Cyber Diplomacy: The Need for a U.S. Cyber Ambassador

By Daria Etezadi, MCPA Fellow

Redefining Diplomacy as an Instrument of National Power

Diplomacy is a formally recognized tool for curbing and resolving international conflict. Though cyberspace has challenged conventional rules of engagement, it still requires serious discussion about opportunities for diplomatic action.

Traditionally, the domains of warfare -- land, sea, air, and space -- have been tied to the military arm of the government and have rested on known doctrine, containing both offensive and defensive strategies. This trend traces back to the French Revolution and the Napoleonic war, with the publication of works like "On War" by Carl von Clausewitz.[1] But in the past 200 years, warfare has diversified to the point where traditional strategies don't always work.

While historians once defined war as acts of physical violence, cases of cyber-physical attacks and cloud intrusions have expanded the scope of warfare beyond kinetic action. Cyber operations can impact digital systems that are used on a regular basis, thus compromising the networks that process anything from credit card transactions to military operations to water and food distribution programs.

When cyber evolved into the fifth domain of warfare in 2009 with the establishment of U.S. Cyber Command, the U.S. government demonstrated its commitment to running intelligence operations to defend domestic infrastructure from cyber attacks.[2]

As cyber warfare has become more popular, the unconventional has started to become the new normal. There are no recorded deaths directly resulting from cyber attacks, but individual lives have been put in danger due to incidents ranging from identity theft to restricted access to healthcare. So how does this impact the parameters around which nation-states can and should engage in modern warfare?

Cyber does not stand in isolation. It operates in conjunction with activity in land, air, sea, and space. Just as cyber attacks can compromise the other domains, utilizing each domain in a multi-pronged offensive or defensive strategy is necessary to protect the homeland from known and unknown cyber threats.

To that end, developing and rolling out a cyber-inclusive national security strategy relies on every arm of national power, not just the military arm. The U.S. Congressional National Security Strategy identified the instruments of national power through the DIME acronym: diplomacy, information, military, and economic power.[3] DIME exists largely to remind policymakers and governing entities that national power need not be reduced to military force. DIME later transitioned into DIME(FIL) from 2001 to 2006, particularly after the U.S. launched the War on Terror, to consider asymmetric warfare against insurgents and to include finance, intelligence, and law enforcement within a broader strategy.[4]

DIME(FIL)

Diplomacy
Information
Military
Economic
Finance
Intelligence
Law Enforcement

As part of the checks and balances system, Congress ultimately determines when and where to engage in warfare. But after the events of September 11, 2001, President Bush invoked the Authorization for Use of Military Force (AUMF), which was intended to give the Executive Office (EO) the chance to declare war in the case of a national emergency without waiting for Congress's approval.[5] Doing so allowed the U.S. to engage the War on Terror and target non-state actors responsible for the 9/11 attacks. It also strengthened the U.S. Department of Defense.

Operation Enduring Freedom and Operation Iraqi Freedom involved concentrated efforts in U.S. military diplomacy, military information operations, and military intelligence. This weakened the Department of State's diplomacy initiatives, which would have included nation-building and stability operations.[6] Failure to balance the state pillars of power in countries like Afghanistan and Iraq introduced a heavy reliance on the use of force that was not contextualized within a larger strategy due to insufficient information. Subsequently, the U.S. struggled in its efforts to navigate the terrain and focus on collaboration efforts with local communities.

> *"Diplomacy settles wars and prevents them"*

The U.S. does not have a clearly established diplomacy strategy in the cyber domain. Often, discussions around creating a strategy boil down to the same questions: is it needed and why? Diplomacy settles wars and prevents them; it sets standards and holds actors accountable for their actions via ambassadors and well-rounded teams of experienced subject-matter experts. However, measures of relationship-building, negotiation, compromise, and peacekeeping are hard to quantify, so the cyber diplomacy conversation has continued to survive in limbo between the three branches of government. And the hard truth is we are running out of time.

Cyber attacks have already been proven capable of damaging the economy, infiltrating bank networks, destabilizing healthcare infrastructure, and compromising election results. They have targeted both the public and private, government and civilian networks. Knowing this, there must be a plan of action to craft appropriate, proportional responses in any given situation, in order to neutralize these threats.

The United States government has a duty to strategize a structured plan of action in response to emerging and continuing cyber security threats using every arm of U.S. national power. To that end, appointing a cyber ambassador to represent and advocate for the arm of diplomacy is critical for the effective formulation and execution of a plan to mitigate breaches in cyber operations.

Where Diplomacy Matters: Threats in Cyberspace

The lack of rules of engagement means there aren't enough protective measures for civilians in the cyber domain, which puts individual lives at risks and makes an opportunity for diplomatic cooperation that much more important. The matrix of cyber threats is deceptive because it redefines standard definitions of war casualties and targets noncombatants on a regular basis.

Common types of cyber attacks include malware, phishing, Man-in-the-Middle (MitM) attacks, Denial of Service (DoS) attacks, Structured Query Language (SQL) injections, and zero-day exploits.[7]

- Malware includes spyware, ransomware, viruses, and worms. It infiltrates a system through a vulnerability, especially through a bugged link or email attachment, which then translates into ransomware or spyware, harming the system itself or incapacitating it.
- Phishing involves fraudulent communications that steal Personal and Professional Information Narrative (PPIN) or install malware remotely on the recipient's device.
- MitM attacks occur when attackers essentially eavesdrop on a two-party transaction. They become the filter through which all activity passes and typically infiltrate via an unsecured, public network or using malware, which can then give the attacker access to said device.
- DoS attacks flood and overwhelm the devices or networks in question, so they stop functioning or are unable to fulfill requests. Multiple devices can also be impacted in this way in what is referred to as a Distributed-Denial-of-Service (DDoS) attack.
- An SQL injection is used by an attacker to insert a malicious code into a server and force said server to reveal information.
- A zero-day attack strikes before a vulnerability is known, or after a vulnerability is known but before a patch or solution is implemented.

FortiGuard Labs' Senior Security Strategist and Researcher Anthony Giandomenico also has a running list of the types of attacks that continue to surface, available for further reference.[8]

Motive: Political Power

Cyber attacks have impacted political, economic, and physical spheres. In the cyber-physical space, critical infrastructure (CI) is particularly vulnerable. Should an attack be launched on the valve controls of a water source or disrupt electrical services, then communities will risk losing access to basic necessities like food, shelter, and water. Russian hackers have demonstrated this capability with Ukraine's CI. Hackers with suspected connections to the Russian government remotely accessed the control centers of three Ukrainian electricity distribution companies through a DDoS attack in December 2015. This caused over 200,000 consumers to lose electrical power in the middle of winter.[9] Similar attacks continued to roll through Ukraine in the years following amidst the political revolution in Kiev and the annexation of Crimea. The attacks positioned Russia to flex its muscles before the world as its government marched on with its destabilization campaign in Ukraine. Cue the unofficial introduction of hybrid warfare, where every domain is fair game.

The U.S. and other NATO allies intervened to offer Ukraine multilateral support in identifying and fending off these attacks. Multilateral cyber diplomacy is still in its infancy, but the diplomatic cooperation across the board helped identify Russian hackers and the Russian government as the top suspects. In July, Ukrainian security services made a breakthrough in strengthening their defenses by thwarting a Russian VPNFilter malware attack against one of their chlorine distribution plants.[10] If the attack had been successful, it would have disrupted the plant's distribution of clean water to local communities.

Other DoS and cyber-physical attacks have been recorded domestically. In March 2018, reports from Mayor Catherine Pugh's office confirmed that unidentified actors successfully hacked into Baltimore's 911 computer-aided dispatch (CAD) system and forced city personnel to switch to 'manual mode' to process 911 and 311 calls.[11] Operators had to manually determine and record the origins of emergency phone calls, which poses obvious risks should a caller have insufficient time or resources to determine his or her whereabouts. Baltimore's CAD system was back online nearly 24 hours later and luckily didn't stall operations in the interim. The actors behind this breach have not been identified and are still in the wind.

Security breaches that infiltrate municipal emergency response systems threaten to isolate communities and place them in harm's way, while locking down any opportunities victims might have had to ask for help. There have been 184 cyberattacks on public safety agencies and local governments since 2016, with 42 of those targets being 911 centers.[12] As the U.S. government has increasingly been pointing fingers at Russian actors with suspected ties to the Russian government, the need for diplomacy is increasing in importance. Appointing a cyber ambassador and engaging in multilateral diplomacy would give the U.S. access to a formal international institution that could attribute attacks to suspected actors and hold them responsible for their actions.

Motive: Financial Gain

Sometimes, attackers are seeking profit. According to a report released by Cisco, 53% of cyberattacks resulted in damages of $500K or more.[13] The Ponemon 2017 Cost of Data Breach study suggests that the financial loss per data record is $141, putting the global average at $3.6 million.[14] The study also estimates the average cost of a data breach in the U.S. around $7.3 million.[15] Given that between four to five million data records are lost or stolen internationally every single day,[16] these numbers measure a significant impact on institutions, on companies, and on individual lives. The infamous Equifax breach allowed an unidentified group of hackers to collect 147.9 million Americans' names, driver's license numbers, and social security numbers, among other forms of personal information.[17] According to the National Foundation for Credit Counseling, around 1,500 breaches occur each year, but the size of the Equifax breach surpassed all others.[18] Modern ransomware attacks combine encryption and bitcoin transactions to become virtually untraceable. A ransomware attack targeted the city of Atlanta in March 2018 and scrambled operations across all CI. Users were locked out of their accounts and told to pay a ransom of $50,000 in bitcoin within a week if they wished to regain access. Dell SecureWorks identified the attackers as members of the SamSam hacking group, who are reported to have acquired over $1 million from similar attacks in 2018 alone.[19]

In support of the investigation, Microsoft and a team from Cisco's Incident Response Services teamed up with the Department of Homeland Security to restore Atlanta's municipal systems. This public-private partnership helped the city of Atlanta get back on its feet, but for a price of $2.6 million--a dollar amount 52 times greater than the original ransom demand.[20]

Ultimately, the city of Atlanta was able to regain control over its systems. But audit reports reveal that the cyber vulnerabilities in Atlanta's municipal networks could have been identified months before the breach.[21] Cyber threats evolve quickly, so it is every institution's responsibility to maximize its resources and stay ahead of those threats as much as possible.

When Wannacry hit the United Kingdom in 2017, it became a well-known example of a ransomware attack. Wannacry shut down more than 80 National Health Service organizations in England alone, which cancelled 20,000 appointments and forced 60 General Practitioners to do their work manually, using pen and paper. It also pressured five hospitals into sending patients elsewhere because they could not retain their normal capacity.[22]

Targeting CI using ransomware leaves everything including transportation, financial services, and waterways vulnerable to disruption. Attackers can put basic operations on hold and control access to food and shelter in exchange for money and/or power. CI attacks impact communities indiscriminately and hold the potential to weaken the structure of society. Given that cyber attacks have triggered so many consequences and impacted the framework of American society, the U.S. needs to weigh in on multilateral conversations to attribute said attacks and hold these perpetrators responsible for their actions. Without a formal diplomacy office, U.S. participation is limited and cannot have the same impact as it would with an ambassador in place.

Developing a Deterrence Framework: Legislation

The objective of a cyber diplomat would be to establish and help enforce a deterrence framework. Diplomacy is one of the ways the United States can effectively incorporate a deterrence framework in response to cyber threats and balance out the pillars of power. This would begin with a cyber ambassador who can serve as the face of these discussions.

For cooperation across DIME(FIL) to succeed, Congress must begin securing positions for cyber security advocates beyond the Department of Defense, to include the Executive Office (EO), the Department of Justice, and the Department of State, at the very least. Congress has been working to acquire bipartisan approval for bills that would address these needs, in an increasingly polarized environment.

Department of Defense

Earlier this year, U.S. Cyber Command (USCYBERCOM) released a new command strategy or "Command Vision" that revised the Command's approach to cyber strategy given the domain's evolution since 2009.[23] Though the U.S. government has placed emphasis on the physical domains, aggressors are more likely to use cyber attacks against the physical domain to target the military, as well as society.

To the point of the new Command strategy, attackers can act without fear of legal or military repercussions. While there must always be an emphasis on the need for interagency communication and vigilance, defining and establishing consequences for criminal cyber behavior is one of the first orders of business. The U.S. must continue to classify cyber attacks with more seriousness and urgency, particularly the ones that infiltrate domestic systems every day. The Command, alongside ongoing policy discussions, is opening up doors for USCYBERCOM to expand its reach and offer more protection to the private sector, particularly those that influence CI systems. Further, USCYBERCOM is looking to revise common terminology. In years past, terms like "hacking" or "breach" were used to describe adversarial behavior, words that fall short of identifying an attack as armed aggression. The Command has begun to shift its approach, calling on strategists to identify these seemingly less aggressive attacks as what they are: calculated maneuvers to weaken the U.S.'s power, while simultaneously sidestepping any repercussions. The new strategy points out that cyber operations can still impact a nation state's relative power without traditional armed aggression.[24,25]

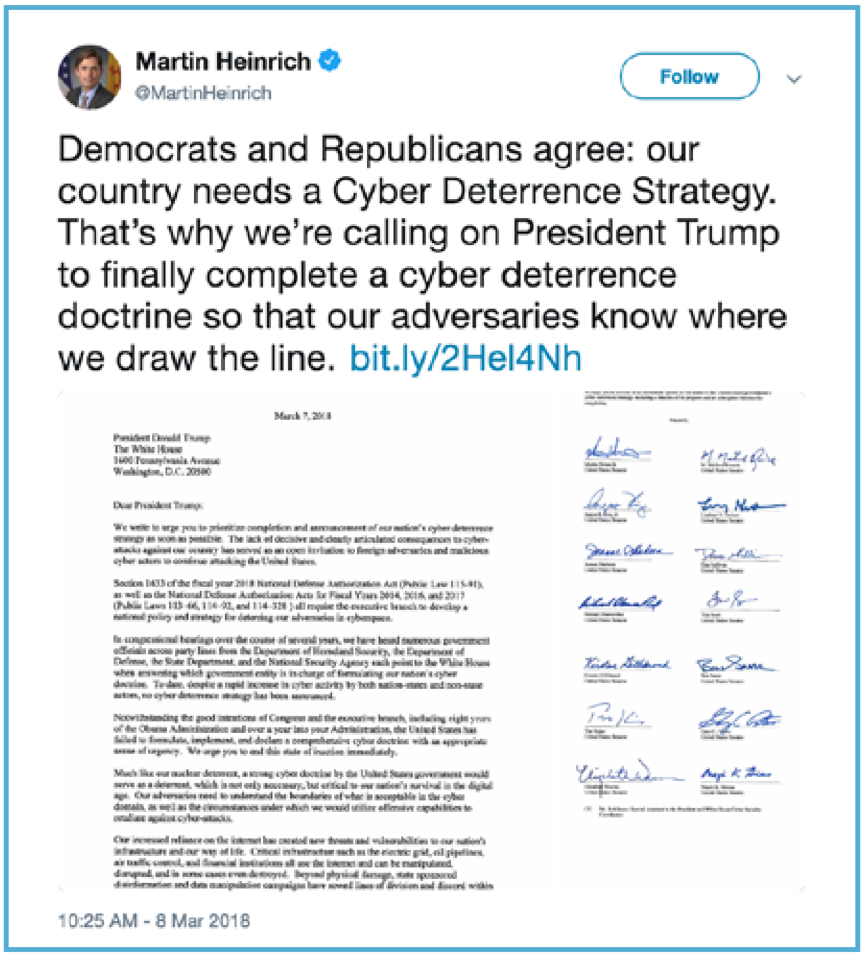
The Executive Office

Back in May, Congressman Jim Langevin (D-RI) and Congressman Ted Lieu (D-CA) introduced a bill known as the Executive Cyberspace Coordination Act, intended to create a permanent Director of Cybersecurity Policy in the White House.[26]This bill surfaced in response to White House Cybersecurity Coordinator Rob Joyce stepping down to return to the NSA, leaving the position unfilled.[27] Representatives from the Government Accountability Office (GAO) have made mention of an ongoing review of Joyce's former position, which would determine how effective the role has been. The review would then be taken to Congress for consultation, regarding whether appointing someone new would be worthwhile.[28] The latest release of the GAO's cyber risk assessment only recommends that the White House Cybersecurity Coordinator "develop an overarching federal cybersecurity strategy" to include performance measures, cost and resource needs, as well as the distribution of responsibilities across federal organizations.[29] However, it neither mentions the position's vacancy nor references any plans or recommendations to fill it.

In the meantime, the Vulnerabilities Equities Process (VEP) board at the White House remains active. Though the VEP continues to stir controversy, its intention is to provide the U.S. government with a process through which it can vet whether discoveries of vulnerabilities in domestic cyber networks can and/or should be declassified and disclosed to the public.[30] It serves as a filter for the U.S. government to determine how to engage in information sharing between the public and private sector without compromising national security. Joyce had played a critical role as the head of the Equities Review Board (ERB), which leads the decision-making process within the VEP. Since Joyce stepped down, the White House has appointed a new chairman, Grant Schneider, to head the VEP, but the conversation around whether the Cyber Coordinator in the EO will be preserved or eliminated is still in the hands of the GAO and Congress.[31]

Department of Justice

In June, the Cyber-Digital Task Force released a report laying out the Department of Justice's (DOJ) strategy in response to threats of election interference, attacks on critical infrastructure (CI), industry and government, and the increase of digital propaganda.[32] Part of the report touches on Russia's interference with the 2016 elections and the anticipated repeat of these attacks in the 2018 campaigns. For context, two city-level Democratic campaigns were hit with DDoS attacks in 2016 during the launch of their fundraisers, incapacitating their campaign websites.[33] In response to the distribution of personal information and interference with fundraising efforts, election officials across 44 states recently participated in an election security drill with the NSA and USCYBERCOM.[34] Meanwhile, the DOJ has indicted 12 Russian military intelligence officers suspected to be involved with the 2016 crimes, as part of a broader public shaming and deterrence strategy. But without an ambassador to steer these international relationships, U.S. legislation can only respond to individual actors, rather than the state itself. Diplomacy opens up the conversation for cooperative nation-states to establish norms of behavior and appropriate repercussions. Even when a nation cannot or will not agree to those terms, working in conjunction with partner nation-states provides multilateral backing that can further deter state-sponsored cybercrime.



Democrats and Republicans agree: our country needs a Cyber Deterrence Strategy. That's why we're calling on President Trump to finally complete a cyber deterrence doctrine so that our adversaries know where we draw the line. bit.ly/2HeI4Nh

March 7, 2018

President Donald Trump
The White House
1600 Pennsylvania Avenue
Washington, D.C. 20500

Dear President Trump:

We write to urge you to prioritize completion and announcement of our nation's cyber deterrence strategy as soon as possible. The lack of decisive and clearly articulated consequences to cyber-attacks against our country has served as an open invitation to foreign adversaries and malicious cyber actors to continue attacking the United States.

Section 1633 of the fiscal year 2018 National Defense Authorization Act (Public Law 115-91), as well as the National Defense Authorization Acts for Fiscal Years 2014, 2016, and 2017 (Public Laws 113-66, 114-92, and 114-328) all require the executive branch to develop a national policy and strategy for deterring our adversaries in cyberspace.

In congressional hearings over the course of several years, we have heard numerous government officials across party lines from the Department of Homeland Security, the Department of Defense, the State Department, and the National Security Agency each point to the White House when answering which government entity is in-charge of formulating our nation's cyber doctrine. To date, despite a rapid increase in cyber activity by both nation-states and non-state actors, no cyber deterrence strategy has been announced.

Notwithstanding the good intentions of Congress and the executive branch, including eight years of the Obama Administration and over a year into your Administration, the United States has failed to formulate, implement, and declare a comprehensive cyber doctrine with an appropriate sense of urgency. We urge you to end this state of inaction immediately.

Much like our nuclear deterrent, a strong cyber doctrine by the United States government would serve as a deterrent, which is not only necessary, but critical to our nation's survival in the digital age. Our adversaries need to understand the boundaries of what is acceptable in the cyber domain, as well as the circumstances under which we would utilize offensive capabilities to retaliate against cyber-attacks.

Our increased reliance on the Internet has created new threats and vulnerabilities to our nation's infrastructure and our way of life. Critical infrastructure such as the electric grid, oil pipelines, air traffic control, and financial institutions all use the Internet and can be manipulated, disrupted, and in some cases even destroyed. Beyond physical damage, state sponsored disinformation and data manipulation campaigns have sowed lines of division and discord within

[illegible]

10:25 AM - 8 Mar 2018

Department of State

In January 2018, the House of Representatives passed the Cyber Diplomacy Act (H.R. 3776), authorized by Chairman Ed Royce (R-CA). H.R. 3776 establishes a premise for U.S. engagement in a system of international cyber diplomacy and is designed to help keep the internet open, reliable, and secure, while resisting censorship attempts by China, Russia, North Korea, Iran, and Syria.

H.R. 3776 has 25 cosponsors (13 Democrat, 12 Republican). The bill has five main points with the overarching goal of giving the State Department leeway to work with foreign governments on international cyberspace policy. They include:

1. Establishing an Ambassador for Cyberspace position to lead the State Department's cyber diplomacy efforts;
2. Mandating State Department's annual country reports to include an assessment on internet freedoms;
3. Positioning the United States to work with foreign governments to support U.S. international cyberspace policy;
4. Securing commitments on responsible state behavior and requiring regular updates to the strategy;
5. Creating an overarching cyber policy that advances democratic principles in cyberspace.

Though Congress hit the ground running at the beginning of 2018, progress slowed as conversations became more complex. By March, Senator Martin Heinrich (D-N.M.) spearheaded bipartisan discussions within the Senate Armed Services Committee about the importance of establishing and announcing a cyber deterrence strategy, which has already been mandated by the FY 2018 National Defense Authorization Act.[35]

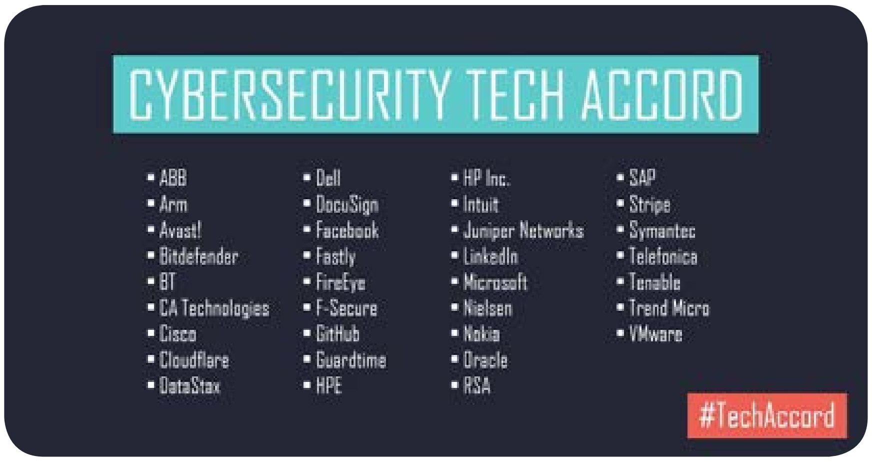
In theory, this deterrence strategy would be led by a cyber diplomat. Former Cyber Coordinator Christopher Painter--the closest equivalent to a U.S. cyber ambassador--ran the Office of the Coordinator for Cyber Issues at the Department of State from 2011-2017. After Painter left, former Secretary of State Rex Tillerson spoke of folding the Cyber Office into the Bureau of Economic Affairs for the sake of efficiency.[36] But the proposal met resistance in Congress, as discussions around the necessity for a cyber diplomacy office surfaced. By June, the Senate Foreign Relations Committee combined H.R. 3776 with updated language to restore the Office of Cyberspace in conjunction with the new Digital Economy office.[37] Yet over a year later, Painter's role remains unfilled.

A cyber diplomat can create a framework that establishes the U.S. will not tolerate certain behaviors and will pursue proportional responses. Establishing international norms of cyber behavior can then lay the groundwork for multilateral talks and leverage more nation states to expose and penalize cyber criminals.

Strengthening Defenses: Public-Private Partnerships

Public-private partnerships in the cyber industry are essential. While diplomacy has historically been focused on the public sector, cyber threats have continued to target the private sector. If both public and private sector institutions could team up, they could collectively deter cyber threats, share technological advances, and achieve the end goal of cooperation in the cyber domain.

Private companies are already engaged in government-sponsored cyber activity, whether they want to be or not--even if only as victims of cyber attacks. Many private companies demonstrated their commitment to combating cyber threats with the signing of the Cybersecurity Tech Accord, led by Microsoft and joined by Facebook, along with 32 other companies.[38] The pledge serves as an acknowledgement that cybersecurity is a priority and creates a space for companies to cooperate and share information to strengthen their cyber defenses. Cyber hackers whose actions bolster their country's political agenda treat operations across the public and private sector as fair game, and each attack comes with a steep cost. By 2022, the cost of cyber attacks at the hands of international actors will have risen to $8 trillion.[39] The Cybersecurity Tech Accord is an example of how the U.S. private sector can own up to these vulnerabilities and join forces to respond to cyber threats domestically. Strong collaboration in this space could then lend itself to effective public-private partnerships and empower the United States to maximize its resources, gather reliable intelligence, and be in the best position to hold cyber aggressors responsible for their actions.[40]



CYBERSECURITY TECH ACCORD

- ABB
- Arm
- Avast!
- Bitdefender
- BT
- CA Technologies
- Cisco
- Cloudflare
- DataStax
- Dell
- DocuSign
- Facebook
- Fastly
- FireEye
- F-Secure
- GitHub
- Guardtime
- HPE
- HP Inc.
- Intuit
- Juniper Networks
- LinkedIn
- Microsoft
- Nielsen
- Nokia
- Oracle
- RSA
- SAP
- Stripe
- Symantec
- Telefonica
- Tenable
- Trend Micro
- VMware

#TechAccord

Some of these collaborative efforts are already in full swing. The U.S. Air Force is outsourcing all day-to-day IT operations in partnership with Microsoft Office and Oracle Cloud Services.[41] This collaboration between Silicon Valley tech companies and the U.S. military marks a transition into deeper integration of public-private partnerships for cyber defense. The idea is to leave administrative IT operations to private companies and to rely on U.S. Airmen to concentrate their efforts on Mission Defense Teams.

The Pentagon had also partnered with Google to assist with Project Maven, which uses Artificial Intelligence (AI) and machine learning to identify objects of interest in both photo and video captures and allow for precision targeting.[42] The stigma around weaponized AI eventually dissolved the partnership as Google employees and stakeholders protested against the project.[43] However, the weaponization of AI is an emerging strategy that is actively being pursued by the Russia, China, and the U.S. and is listed as one of the cyber threats to look out for in 2018, according to MIT's Technology Review.[44] The potential AI holds as a weapon scales up to an arms race. Autonomous weapons, for example, have been under scrutiny by the United Nations. The Convention on Certain Conventional Weapons (CCW) is considering placing an international ban on what it calls "killer robots," which continue to possess an element of unpredictability, should humans lose control of these machines.[45]

Public-private partnerships allow for the maximization of resources to respond to threats like the ransomware attack on the city of Atlanta. By continuing to work through communication methods and known historic barriers to information sharing, both the government and private companies can keep each other in the know about incoming threats and keep their operations secure.

Global Integration: Working within an International Sphere

In 2017 Australia released its International Cyber Engagement Strategy and led a two-pronged diplomatic cyber charge by both establishing cyber laws and criminalizing cyber interference attacks, and by inaugurating its first Ambassador for Cyber Affairs.[46] Dr. Tobias Feakin, Australia's Cyber Ambassador, has led dialogue around the norms of behavior that need to be established and has coordinated a larger strategy alongside foreign governments.

Given Australia's demonstrated commitment to cyber diplomacy, it would be appropriate for the other "Five Eyes" nations to follow suit, which would also include Canada, New Zealand, the United Kingdom, and the United States. The Five Eyes are well-positioned to set the tone for norms of behavior on an international scale, taking what started as a signals, military, and human intelligence sharing alliance and using that foundation to help establish a global standard for conduct in cyberspace.

As a known influencer of international norms, the U.S. is well positioned to follow in the footsteps of Australia's approach. Doing so will strengthen the U.S. government's approach to defining cyber diplomacy and unfolding a plan of action across its domestic industries, but public and private.

Attribution in and of itself is difficult to prove. The U.S. government and other NATO allies attributed the attacks on Ukraine to the Sandworm Team because of the use of the signature malware trojan BlackEnergy3. The Sandworm Team's connection to Russian intelligence and the obvious benefits to Russian state interests strongly suggest the Russian government was behind these attacks and multilateral cyber cooperation made that theory known to the world.[47] However, Russia maintained degrees of separation to maximize plausible deniability, thereby complicating attribution efforts. In order to combat plausible deniability, the U.S. must participate in multilateral discussions.

International cooperation will also become increasingly critical as the U.S. develops a cyber deterrence strategy. Cyber continues to pose a unique problem with attribution. As the former Director of the NSA and first USCYBERCOM Commander, General Keith Alexander, said, "We can't see other nations attacking us."[48] State actors often sponsor cyber attacks anonymously. Other times, non-state actors and individuals alike engage cyber attacks on their own.[49] The Advanced Persistent Threat (APT) groups demonstrate this behavioral pattern.[50] The U.S. government has the capability to pinpoint individual actors behind these attacks, but it's a matter of building up international norms so countries can identify attackers and enforce rules of engagement multilaterally. According to Dr. Feakin, blaming Russia for the NotPetya attack was a coordinated diplomatic effort.[51] Seven nations--the U.S., the U.K., Denmark, Lithuania, Estonia, Canada, and Australia--came together in what Feakin refers to as the largest coordinated effort at cyber attribution in history. This followed a similar coordinated attribution of the DPRK as the responsible party behind Wannacry.

Continued and unrestricted cyber attacks have had such profound financial and security implications that the vulnerability of domestic critical infrastructure has been a point of discussion for decades. Recently, Russia has been accused of launching a supply chain cyberattack on Texas-based Energy Services Group LLC, disrupting the customer transaction service of Energy Transfer Partners LP, which manages 71,000 miles of pipelines containing natural gas, crude oil, and other commodities. DHS has warned that Russian government actors have been targeting U.S. energy infrastructure since March 2016 with a "multi-stage hacking campaign."[52]

When the U.S. Office of the Coordinator for Cyber Issues (CCI) launched in 2011 to develop an open and secure Internet, it was assigned the task of determining international norms and establishing agreements with its foreign counterparts in government. These agencies extend to the European Union Agency for Network and Internet Security (ENISA) and the National Cyber Security Centre (NCSC) in the Republic of Korea (South Korea). Diplomatic conversations between said agencies would make it easier to create norms of behavior and take a united stance against malicious behavior.[53]

Conclusion

Despite continued efforts to bolster a cyber engagement framework, the consequences of not having a cyber diplomat creates missed opportunities for the U.S. to advocate for the freedom of the people and the protection of human rights.

Countries like China, Russia, and Iran have demonstrated that they view cyber as a sovereign opportunity to maintain internal stability and filter information, both incoming and outgoing. If the U.S. wishes to champion for freedom of communication, equal opportunity, and a free market, then it must join the global cyber conversation a diplomatic actor in favor of protecting the homeland and promoting democracy.

Daria Etezadi is a Fellow at the Military Cyber Professionals Association and also serves as a Communications Officer for the Cyber Security Forum Initiative. Having studied International Security at Georgetown University's School of Foreign Service, she is particularly interested in using strong communication and public-private partnerships to empower communities and to serve our national security interests. She's published in Newsweek and currently works for the National Geographic Society as their Philanthropic Partnerships Coordinator.

[1] Azar Gat, "Carl von Clausewitz | Prussian General," Encyclopedia Britannica, accessed September 8, 2018, https://www.britannica.com/biography/Carl-von-Clausewitz.

[2] "Command History," accessed September 8, 2018, https://www.cybercom.mil/About/History/.

[3] Brett Daniel Shehadey, "Putting the 'D' and 'I' Back in DIME," accessed August 25, 2018, https://inhomelandsecurity.com/putting-the-d-and-i-back-in-dime/.

[4] The acronym DIMEFIL replaced MIDLIFE--military, intelligence, diplomacy, law enforcement, information, finance, and economics--as referenced in Interim Field Manual FMI 3-07.22, Counterinsurgency Operations, which expired October 2006.

[5] Mary Louise Kelly, "When The U.S. Military Strikes, White House Points To A 2001 Measure," NPR.org, accessed September 8, 2018, https://www.npr.org/sections/parallels/2016/09/06/492857888/when-the-u-s-military-strikes-white-house-points-to-a-2001-measure.

[6] Shehadey, "Putting the 'D' and 'I' Back in DIME."

[7] "Cyber Attack - What Are Common Cyberthreats?," Cisco, accessed August 25, 2018, https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html.

[8] Anthony Giandomenico, "Know Your Enemy: Understanding Threat Actors | CSO Online," accessed August 25, 2018, https://www.csoonline.com/article/3203804/security/know-your-enemy-understanding-threat-actors.html.

[9] Donghui Park, Julia Summers, and Michael Walstrom, "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks - The Henry M. Jackson School of International Studies," accessed August 25, 2018, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

[10] Brian Barrett, "Ukraine Blocks a Russian Hack, a Silk Road Arrest, and More Security News This Week | WIRED," accessed August 25, 2018, https://www.wired.com/story/security-roundup-ukraine-blocked-a-russian-hack-of-its-critical-infrastructure/.

[11] Colin Wood Wood, "Baltimore 911 Dispatch Hacked, Dispatchers Switch to Manual Mode," StateScoop, March 27, 2018, https://statescoop.com/baltimore-911-dispatch-hacked-dispatchers-switch-to-manual-mode.

[12] Jon Schuppe, "Hackers Have Taken down Dozens of 911 Centers. Why Is It so Hard to Stop Them?," NBC News, April 3, 2018, https://www.nbcnews.com/news/us-news/hackers-have-taken-down-dozens-911-centers-why-it-so-n862206.

[13] "Cisco 2017 Annual Cybersecurity Report," Cisco, accessed September 13, 2018, https://engage2demand.cisco.com/en-us-annual-cybersecurity-report-2017.

[14] "2017 Cost of Data Breach Study: United States," Ponemon Institute, accessed September 8, 2018, https://www.ponemon.org/blog/2017-cost-of-data-breach-study-united-states.

[15] Michelle Drolet, "What Does Stolen Data Cost [per Second] | CSO Online," CSO from IDG, January 26, 2018, https://www.csoonline.com/article/3251606/data-breach/what-does-stolen-data-cost-per-second.html.

[16] Gemalto, "Data Breach Statistics by Year, Industry, More," Breach Level Index, accessed August 25, 2018, https://breachlevelindex.com.

[17] Nick Clements, "Equifax's Enormous Data Breach Just Got Even Bigger," Forbes, March 5, 2018, https://www.forbes.com/sites/nickclements/2018/03/05/equifaxs-enormous-data-breach-just-got-even-bigger/#77d2d09153bc.

[18] Jessica Dickler, "In the Wake of the Equifax Data Breach, Consumers More at Risk," March 11, 2018, https://www.cnbc.com/2018/03/10/in-the-wake-of-the-equifax-data-breach-consumers-more-at-risk.html.

[19] Lily Hay Newman, "Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare | WIRED," Wired, April 23, 2018, https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/.

[20] Newman.

[21] "Atlanta Was Warned about Vulnerabilities Months before Cyberattack, Audit Shows - CBS News," CBS, March 28, 2018, https://www.cbsnews.com/news/atlanta-warned-cyber-vulnerabilities-audit-shows/.

[22] Alex Hern, "WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017," The Guardian, December 30, 2017, sec. Technology, https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.

[23] Richard Harknett, "United States Cyber Command's New Vision: What It Entails and Why It Matters," Lawfare, March 23, 2018, https://www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters.

[24] Harknett.

[25] "Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority" (US Cyber Command, March 23, 2018), https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf.

[26] "Langevin, Lieu Introduce Legislation to Re-Establish White House Cybersecurity Advisor Role | Congressman Jim Langevin," Congressman Jim Langevin, May 15, 2018, https://langevin.house.gov/press-release/langevin-lieu-introduce-legislation-re-establish-white-house-cybersecurity-advisor.

[27] Dustin Volz, "White House Cyber Czar to Leave, Return to NSA," Reuters, April 17, 2018, https://www.reuters.com/article/us-usa-cyber-joyce/white-house-cyber-czar-to-leave-return-to-nsa-spokesman-idUSKBN1HN2P3.

[28] Jory Heckman, "GAO Asks Whether Trump Admin. Erred by Axing Cybersecurity Coordinator," FederalNewsRadio.com, July 26, 2018, https://federalnewsradio.com/cybersecurity/2018/07/gao-examining-whether-trump-administration-erred-by-axing-cybersecurity-coordinator/.

[29] Nick Marinos and Gregory C. Wilshusen, "High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation" (Government Accountability Office, September 2018), https://www.gao.gov/assets/700/694355.pdf.

[30] "Vulnerabilities Equities Policy and Process for the United States Government" (The White House, November 15, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

[31] Chris Bing, "Trump Administration Picks New Leader for Vulnerabilities Equities Process Board," accessed September 8, 2018, https://www.cyberscoop.com/grant-schneider-vulnerabilities-equities-process/.

[32] "Cyber Digital Task Force Report" (Department of Justice: Office of the Deputy Attorney General, July 2, 2018), https://justice.gov/cyberreport.

[33] Chris Bing, "Two Democratic Campaigns Hit with DDoS Attacks in Recent Months," Cyberscoop (blog), July 9, 2018, https://www.cyberscoop.com/ddos-democratic-campaigns-primary-dnc-dccc/.

[34] Sean Lyngaas, "Election Exercise Pairs States with Intelligence Community in 'unprecedented' Opportunity," Cyberscoop (blog), August 20, 2018, https://www.cyberscoop.com/election-exercise-pairs-states-with-intelligence-community-in-unprecedented-opportunity/.

[35] U. S. Senator Martin Heinrich (D-N.M.), "Bipartisan Senators: Our Country Needs A Cyber Deterrence Strategy," accessed August 25, 2018, http://www.krwg.org/post/bipartisan-senators-our-country-needs-cyber-deterrence-strategy.

[36] Chris Bing, "Rex Tillerson Proposes New 'cyber Bureau' at the State Department," Cyberscoop (blog), February 7, 2018, https://www.cyberscoop.com/state-department-cyber-bureau-rex-tillerson/.

[37] "Senate Panel Moves to Restore State Cyber Office | TheHill," accessed August 25, 2018, http://thehill.com/policy/cybersecurity/394238-senate-panel-advances-cyber-diplomacy-bill-that-would-restore-state.

[38] Sara Ashley O'Brien, "Microsoft, Facebook and 32 Other Tech Firms Join CyberSecurity Tech Accord," CNNMoney, April 17, 2018, https://money.cnn.com/2018/04/17/technology/cybersecurity-tech-accord/index.html.

[39] James Moar, "The Future of Cybercrime & Security Research Report," Juniper Research, accessed August 25, 2018, https://www.juniperresearch.com/researchstore/innovation-disruption/cybercrime-security/threat-analysis-impact-assessment-leading-vendors.

[40] O'Brien, "Microsoft, Facebook and 32 Other Tech Firms Join CyberSecurity Tech Accord."

[41] Patrick Howell O'Neill, "Air Force's Cloud Migration Frees up Airmen for Cybersecurity Mission Teams," Cyberscoop (blog), April 3, 2018, https://www.cyberscoop.com/us-air-force-cybersecurity-cloud-outsource-it/.

[42] Sara Ashley O'Brien, "Microsoft, Facebook and 32 Other Tech Firms Join CyberSecurity Tech Accord," CNNMoney, April 17, 2018, https://money.cnn.com/2018/04/17/technology/cybersecurity-tech-accord/index.html.

[43] Daisuke Wakabayashi and Scott Shane, "Google Will Not Renew Pentagon Contract That Upset Employees," The New York Times, July 30, 2018, sec. Technology, https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html.

[44] Martin Giles, "The Nasty Surprises Hackers Have in Store for Us in 2018," MIT Technology Review, accessed August 25, 2018, https://www.technologyreview.com/s/609641/six-cyber-threats-to-really-worry-about-in-2018/.

[45] "Weaponizing Artificial Intelligence: The Scary Prospect Of AI-Enabled Terrorism," accessed August 25, 2018, https://www.forbes.com/sites/bernardmarr/2018/04/23/weaponizing-artificial-intelligence-the-scary-prospect-of-ai-enabled-terrorism/#719266e477b6.

[46] "Australia's International Cyber Engagement Strategy," October 2017, https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/pdf/DFAT%20AICES_AccPDF.pdf.

[47] Park, Summers, and Walstrom, "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks - The Henry M. Jackson School of International Studies."

[48] Sean Lyngaas, "Ex-NSA Chief Keith Alexander: U.S. Flying Blind to Nation-State Hackers," Cyberscoop (blog), April 11, 2018, https://www.cyberscoop.com/keith-alexander-nation-state-hackers/.

[49] Lyngaas.

[50] "Advanced Persistent Threat Groups," FireEye, accessed September 8, 2018, https://www.fireeye.com/current-threats/apt-groups.html.

[51] Stilgherrian, "Blaming Russia for NotPetya Was Coordinated Diplomatic Action," ZDNet, accessed August 25, 2018, https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/.

[52] Sean Lyngaas, "Major U.S. Pipeline Hit by Cyberattack on Transaction Software," Cyberscoop (blog), April 3, 2018, https://www.cyberscoop.com/major-u-s-pipeline-disrupted-cyberattack-transaction-software/.

[53] Tim Scargill, "The Growing Need for Cyber Diplomacy," accessed August 25, 2018, https://www.secureworldexpo.com/industry-news/the-growing-need-for-cyber-diplomacy.