2003: 10). In addition, according to a 2007 Department of State report, "TIP provided photos and travel history to 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" (US Department of State 2007: 63).

Depending on how they are set up, PISCES systems can also pull or 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" (US Department of State 2013: 161). Also, at least some PISCES systems are mentioned as having INTERPOL and Schengen II interfaces (2013: 216–7). Access to the Schengen system is presumably limited to Schengen members which run PISCES systems. However, there is no reason that installation of INTERPOL interfaces should be limited. For example a Pakistani government website describing PISCES mentions using INTERPOL data as well as "linking" to other countries' visa issuance systems.

Information Ecology

Unpacking US surveillance hegemony reveals an ecology of programs and practices that shuffles information around for analysis and development of future surveillance tasks. To continue with the

[10] The countries are: Afghanistan, Cambodia, Cote D'Ivoire, Djibouti, Ethiopia, Ghana, Iraq, Kenya, Kosovo, Macedonia, Malta, Pakistan, Tanzania, Thailand, Uganda, Yemen, Zambia, and Niger.

current examples, the NSA, HSPD 6 agreements, and PISCES systems are all part of the same surveillance system. The information obtained from each redounds and feeds the others.

The axis about which all US surveillance on suspected terrorists revolves is the National Counterterrorism Center (NCTC) and a database known as TIDE. By law, the NCTC is responsible for integrating and analyzing *all* foreign terrorism information. If the CIA or the NSA comes across new information on a terrorist suspect, it must get reported to the NCTC. The NCTC, in turn, is required to share terrorism information with other intelligence agencies and parts of the US government.

The US shores up "digital power" through databases (Teboho Ansorge 2011), the most important of which for counterterrorism purposes is the Terrorist Identities Datamart Environment (TIDE). TIDE is a centralized master-list containing information on all persons of interest related to terrorism. Run by the NCTC, it supports the entire US government's counterterrorism efforts. There are currently around 870,000 individuals listed in TIDE. The terrorism watchlist mentioned above is a subset of TIDE.[11]

The NSA, like other agencies in the intelligence community, pulls and pushes information from TIDE. "TIDE includes a great deal of intelligence information obtained through the activities of the Intelligence Community, often implicating the most sensitive sources and methods of intelligence gathering" (Clapper 2013: 5). If the NSA discovers new terrorism information from its bulk collection programs such as PRISM (Greenwald and MacAskill 2013) or SOMALGET (Devereaux, Greenwald and Poitras 2014), it is required to send this information to the NCTC. Upon review, the NCTC will decide whether the TIDE will be updated.

HSPD 6 agreements and the State Department's PISCES program also relate to TIDE. Any information gained through an HSPD 6 agreement, assuming it is credible, will end up in TIDE. While there is no public accounting of just how much the US has learned from these agreements, we can infer their importance from the diplomatic weight the US has put behind getting them signed. Not only were the agreements mandated by presidential directive, the US made travel privileges with close allies contingent on signing the agreements. Moreover, according to a 2012 information sharing report, HSPD 6 "agreements have enhanced current information already contained in the [terrorism watchlist] as well as added new identities to the [TIDE master list] and the information provided downstream to our domestic and international screening partners" (ISE Program Manager 2012: 19). Finally, we also know the watchlist data gets used frequently. In 2009, for example, the US processed over 55,000 "encounters" with individuals, of which "over 19,000 were a positive match to a watchlisted known or suspected terrorist" (ISE Program Manager 2012: 19).

The role of PISCES in the surveillance ecology is less direct. On the one hand, recent reporting suggests that the NSA has a direct line into the systems. According to reporting by the *New York Times* based on documents provided by Snowden, "In addition, the agency was working with the C.I.A. and the State Department on a program called Pisces, collecting biometric data on border crossings from a wide range of countries" (Risen and Poitras 2014). It is unclear whether or not countries using PISCES are aware of this. Since 2010, the NSA has been able to cross-reference its own biometric database, known as Pinwale, with data held by TIDE. Therefore, it is likely that data collected from PISCES systems also serves to update TIDE.

Regardless of whether the US gets direct access to data processed by PISCES, the systems play a surveillance role informed by TIDE. The US can urge those states receiving PISCES to populate the system with specific data. Used as such, travelers moving in and out of recipient states have their identities

[11] The so-called "No Fly" list is an even smaller subset of the Watchlist.

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.

In 2012, PISCES "processed an estimated 250,000 travelers every day" (US Department Of State, Bureau of Counterterrorism 2013). This is a significant achievement for US surveillance. If only one tenth of one per cent of those travelers raise a flag, there would be over 90,000 matches every year. The US has effectively delegated surveillance activity through the PISCES program.

In sum, the NSA feeds TIDE and vice versa. TIDE feeds other terrorism-related databases and activity. As other surveillance activity, both secret and public, gather information, the TIDE gets updated. Moreover, the US can push out data to other states for use in their screening and intelligence activity. This allows the US to use other states for its surveillance agenda. The entire picture reflects a surveillance ecology that circulates information to great effect.

Conclusion

I have argued that the NSA activity disclosed by Edward Snowden is but one element of US surveillance hegemony. There is a wide array of surveillance practices that serve to feed US information on individuals around the globe. However, these practices do not rest on brute material power alone. Surveillance hegemony also derives from ideas that normalize surveillance practices and institutions that concretize them.

Two examples of more public surveillance—HSPD 6 agreements and PISCES systems—showed other significant ways the US conducts surveillance on individuals abroad. Moreover, along with the NSA (and other intelligence programs) US surveillance activities form part of an information ecology. They all, in some way, rely on and contribute to data held by the NCTC and TIDE.

I want to close with two takeaways. The first speaks more directly to the relevance of this analysis to today. The second speaks to what seems to be the US's future surveillance ambitions.

Decisions by the NCTC and reflected in TIDE can literally kill people. There is a "kill list" naming individuals who might be targeted by drone strikes. The process by which individuals get "nominated" (an unfortunate term) starts with the NCTC and TIDE. According to reporting in 2012, the NCTC creates a list for, and using criteria provided by, the White House. That list receives further review by a group at the National Security Council. For those individuals who eventually get targeted, the President signs off on some and the CIA on others. The information ecology revolving around TIDE serves this undertaking. (For more the nominations process see Becker and Shane 2012; Miller 2012; Brennan 2012; for more on how the NSA has directly contributed to drone strikes see Miller, Tate and Gellman 2013). The potential for enormous consequences is all the more reason to take state-led surveillance practices seriously.

The second takeaway concerns the future. US surveillance hegemony suggests—and the recently disclosed NSA activity makes clear—an ambition to insinuate state power into the lives of people across the globe. Even if the US makes reforms to address these concerns *domestically*, the US is unlikely to significantly dial down its *foreign* surveillance activity. Underpinned as it is by hegemony, the US has coopted others—particularly the UK (MacAskill et al. 2013)—into playing integral roles in global surveillance. The goal, it seems, is to make populations everywhere "legible" to the US (Scott 1998). This "conquest of illegibility" is quintessentially a state making activity. If the present continues on the trajectory of *more* surveillance by states over individuals globally, surveillance will be normalized as a global phenomenon dealt with by international—not domestic—states structures. It could be argued that what we are seeing is an instance of international state formation along a particular dimension of state power. There are obvious implications for those concerned with privacy and the democratic deficit of

international state power. While privacy concerns may seem increasingly quaint in the digital age, *global* publics will surely clamor for more accountability and transparency. Whether or not enough pressure builds for states to make meaningful changes remains to be seen.

References

Andreas, Peter and Ethan Avram Nadelmann. 2006. *Policing the Globe: Criminalization and Crime Control in International Relations*. Oxford; New York: Oxford University Press.

Becker, Jo and Scott Shane. 2012. "Secret 'Kill List' Tests Obama's Principles." *The New York Times*, May 29, sec. World. http://www.nytimes.com/2012/05/29/world/obamas-leadership-in-war-on-al-qaeda.html.

Bigo, Didier. 2008 "Globalized (In)Security: The field and the Ban-Opticon" in Bigo, D and Anastassia Tsoukala, eds. *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*. Routledge Studies in Liberty and Security. London ; New York: Routledge.

Brennan, John. 2012. "The Efficacy and Ethics of U.S. Counterterrorism Strategy." *Wilson Center*, April 30. http://www.wilsoncenter.org/event/the-efficacy-and-ethics-us-counterterrorism-strategy.

Bush, George W. 2003. "Homeland Security Presidential Directive / HSPD-6." https://www.fas.org/irp/offdocs/nspd/hspd-6.html.

Clapper, James R. 2013. Rahinah Ibrahim v. Department of Homeland Security, et al. Declaration of James R. Clapper, Director of National Intelligence. U.S. District Court, Northern District of California. San Francisco Division.

Cox, Robert W. 1981. "Social Forces, States and World Orders: Beyond International Relations Theory." *Millennium - Journal of International Studies* 10 (2): 126–55.

Devereaux, Ryan, Glenn Greenwald and Laura Poitras. 2014. "Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas." *The Intercept*. https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/.

Gallagher, Ryan. 2014. "How Secret Partners Expand NSA's Surveillance Dragnet." *The Intercept*, June 18. https://firstlook.org/theintercept/article/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/.

Gellman, Barton and Greg Miller. 2013. "'Black Budget' Summary Details U.S. Spy Network's Successes, Failures and Objectives." *Washington Post*, August 29. http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html.

Gilpin, Robert. 1983. *War and Change in World Politics*. Cambridge: Cambridge University Press.

Gonzáles, Miguel. 2013. "Washington controló millones de llamadas y espió a políticos en España." *El País*, October 24. http://internacional.elpais.com/internacional/2013/10/24/actualidad/1382642579_515479.html.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Metropolitan Books.

———. and Germán Aranda. 2013. "La NSA Espió 60 Millones de Llamadas En España En Sólo Un Mes." *El Mundo*, October 28. http://www.elmundo.es/espana/2013/10/28/526dcbad61fd3d07678b456b.html.

———. and Ewen MacAskill. 2013. "Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data." *The Guardian*, June 11, sec. World news. http://www.guardian.co.uk/world/2013/jun/08/nsa-boundless-informant-global-datamining#zoomed-picture.

Haggerty, Kevin D. and Richard V. Ericson. 2000. "The Surveillant Assemblage." *The British Journal of Sociology* 51 (4): 605–22.

Healy, Timothy. 2009. "The Terrorist Screening Center and Its Role in Combating Terrorist Travel." http://www.fbi.gov/news/testimony/the-terrorist-screening-center-and-its-role-in-combating-terrorist-travel.

Herz, John H. 1950. "Idealist Internationalism and the Security Dilemma." *World Politics* 2 (02): 157–80.

Hopf, Ted. 1991. "Polarity, the Offensive-Defense Balance, and War." *American Political Science Review* 85 (2): 475–93.

———. 2013. "Common-Sense Constructivism and Hegemony in World Politics." *International Organization* 67 (02): 317–54.

Ikenberry, G. John. 2004. "Liberalism and Empire: Logics of Order in the American Unipolar Age." *Review of International Studies* 30 (04).

Imtiaz, Saba. 2011. "Pakistan to Replace 'Insecure' US Border Watch Software." *The Express Tribune*, June 8. http://tribune.com.pk/story/184568/pakistan-to-replace-insecure-us-border-watch-software/.

ISE Program Manager. 2012. Information Sharing Environment Annual Report 2012. http://ise.gov/sites/default/files/ISE_Annual_Report_to_Congress_2012.pdf.

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: Routledge.

Jervis, Robert. 1978. "Cooperation under the Security Dilemma." *World Politics* 30 (02): 167–214.

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.

Keohane, Robert O. 2005. *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton Classic Editions). 1st Princeton Classic Ed edition. Princeton, NJ: Princeton University Press.

Kronstadt, K. Alan. 2003. *Pakistan-U.S. Anti-Terrorism Cooperation*. Congressional Research Service RL31624. Congressional Research Service. http://www.fas.org/man/crs/RL31624.pdf.

Lyon, David. 2004. "Globalizing Surveillance: Comparative and Sociological Perspectives." *International Sociology* 19 (2): 135–49.
———. 2007. *Surveillance Studies : An Overview*. Cambridge, UK; Malden, MA: Polity.
MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies and James Ball. 2013. "GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications." *The Guardian*, June 21, sec. UK news. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
Mattelart, Armand. 2010. *The Globalization of Surveillance*. Cambridge: Polity.
Mearsheimer, John J. 1990. "Back to the Future: Instability in Europe after the Cold War." *International Security* 15 (1): 5-56
Miller, Greg. 2012. "Plan for Hunting Terrorists Signals U.S. Intends to Keep Adding Names to Kill Lists." *Washington Post*, October 23. http://www.washingtonpost.com/world/national-security/plan-for-hunting-terrorists-signals-us-intends-to-keep-adding-names-to-kill-lists/2012/10/23/4789b2ae-18b3-11e2-a55c-39408fbe6a4b_story.html.
———., Julie Tate and Barton Gellman. 2013. "Documents Reveal NSA's Extensive Involvement in Targeted Killing Program." *The Washington Post*, October 17, sec. World. 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.
Mueller, John. 2009. *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them*. Free Press.
———. and Mark G. Stewart. 2012. "The Terrorism Delusion America's Overwrought Response to September 11." *International Security* 37 (1): 81-110.
Murakami Wood, David. 2012. "Globalization and Surveillance." In *Routledge Handbook of Surveillance Studies*, edited by Kirstie S. Ball, Kevin D. Haggerty, and David Lyon, 333–42. Florence, KY, USA: Routledge.
———. 2013. "What Is Global Surveillance? Towards a Relational Political Economy of the Global Surveillant Assemblage." *Geoforum* 49 (October): 317–26.
Posen, Barry R. 2003. "Command of the Commons: The Military Foundation of U.S. Hegemony." *International Security* 28 (1): 5–46.
Ramotowski, Edward. 2012. *Eleven Years Later: Preventing Terrorists from Coming to America*.
Rapoport, David C. 2002. "The Four Waves of Rebel Terror and September 11." *Anthropoetics* 8 (1).
Risen, James and Laura Poitras. 2014. "N.S.A. Collecting Millions of Faces From Web Images." The *New York Times*, May 31. http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html.
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.
Scheppele, Kim Lane. 2010. "The International Standardization of National Security Law." *Journal of National Security Law & Policy*: 437.
Scott, James C. 1998. *Seeing like a State : How Certain Schemes to Improve the Human Condition Have Failed*. New Haven: Yale University Press.
Szasz, Paul C. 2002. "The Security Council Starts Legislating." *The American Journal of International Law* 96 (4): 901–5.
Teboho Ansorge, J. 2011. "Digital Power in World Politics: Databases, Panopticons and Erwin Cuntz." *Millennium - Journal of International Studies* 40 (1): 65–83.
The White House. 2003. "U.S. National Strategy for Combating Terrorism." https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf.
———. 2006. "U.S. National Strategy for Combating Terrorism." http://www.cfr.org/counterterrorism/national-strategy-combating-terrorism-2006/p11389.
———. 2011. "U.S. National Strategy for Counterterrorism." https://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf.
US Department of State. 2007. The Fiscal Year 2008 Performance Summary. 11359. Washington D.C.
———. 2013. U.S. Department of State Congressional Budget Justification: Foreign Operations. Vol 2. FY14.
US 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. http://www.state.gov/j/ct/rls/other/rpt/206686.htm.
US Diplomatic Cable. 2008. HSPD-6 Team Visits to Discuss Terrorist Screening Information Exchange with Sweden. 08STOCKHOLM748_a. WikiLeaks Cable. http://www.wikileaks.org/plusd/cables/08STOCKHOLM748_a.html.
Vaughan-Williams, Nick. 2009. *Border Politics: The Limits of Sovereign Power*. Edinburgh: Edinburgh University Press.
Vella, Matthew. 2004. "FBI May Have Its Bugs on Malta's Arrivals and Departures." *Malta Today*, June 27. http://www.maltatoday.com.mt/2004/06/27/t12.html.
Waltz, Kenneth. 1979. *Theory of International Politics*. New York: McGraw-Hill.
———. 2000. "Structural Realism after the Cold War." *International Security* 25 (1): 5–41.
Wendt, Alexander. 1999. *Social Theory of International Politics*. Cambridge: Cambridge University Press.