



Calhoun: The NPS Institutional Archive
DSpace Repository

NPS Scholarship

Publications

2018

A Crisis of Trust in Transatlantic Cybersecurity Relations in the Post-Snowden Era

Maness, Ryan

Maness, Ryan C. "A Crisis of Trust in Transatlantic Cybersecurity Relations in the Post-Snowden Era." (2018)

<https://hdl.handle.net/10945/63123>

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>

A Crisis of Trust in Transatlantic Cybersecurity Relations in the Post-Snowden Era

Ryan C. Maness
Assistant Professor
Defense Analysis Department
Naval Postgraduate School
Monterey, CA, USA
rmaness@nps.edu

Abstract: A crisis of trust between the United States and its European allies has existed since the advent of the leaked classified documents by whistleblower Edward Snowden, who exposed the potential overreach of digital surveillance by the National Security Agency (NSA). Disagreements over privacy, security, and individual liberty has put the US at odds with its European friends. As the Obama Administration worked to rectify the past overreach by the NSA and implement more oversight on the agency, another crisis has engulfed the West; the rise of populist platforms with Russian cyber and information warfare accompanying these movements. With the United States electing populist candidate Donald Trump as president, the crisis of transatlantic trust has widened further with the new administration's "America First" policies. This chapter addresses potential avenues for resilience as both sides of the Atlantic endure the populist phenomenon while striking a balance between security and individual liberty on the one hand, and keeping the transatlantic bond intact on the other.

Keywords: Cybersecurity, cyber espionage, information warfare, transatlantic relations, resiliency

Introduction

Cyber conflict and security is becoming one of the defining issues of the 21st century. As countries of the transatlantic alliance continue to be victimized in both the private and public sectors, policies and modes of behavior have continued to develop alongside this growing international security concern. High-profile breaches on the United States such as the Sony hack (2014)¹, the OPM data breach (2015)², and the Russian cyber and information operations during the recent presidential election in 2016 (ODNI Report 2017) have led to different reactions from the US government, with some retaliatory actions in the form of economic sanctions, and others toward diplomatic reconciliation and bilateral agreements, where modes of behavior are normalized. Yet there remains a gaping divide for policymakers, scholars, and media pundits on both sides of the Atlantic regarding the best way to deal with reducing data breaches, when to act offensively in the cyber realm, and retaliating against international adversaries for violating private and government networks.³ These disagreements have widened after the Edward Snowden revelations, exposing US National Security Agency (NSA) and the UK's Government Surveillance Headquarters (GCHQ) surveillance action on friend and foe alike.

For eight years, the Obama Administration restrained American cyber power from overt cyber coercive action or computer network attacks (CAN); with the exception being Stuxnet and the Olympic Games campaign on Iran's nuclear program (Lindsay 2013). This was an operation started by the Bush Administration and continued under Obama, and the combined use of cyber espionage and degradation through physical destruction of centrifuges was an act of sabotage never before seen. The impact of this sophisticated cyber campaign was limited, however, as Iran actually put more centrifuges online after the malware was discovered, and it was the weight of the economic sanctions that finally broke Iran and brought them to the negotiating table for the Iran Deal with the UN's Security Council (Valeriano and Maness 2015). However, this overt use of cyber weaponry by the global hegemon arguably ushered in a more permissive normative system of the use of cyber tactics by other state actors. Indeed, Maness and Valeriano (2016) find that cyber incidents between states have been on the rise since the Stuxnet worm's discovery, and a sizable portion of this uptick in cyber aggression has been against American networks. This seemingly more permissive norm of the use of cyber tactics has led to a growing number of policymakers to support more aggressive offensive retaliatory actions.

Obama has responded to American victimization of data breaches with relative restraint. Responses to high profile breaches such as Sony, various Chinese espionage attacks, and Russian election meddling have been met with economic sanctions on certain individuals.⁴ The backlash to OPM on the administration was harsh, and he used the opportunity of Chinese President Xi Jinping's state visit in September 2015 to diplomatically persuade Xi to stop the hacks of US private intellectual property and non-military parts of the government. Chinese cyber espionage,

¹ Andrea Peterson. "The Sony Pictures hack, explained." *The Washington Post*, 12/18/2014, accessed 2/27/2017, https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.c9c091d34b59

² Brenden I. Koerner. "Inside the Cyberattack that shocked the US government." *Wired*, 10/23/2016, accessed 3/5/2017, <https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/>

³ Jason Murdock. "US faces uphill battle over China retaliation following OPM hack," *V3*, 8/4/2015, accessed 3/2/2017, <http://www.v3.co.uk/v3-uk/news/2420391/us-considers-retaliation-against-china-after-opm-cyber-attacks>

⁴ Beth Rowen. "Cyberwar Timeline." *Info Please*, accessed 3/8/2017, <http://www.infoplease.com/world/events/cyberwar-timeline.html>

although not fully eliminated, has been significantly reduced since this high-level meeting.⁵ Besides pragmatic individual responses to international incidents, the Obama Administration has signed legislation such as the Cybersecurity Information Sharing Act (2015)⁶ and issued executive orders such as the Cybersecurity National Action Plan (2016).⁷ Internationally, the administration has promoted the adoption of norms of restraint by states in such venues as the UN, the G20, and G7, as well as bilateral agreements with various states.⁸ At the time of this writing, it seems as if not much has changed in terms of responses to data breaches with the Trump Administration.

However, it has been computer network exploitation (CNE) by the NSA that has brought a crisis in trust between the United States and its allies, and has also arguably emboldened its two top competitors, Russia and China, to act more aggressively in the digital realm (Easley 2014). The Snowden revelations took the high ground away from the US in terms of naming and shaming Russia and China for their recent cyber antics, and can arguably be the tipping point for bolder cyber actions by Russia in the body politics of Western countries (Kaplan 2016). Furthermore, the non-English speaking allies not comprised of the Five Eyes coalition, which includes the US, UK, Canada, Australia, and New Zealand, have felt slighted by the lack of disclosure of these metadata exploitations that even went as far as to listen in on German Chancellor Angela Merkel's mobile phone (Bauman et. al. 2014).

The Snowden revelations have therefore created a crisis in trust in cybersecurity relations between the United States and its European (and other) allies. Spearheaded by Germany and Brazil, discussions of circumventing US servers to keep out of NSA reach, calls for fresh norms that stigmatize this sort of metadata collection and perceived sovereign overreach, and went as far to argue that in the pursuit of its own national security interests, the United States had been imperiling the national security of its allies (Bauman et. al. 2014). As the Obama Administration worked to rectify the lack of oversight over the NSA by appointing an independent commission to audit the agency, a new threat began to emerge in Western cyberspace from Russia. Russian cyber and information warfare on the body politics of Western countries is the new cyber threat, and the transatlantic alliance can and should find ways to work together to counter this threat, and these prescriptions will be presented in the following pages.

This chapter is structured as follows: the next section will look at how the fallout between the United States and its European allies evolved after NSA contractor Edward Snowden released roughly 1.5 million documents to the press and then subsequently running to Moscow to avoid extradition. Russia as the new main threat to the transatlantic alliance in the cyber domain will then be unpacked; then a discussion of international norms and how they are being applied to the cyber realm as well as their potential to further constrain malicious behavior from

⁵ Fireeye Isight Intelligence. "Red Line Drawn: China Recalculates its Use of Cyber Espionage." *Fireeye*, accessed 3/2/2017, <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf>

⁶ S.754: Cybersecurity Information Sharing Act of 2015: available at: <https://www.congress.gov/bill/114th-congress/senate-bill/754>

⁷ The White House. "Cybersecurity National Action Plan." Available at: <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>

⁸ NATO CCE COE. "2015 UN GGE Report: Major Players Recommending Norms of Behavior, Highlighting Aspects of International Law." 8/31/2015, accessed 2/23/2017, <https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html>

Cody M. Poplin. "Cyber Sections of the Latest G20 Leaders' Communique." *Lawfare Blog*, 11/17/2015, accessed 3/4/2017, <https://www.lawfareblog.com/cyber-sections-latest-g20-leaders-communiqu%C3%A9>

The White House. "G7 Ise-Shima Leaders' Declaration." Available at: <https://obamawhitehouse.archives.gov/the-press-office/2016/05/27/g7-ise-shima-leaders-declaration>

international actors and reigning in the NSA's metadata collection program (or not). Implications for the transatlantic alliance of Europe and the United States (as well as Canada) will then be discussed in light of the Trump Administration's National Security Strategy (NSS) and what that may mean for cooperation on cyber security policy. Concluding remarks will wrap things up.

Caught Red-Handed: NSA Metadata Collection and the War on Terror

In June of 2013 the United States had been naming and shaming the Chinese government and its People's Liberation Army (PLA) for its malicious activity in American networks in both the public and private spheres (Kaplan 2016). The Lockheed-Martin theft of the plans of the F-35 fighter jet, the cyber espionage launched against the New York Times, and several hacks of government entities including the Energy Department, the White House, and even the Pentagon (Maness et. al. 2017) were public knowledge and used by the Obama Administration to push for norms of behavior in cyberspace, which cited China as the example of what not to do in the domain (Kaplan 2016). Obama was scheduled to meet with Chinese President Xi Jinping at a summit on June 7-8, 2013, with Chinese cyber malfeasance on the top of the agenda. However, on June 6 of that year, *The Washington Post* and *The Guardian* exposed troves of stolen unclassified data about the NSA's clandestine metadata collection activities that arguably broke numerous domestic privacy laws as well as international human rights laws (Bauman et. al. 2014). Obama's high ground was lost, and fallout from these revelations was widespread, with friend and foe alike. The Obama-Xi summit promptly fell apart.

The global public was outraged. A July 2014 Pew Global Attitudes and Trends poll found that supermajorities in countries including China, Russia, Germany, France, the United Kingdom, and Israel disapproved of the NSA being able to spy on the citizens of their country.⁹ In contrast, 47 percent of Americans surveyed disapproved of the NSA's actions, with 49 percent of US citizens approving of them.¹⁰ With Americans evenly divided over this issue, and most of the world overwhelmingly against it, the United States found itself as a pariah and an irresponsible superpower with way too many unchecked capabilities that could imperil the national security of various countries. For China and Russia, the Snowden revelations emboldened their push for digital sovereignty and securitization of the internet. The Snowden revelations could also very well be responsible for the uptick in Chinese cyber espionage until the OPM hack was revealed and the ongoing Russian cyber and disinformation campaigns.

For the European as well as other democracies, talks of circumventing US (and UK) servers if the NSA and GCHQ continued its perceived overreach into the private activities of its citizens as well as its sovereign cyberspace (Bauman et. al. 2014). The assault on NSA activity from the democratic world was therefore twofold: to frame unauthorized surveillance of private citizens as a violation of human rights through the UN Human Rights Council, and to sympathize with America's authoritarian adversaries with proposals of circumventing US jurisdiction in cyberspace. At the time of the Snowden leaks, nearly 80 percent of internet traffic passed through US territory via private and public servers, which gave the NSA the ability to legally access most of the world's internet traffic in terms of domestic US law (Bauman et. al. 2014). However, as the entire world turned against the United States as a result of this perceived

⁹ Pew Research Center 2014: Global Attitudes and Trends, *Global Attitudes and Trends*, 7/14/2014, accessed 12/13/2017, <http://www.pewglobal.org/2014/07/14/nsa-opinion/table/country-citizens/>

¹⁰ Pew Research Center 2014.

overreach, the Obama Administration moved to rectify the situation and reassure its allies that the NSA's spying on their citizens would no longer happen without permission (Kaplan 2016).

President Obama appointed a five-person independent commission to audit the NSA's practices to see if it had been operating in accordance with US law as well as uncover this massive data collection effort had actually been producing results in terms of preventing terrorist attacks, countering state cyber campaigns, and preventing private sector data breaches. What became to be known as the "Five Guys" report, the document made recommendations that reinforced the legitimacy of the NSA's metadata collection program, as well as recommendations that balanced privacy and security as well as be more transparent to key US allies outside of the Five Eyes alliance, such as France, Germany, Japan, and South Korea (Clarke et. al. 2013). Furthermore, although the NSA had been operating within the confines of existing US law, the metadata collection was too clandestine, without sufficient congressional oversight, and too much power was in the hands of one position, the dual hat commander of both the NSA and Cyber Command, the latter being a new organization created in 2010. The warrants granted by top-secret FISA courts, the report noted, had also been issuing without adequate oversight. It seemed as if the Obama Administration had been taking proactive steps to reassure the American public, Congress, and America's allies that it was acting in a responsible manner with its cyber surveillance practices (Kaplan 2016).

One of the first steps toward more accountability for these secretive programs was to split the NSA and US Cyber Command under different commands. The NSA would continue its clandestine activities under Title 50 under US law, which allows them their continued surveillance of the digital landscape within its jurisdiction, under a separate commander than Cyber Command (Thaler et. al. 2016). The latter would have Title 10 authority, which allowed it to conduct offensive cyber operations against foreign entities deemed a threat to US national security (Diebert 2015). Another change was the storage of the metadata outside of Fort Meade, NSA's secretive headquarters, and stored with various telecom companies. The NSA would then obtain warrants to access specific files pertinent to any investigation. Another recommendation was to have a liaison between the NSA and the elected branches of government, including the president and Congress, to update them on activities of the organization periodically to ensure oversight and prevent potential abuse by the agency (Clarke et. al. 2013).

The group of experts felt satisfied in restoring public trust in the intelligence community. Command of US cyber operations and surveillance was to be split, data was to be stored offsite and only accessible through court approval, and accountability to the elected representatives of the American people was to be established. US allies would be given notice if the NSA was to penetrate the sovereign cyberspace for US national security purposes. Furthermore, the group found that no boundaries had been overstepped by the NSA, although the potential for abuse had been present (Clarke et. al. 2013). The NSA had been operating within the confines of US law, and this was good enough for them. However, these recommendations and policies were met with ridicule and cynicism by friend and foe alike, and Germany and Brazil continued their campaign against US overreach in the United Nations (Bauman et. al. 2013).

In December of 2013 and then later in September of 2014, the UN Human Rights Council, comprised of 47 states, was focused on framing the privacy and mass surveillance issue as one of human rights, and attempted to garner support from all of the current members (Bauman et. al. 2014). One of the main narratives (led by the Germans and Brazilians) is that as the global hegemon and leader of the free world, the United States had unique responsibilities to pursue its national security with privacy, human rights, and the rule of law being preserved first

and foremost, with security playing a secondary role to these liberal ideals. The United States collective mind, with 9/11 in mind, as well as public angst against Edward Snowden's activities as much as support for them, disagreed with this outlook on digital surveillance, and pointed to the NSA's operations working within US statutes and codes, even if that breached other nation's sovereign cyberspace. Illiberal states such as Russia, Cuba, Iran, and China also condemned this German-Brazilian led push against digital surveillance, pointing to these countries' hypocrisies in that their intelligence agencies are no less guilty when surveilling domestic populations (Bauman et. al. 2014). The push for more responsible digital surveillance, at least among the liberal nations of the world in the UN, was having trouble making traction in terms of consensus.

The Obama Administration was satisfied with the findings and recommendations of the Five Guys report, and enacted the recommendations highlighted above. Obama himself noted that the NSA had been operating legally and in the interests of US national security, without violating the privacy rights of American citizens (Kaplan 2016). The 44th president also reassured concerned allies, the most vocal being Germany, France, and Brazil, that he would direct the NSA as well as Cyber Command to loop their respective intelligence agencies in if their sovereign cyberspace were to be breached in any of these surveillance operations (Diebert 2015). Public support for privacy over security grew in Europe, while the opposite dynamic continued in the United States.¹¹ A crisis in trust would continue within the transatlantic alliance and the US would continue its metadata collection program, albeit in a reformed manner. The public outing of the data breach of the OPM, which compromised the personal information of 20 million federal employees and contractors, shifted the Obama Administration's focus away from satisfying its European allies' concerns with NSA activity (Fonseca and Rosen 2017).

US public fallout with trust in government operations in cyberspace shifted to one of overreach to one of incompetence. How could a cyber superpower let something like this happen? The Chinese breach of a federal agency with the information on every employee and government contractor with a security clearance was an enormous intelligence failure, as well as an international embarrassment (Kaplan 2016). The United States looked to shore up its defenses and be more resilient rather than appeasing its allies for something it, for the most part, had little issue with in the first place. Obama and Chinese President Xi Jinping came to a diplomatic agreement in September of 2015 during the latter's state visit to the United States that each government would not knowingly hack the other's private networks or intellectual property, as well as non-military parts of their governments.¹² Furthermore, the CNAP executive order encouraged non-military parts of the US government to update operating systems, software, and hardware, as well as encourage better cyber hygiene for federal employees when operating on government networks.¹³ The focus to cyber defense and resilience also reinforced the need for continued NSA surveillance for future cyber threats in light of this data breach. Regaining trust in the transatlantic alliance, would have to wait. Then in November of 2016, everything in the United States changed. A new president had been elected, and many attributed Russian cyber and disinformation campaigns to Donald Trump's victory (ODNI Report 2017).

¹¹ Pew Research Center 2014.

¹² The White House. "Fact Sheet: President Xi Jinping's State Visit to the United States," <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>

¹³ The White House. "Cybersecurity National Action Plan." Available at: <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>

The New Russian Information Warfare Threat to Transatlantic Cybersecurity

Relations between the United States and its European allies and Russia have been souring very quickly since 2014, with disagreements over the Ukrainian civil unrest and later civil war (Birchfield and Young 2017). Although Russian-Western relations had been deteriorating steadily for years, it was the crisis in Ukraine that brought the relations to a head. The geopolitical as well as historical importance of Ukraine to Russia was underestimated by Western governments, and when pro-Moscow President Viktor Yanukovich was ousted as a result of popular unrest, Russian President Vladimir Putin saw this as a direct threat by the West to Russia's national security (Ambrosio 2017). Making moves such as annexing the Crimean Peninsula into Russia, sending troops and supplies into eastern Ukraine to support separatists against Kyiv, and launching numerous cyber attacks in Ukraine, Russia upped the ante in its dispute with the West over the fate of Ukraine (Snegovaya 2015). The West, led by the United States, responded with crippling sanctions on the Russian government, companies, and individuals. Since 2015, the conflict in Ukraine has stalemated and the Russians have held steadfast in the face of these sanctions (Ashford 2016).

Outmatched militarily and economically by the West, and with the nuclear deterrent in play, Moscow has few options to pursue its national interests as its post-Soviet self (Maness and Valeriano 2015). However, with an issue such as Ukraine being so salient to Russian interests and identity, the Kremlin has been utilizing its cyber and information capabilities to undermine the West. Known as reflexive control theory or non-linear warfare (Snegovaya 2015, Giles 2016), Russia has incorporated the cyber domain into its national security strategy for the new century. Reflexive control is the idea of convincing your adversary to make decisions that are in line with your national interests by using overt propaganda and covert espionage to inject a narrative that is accepted by citizens and eventually adopted by the government (Snegovaya 2015). This theory has been around since the 1970s and Soviet times, and has been adopted, arguably more successfully, in the digital age. As a diminished power, Russia must project its power in unconventional ways, and it seems in the cyber domain it has found its niche (Maness and Valeriano 2015).

Russia has been penetrating Western government and private networks for some time, but it is after 2014 that we see a huge uptick in Russian cyber activity on the West (Maness et. al. 2017). Seen as a reaction to Western sanctions and paranoia about future Western incursions into post-Soviet space, Russian cyber and information warfare has attempted to sow discontent and division in the minds of the Western public, distrust in its democratic institutions, and polarization of its various body politics (Maness 2018). The most high-profile political event in the West where Russian cyber malfeasance has been attributed is the election of populist candidate Donald Trump to the US presidency (ODNI Report 2017). Although causal links between Russian cyber and information activities and the election of Donald Trump are slim, there is no question that Russian activities were directed to make the Democratic candidate, Hillary Clinton, appear corrupt, incompetent, and dangerous if elected. The clear goal was to undermine her legitimacy as a candidate, as well as sow discontent among the American voters and political parties (ODNI Report 2017). Although it remains to be seen whether electing Trump was Moscow's ultimate goal, the goal of undermining American democratic institutions such as the justice system, free press, and civic discourse did take hold in the United States.

The US was not the only Western country to suffer Russian cyber and information warfare activities. Russian digital malice was found in the Brexit referendum campaign in the

UK in 2016, the French presidential election in 2017, the German parliamentary elections of 2017, and the Catalanian independence movement in Spain in 2017, among others (Maness 2018). All Russian actions were anti-status quo policy or candidate, and usually promoted the populist movement or candidate that were on the political fringes (Maness 2018). A new threat in the cyber domain has engulfed the West from its familiar nemesis, the Russian Federation. The transatlantic alliance now has the opportunity to unite under a common threat, with the hope that past disagreements be forsaken for the present danger at hand. The questions that remain are first, will the West unite, especially with Donald Trump as US president and, if so, how will it unite with the US and much of continental Europe at odds in terms of privacy and digital surveillance? There is reason for doubt as well as hope given the contents of the Trump Administration's December 2017 National Security Strategy (NSS), which promotes a realpolitik, zero-sum strategy against Russia, China, Iran, and North Korea, but at the same time encourages a strengthening of trust and information sharing with US allies (White House 2017). The promotion of cyber norms among like-minded democracies that are united against more illiberal regimes' recent practices in cyberspace, such as Chinese industrial espionage and Russian disinformation campaigns, is a forum where the US even under the Trump Administration can find common ground with the status quo governments of Europe.

Norms and Cyberspace

The US NSS, released in December 2017, prioritizes critical infrastructure as the main risk in the digital realm, and that deterrence strategies need to be developed to prevent such actions from malicious actors (White House 2017). This is assuming that cyber-attacks will not only grow in number but also in severity, where escalation will be the future if deterrence mechanisms cannot be put into place. This would require developing sophisticated cyber weapons, communicating these capabilities to potential adversaries in the cyber realm, and being willing to follow through with action that may harm civilians, lead to escalatory retaliation, and provide enemies with digital technologies they did not have before the attack (Valeriano and Maness 2015). Yet this type of thinking is an enduring one as more high-profile data breaches, usually espionage campaigns or disruptive information operations and rarely physical degradations (Valeriano, Jensen, and Maness 2018) continue to proliferate and be misconstrued in popular narratives (Lawson 2013).

Scholars who have looked at past dynamics of cyber conflicts find that there is evidence for restraint from states. Reveron (2012) acknowledges that states have great capabilities in terms of inflicting damage on one another, yet this does not mean that they will. Espionage and disruptions seem to be the majority of state-based actions, and more coercive degrading techniques such as Stuxnet or Shamoon are exceptions to the rule according to Valeriano et. al. (2018). The need for weaponized retaliatory responses and initiating policies that promote this behavior may therefore be premature at this point.

The wider work of Valeriano and Maness (2014, 2015) and Maness and Valeriano (2016) have argued that states are "straightjacketed" from acting more abrasive in the cyber domain, as the fear of retaliation, collateral damage, civilian harm, and the diminishing utility of cyber weapons have not led to escalatory relations between rivals. The deterrent strategy in cyberspace would require investment in offensive cyber weapons which could lead to a digital arms race between rivals. Deterrent strategies also require perfect information where capabilities and intent are made clear, and the threats made to potential adversaries could lead to escalatory responses in

kind. Unlike the nuclear domain, where the mutually assured destruction concept has arguably kept the peace between capable powers, in the cyber domain this concept is not present. This could lead to action by threatened states when confronted by the security dilemma. If the US chooses this path, given its large attack surface in the cyber domain and its dependence on digital technologies, this is a conflict it could very well lose.

It is the contention of this chapter that offensive posturing and digital arms races that the United States may set into motion as policy will be a self-defeating one. But there are normative modes of behavior from states that have been observable since the turn of the century based on collected empirical data that suggest that cyberspace can be governed from a less escalatory strategy, where restraint mechanisms can be built upon if the United States and its transatlantic allies continue to push for stabilizing norms (Valeriano and Maness 2015). Fortunately, the NSS promotes working with US allies, especially in terms of information sharing as well as working in tandem with digital surveillance activities against malicious actors (White House 2017), which has been a primary complaint from Europe. It is here where norm promotion should start with Europe and the United States, as well as other like-minded democracies, and then continue this promotion to adversaries such as Russia and China.

Because most cyber events between states will be at the low severity level, manageable, and non-escalatory, the timing of norm promotion and cascades for the future governance of international cyberspace is therefore ripe. Finnemore and Sikkink's (1998) work on the life cycle of the evolution of international norms can be a useful guide to our argument on why norm development and institutionalization, led by the countries of the transatlantic alliance, is the best path forward for a safe and prosperous cyberspace. Norm life cycles go through three stages: emergence, cascades, and internalization (Finnemore and Sikkink 1998). During the first stage, emergence, the key players are norm entrepreneurs, who persuade what are called norm leaders, in our case, states, to begin to embrace new norms. Norm entrepreneurs for the cyber realm include security experts from the private and public sectors, academics, policy advisers, and practitioners.

After the norm emergence stage is a success, the norm leaders then take the lead in an attempt to bring in other states to follow their lead and to embrace these emerging and path dependent modes of behavior. Once the norm leaders are able to socialize these norms into the vast majority of states in the international system, a tipping point is reached and we see a period of norm cascades (Finnemore and Sikkink 1998). Norm violators who continue to behave in a manner against this growing international consensus are pressured into eventual conformance through naming and shaming, sanctioning, and even military action. Eventually even the most notorious international pariahs will conform to these norms most of the time. The costs of norm violation become too high that continuing to break with these new international traditions bring authoritarian and totalitarian governments into line.

The norm cascade stage is also a period in which norms develop a legal footing at the international and domestic levels. States will have motives to sign treaties and adopt domestic law that transform these norms into more enforceable mechanisms. Giving these norms legal standing will help with not only domestic enforcement of laws to catch and prosecute various cyber criminals, but also foster international cooperation, which is especially important for the cyber realm due to its unique characteristic that transcend international borders. The motivations behind this further institutionalization of norms can be for reputation or esteem, but these demonstrations will lead to the final stages of the norm life cycle, internalization, when states

and other actors conform to these norms out of habit due to their complete institutionalization (Finnemore and Sikkink 1998).

Successful international norm life cycles include behavior such as the outlaw of the use of biological and chemical weapons, the nuclear non-proliferation treaties, quartering of enemy combatants, and immunity from medical officers on the battlefield, among many others (Cortell and Davis 2000). What would give cyber norms a good chance of a successful life cycle? First, as of yet, no deaths have occurred as a result of a cyber-attack. It would be in the interests of states to keep this trend going by pushing for norm cascades and internalization. Second, both democratic and non-democratic states have called for norms in cyberspace, although there are some disagreements over the nature of some of these norms. Lastly, the ubiquity of the cyber realm means that all networks in all countries are potentially vulnerable, and as more information, commerce, and military hardware become digitized, all states in the system will want agreed upon modes of behavior. So, which stage in the norm life cycle for cyberspace are we currently?

Norms for cyberspace have completed the norm emergence state of the norm life cycle and are in the early stages of the norm cascade stage. We have yet to reach a tipping point where the cascade has begun to take hold in a majority of states, and this is why norm leadership for this process should begin with the states of the transatlantic alliance. These countries are the most economically prosperous liberal democracies in the world. They have the most to gain from a safe and free cyberspace and perhaps the most to lose from a securitized and conflict-prone one. Norm leaders from these countries also have the ability to put enormous amounts of pressure, either diplomatically, economically, or even militarily on other states in the system to begin to embrace the norms that they have set forth.

In light of the Trump Administration's tack from the previous administration's emphasis on multilateralism and the absolute gains to an emphasis on transactional politics, hard power utilization, and zero-sum gains, it would be in the interest of US European allies to work with the White House on normative cyber behaviors where they have common ground, and deemphasize the promotion of cyber behaviors that lie with realpolitik prescriptions. Information sharing, for operations that are offensive, defensive, or surveillance activities, is the most promising point of agreement for a transactional president and European allies that want the transatlantic alliance to endure. Promoting more resilient practices, such as more responsible behavior on sensitive networks, strong password promotion, two-factor authentication practices, and more actionable risk curbing strategies is also an avenue of agreement for the Trump Administration and European allies. Finally, the incentivization for the private sector to work with government entities to ensure a safer and more prosperous cyberspace is another avenue of agreement.

An ideal venue for the countries of Europe (and Japan) to promote these common ground strategies with the Trump Administration with a limited amount of distractions would be the annual meeting of the Group of 7 (G7), which consists of the seven largest economies of the world that are also liberal democracies (US, UK, France, Germany, Italy, Canada, and Japan). Here the six non-American members will have the exclusive forum to explain to the Trump Administration how countries such as those of the G7 have the most to gain from a free and open internet and much to lose from securitization and conflict of the digital domain. Development of more malicious cyber weapons to deter or utilize offensively will only lead to conflict spirals, where open societies are at a disadvantage.¹⁴ No one entity owns or controls all access to the

¹⁴The White House. "G7 Ise-Shima Leaders' Declaration." Available at: <https://obamawhitehouse.archives.gov/the-press-office/2016/05/27/g7-ise-shima-leaders-declaration>

internet in these countries, contrary to illiberal regimes such as China and Russia. Furthermore, the liberal democracies of the West are more dependent on digital technologies, from commerce to government services to critical infrastructure, and this multitude of targets leaves these societies much more vulnerable, where they could be on the losing end if the world devolves into cyber war. For the liberal world, norms in the cyber domain are key for its various national interests.

A recent meeting of the Group of 20 (G20), which includes the primary cyber adversaries of the transatlantic alliance, China and Russia, established three overarching cyberspace norms to which all members are signatories: no private-sector cyber espionage or intellectual property theft should be conducted by nation-states, no hacking of networks or systems that are considered critical infrastructure are to be conducted by nation-states, and nation-states should be discouraged from developing highly technical malware that are considered cyber weapons and have the ability to do physical harm.¹⁵ Although there already have been norm violators from member of this group, this should not discourage the international community from pursuing and building upon these digital norms.

The big transatlantic divide remains regarding cyber surveillance by the United States (as well as the countries of Europe) and how this fits into norm development. Along with Chinese economic cyber espionage on intellectual property and defense networks and contractors, which have been addressed in this G20 forum, what should be the consensus on political and military espionage, which has yet to be addressed in the forum of the 20 largest economies. If Russian political warfare through cyber and disinformation means is to be curbed in Western societies, which to this point is proliferating without adequate response or deterrent measures, given Russia's refusal to acknowledge its part in doing these activities, as well as a lack of leadership from the United States thus far since these activities began. However, even if Russia admitted that it has been committing political warfare in Western countries, the Kremlin would more than likely point to the Snowden revelations of US clandestine activities by the NSA to justify it. This type of deflection is common in Russian foreign policy, and many times naming and shaming the Kremlin in international forums is more effective in reigning in their behavior. However, it will take US leadership and strong backing from the international community, especially America's steadfast allies in Europe, to reign in these Russian threats. Thus far, the Trump Administration has failed to address this growing threat to the alliance.

Therefore, if the United States is going to continue its digital surveillance in the name of stopping terrorist attacks or any other threat to its national security, it must establish how its activities are different from in both the moral and legal sense than the Russian political warfare in the digital realm that has been dividing liberal democratic societies as of late. For this to happen, it must have the backing of countries such as Germany, France, Brazil, Japan, among others. As of now, the divide on this issue of NSA overreach endures, and the United States must act upon this growing distrust with its European allies if countering this Russian threat in cyberspace is to gain traction. The Trump Administration must do a better job at diplomacy with its transatlantic allies and specifically address the concerns of these governments regarding NSA surveillance. This would require reassurance that the NSA is not infiltrating their citizens' privacy, regardless of US law, and if it is, that the respective intelligence agencies be notified with probable cause of the need to follow certain leads. Multilateral cyber security policies with

¹⁵ Cody M. Poplin. "Cyber Sections of the Latest G20 Leaders' Communique." *Lawfare Blog*, 11/17/2015, accessed 3/4/2017, <https://www.lawfareblog.com/cyber-sections-latest-g20-leaders-communique%C3%A9>

like-minded countries is key if international norms that promote a free and open internet are going to take hold. As of now, the US and its allies are at an impasse that could lead to securitization and cyber repression.

Although deterrence strategies for future cyber operations from Russia are always an option, they also risk the probability of backfiring on the United States and its allies. Free societies are more vulnerable than their authoritarian counterparts, as they are more dependent upon digital technologies, which gives them a larger attack surface that illiberal countries do not have. Furthermore, authoritarian regimes have more control over their cyber sovereign borders, giving them an edge in cyber conflict if cyber offensive operations in the name of deterrence are to be policy from the transatlantic alliance. The promotion of norms with a like-minded voice from all free societies, led by the United States and Europe is the best suboptimal option if the internet is to remain free, open, and most importantly, prosperous. As more and more commerce moves to the digital domain, the free countries of the world have the most to lose for escalation in the cyber realm, making power politics policy very risky as international cyber conflict evolves.

Conclusions

Right before Barack Obama left office, in late 2016, the United States launched a large cyber operation against the terrorist group ISIS. Named Operation Glowing Sympathy, the now separate US Cyber Command, with Title 10 authority, based on NSA intel, which has Title 50 authority, “obtained the passwords to a number of Islamic State administrator accounts and then used them to access the accounts, change the passwords and delete content such as battlefield video. It also shut the group’s propaganda specialists out of their accounts”¹⁶. This operation required the knowledge, intelligence, and expertise of America’s European allies, and intelligence services from the UK, France, and Germany, were all notified of the operation, as the need to surveil several targets and servers required the NSA penetrate the sovereign cyberspace of these countries. This operation that required cooperation, information sharing, and teamwork is an example of how the transatlantic alliance can work together, establish best practices when it comes to using cyber operations offensively, and serve as an example of what should and should not be done by nation-states. Simultaneously, the recent clandestine actions by Russia and China should be contrasted to actions such as these, naming and shaming China for economic espionage and Russia for political warfare in the cyber domain. This will be the path to norm cascades that lie in the national interests of the transatlantic alliance.

Put simply, Trump’s America First policies will not work in cyberspace. Most cyber incidents and disputes are over more manageable issues such as espionage, which includes the stealing of state and technological secrets, or disruption strategies, such as the use of propaganda and use of denial of service techniques (Valeriano et. al. 2018). Evidence for restraint dynamics and the continuation and strengthening of these modes of behavior is present. Therefore, governance of cyberspace should be promoted in international institutions through norm development and cascades, and led by the United States and its European allies (Finnemore and

¹⁶ Ellen Nakashima. “US Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate Over Alerting Allies,” *The Washington Post*, 5/8/2017, accessed 12/28/2017, https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html?utm_term=.80c9d6b1bfe3

Hollis 2016). The United States cannot go it alone if it is going to adequately protect its networks and promote its national interests. It needs the cooperation of its European allies.

The Tallinn Manual 1.0 (Schmitt 2013) and 2.0 (Schmitt 2017) take existing international law and apply it to the cyber domain. However, much of these applications of law are through the lens of military strategy and the law of armed conflict (LOAR), and the evidence presented in this chapter suggests that military framing may be the wrong track. Norms specific to the uniqueness of the cyber domain should be the path, where these norms develop over time and violations of these constructed norms gradually become taboo. International groups such as the UN's Group of Government Experts (GGE), the G20, and the G7 have held annual meetings and published numerous reports promoting norms, with the former two groups including representatives from the governments of China and Russia.¹⁷ It is here where the United States and European powers can seek common ground with its primary cyber adversaries, and avoid the security dilemma and digital arms races with these powers.

The United States' major initiatives regarding cyber safety and defense include the information sharing legislation CISA bill passed in 2015. This incentivizes private actors to share its data breach information with federal agencies so that current threats can be published and shared society wide. This concept should be extended to international agreements with its European allies where the incentivization of information sharing should be across borders, strengthening the network defenses of all states involved. Furthermore, the CNAP executive order issued by the Obama Administration in 2016 should be continued and strengthened by the Trump Administration. This order directs non-military agencies of the federal government to promote better cyber hygiene agency-wide and use existing budgets to divert resources for better cyber security practices. Trump should ask Congress for increased funding for cyber security for these government agencies so that better defense and cyber resilience can be realized government-wide. European governments should take similar measures to promote these practices and share information with their American counterparts regarding zero-day vulnerabilities and other cyber threats, especially the current threat from the Russian Federation.

The big unknown facing the United States and its transatlantic partners is the track the new Trump Administration will take regarding cyber conflict and security. However, the National Security Strategy shows promise. It emphasizes cooperation with allies in the cyber domain, and the European powers should capitalize on this. They should also remind the new administration of the dangers of power politics practices in cyberspace, pointing out the disadvantages free societies have in this domain. The US, although having great offensive capabilities, is very vulnerable to attack as well. If the US under the new administration decides to raise the costs of cyber conflict with its adversaries such as China or Russia, it could very well be on the losing end. Working together with its European allies regarding norm promotion is the best track at this time, yet it is uncertain that the new American administration will heed this advice.

¹⁷ NATO CCE COE. "2015 UN GGE Report: Major Players Recommending Norms of Behavior, Highlighting Aspects of International Law." 8/31/2015, accessed 2/23/2017, <https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html>

Cody M. Poplin. "Cyber Sections of the Latest G20 Leaders' Communique." *Lawfare Blog*, 11/17/2015, accessed 3/4/2017, <https://www.lawfareblog.com/cyber-sections-latest-g20-leaders-communiqu%C3%A9>

The White House. "G7 Ise-Shima Leaders' Declaration." Available at: <https://obamawhitehouse.archives.gov/the-press-office/2016/05/27/g7-ise-shima-leaders-declaration>

References

- Ambrosio, T., 2017. "The fall of Yanukovich: structural and political constraints to implementing authoritarian learning." *East European Politics*, 33 (2): 184-209.
- Ashford, E., 2016. "Not-So-Smart Sanctions: The Failure of Western Restrictions Against Russia." *Foreign Affairs*, 95, p.114.
- Bauman, Zygmunt, Dider Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R.B.J. Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology*, 8: 121-144.
- Birchfield, V.L. and Young, A.R. eds., 2017. *Triangular Diplomacy among the United States, the European Union, and the Russian Federation: Responses to the Crisis in Ukraine*. Springer.
- Clarke, Richard A., Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter Swire. 2013. "Liberty and Security in a Changing World." *Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 12/12/2013.
- Cortell, A.P. and Davis, J.W., 2000. "Understanding the domestic impact of international norms: A research agenda." *International Studies Review*, 2 (1): 65-87.
- Diebert, Ron. 2015. "The Geopolitics of Cyberspace After Snowden." *Current History*, 114: 9-15.
- Easley, Lief-Eric. 2014. "Spying on Allies." *Survival*, 56 (4): 141-156.
- Finnemore, M. and K. Sikkink. 1998. "International norm dynamics and political change." *International Organization* 52(4): 887-917.
- Finnemore, M. and Hollis, D.B., 2016. "Constructing Norms for Global Cybersecurity." *American Journal of International Law*, 110 (3): 425-479.
- Fonseca, B. and Rosen, J.D., 2017. Cybersecurity in the US: Major Trends and Challenges. In *The New US Security Agenda* (Springer International Publishing): 87-106.
- Giles, Kier. 2016. "The Next Phase of Russian Information Warfare." Prepared by the *NATO Strategic Communications Center of Excellence*. www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles
- Kaplan, Fred. 2016. *Dark Territory: The Secret History of Cyber War*, (New York: Simon and Schuster).
- Lawson, Sean. 2013. "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats." *Journal of Information Technology & Politics* 10, no. 1: 86-103.

Lindsay, Jon R. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22 (3): 365-404.

Maness, Ryan C. 2018. "Death By A Thousand Cuts: Is Russia Winning the Information Warfare With the West?" Working Paper.

Maness, Ryan C. and Brandon Valeriano. 2015. *Russia's Coercive Diplomacy: Energy, Cyber and Maritime Policy as New Sources of Power* (London: Palgrave Macmillan).

Maness, Ryan C. and Brandon Valeriano. 2016. "The Impact of Cyber Conflict on International Interactions." *Armed Forces and Society*. 42(2): 301-323.

Maness, Ryan C., Brandon Valeriano and Benjamin Jensen. 2017. *Coding Manual for v1.1 of the Dyadic Cyber Incident and Dispute Dataset, 2000-2014*, unpublished manuscript. Available at: drryanmaness.wix.com/cyberconflict.

Office of the Director of National Intelligence. "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution," 1/6/2017, accessed 3/2/2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf

Reveron, Derek. 2012. "An Introduction to National Security and Cyberspace." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Derek Reveron, Editor. (Washington D.C.: Georgetown University Press

Schmitt, M.N., 2013. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.

Schmitt, M.N. ed., 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

Snegovaya, Maria. 2015. *Putin's Information in Ukraine: Soviet Origins of Russia's Hybrid Warfare*, (Washington: Institute for the Study of War).

Thaler, David E., Michael J. McNerney, Beth Grill, Jefferson P. Marquis, and Amanda Kadlec. 2016. *From Patchwork to Framework: A Review of Title 10 Authorities for Security Cooperation*, (RAND Corporation).

Valeriano, Brandon and Ryan C. Maness. 2014. "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011." *Journal of Peace Research*, 51 (3): 347-360.

Valeriano, Brandon and Ryan C. Maness. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press.

Valeriano, Brandon, Benjamin Jensen and Ryan C. Maness. 2018. *Cyber Strategy: The Changing Character of Cyber Power and Coercion*, (New York: Oxford University Press).

White House. 2017. *National Security Strategy of the United States of America*, accessed 12/28/2017, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>