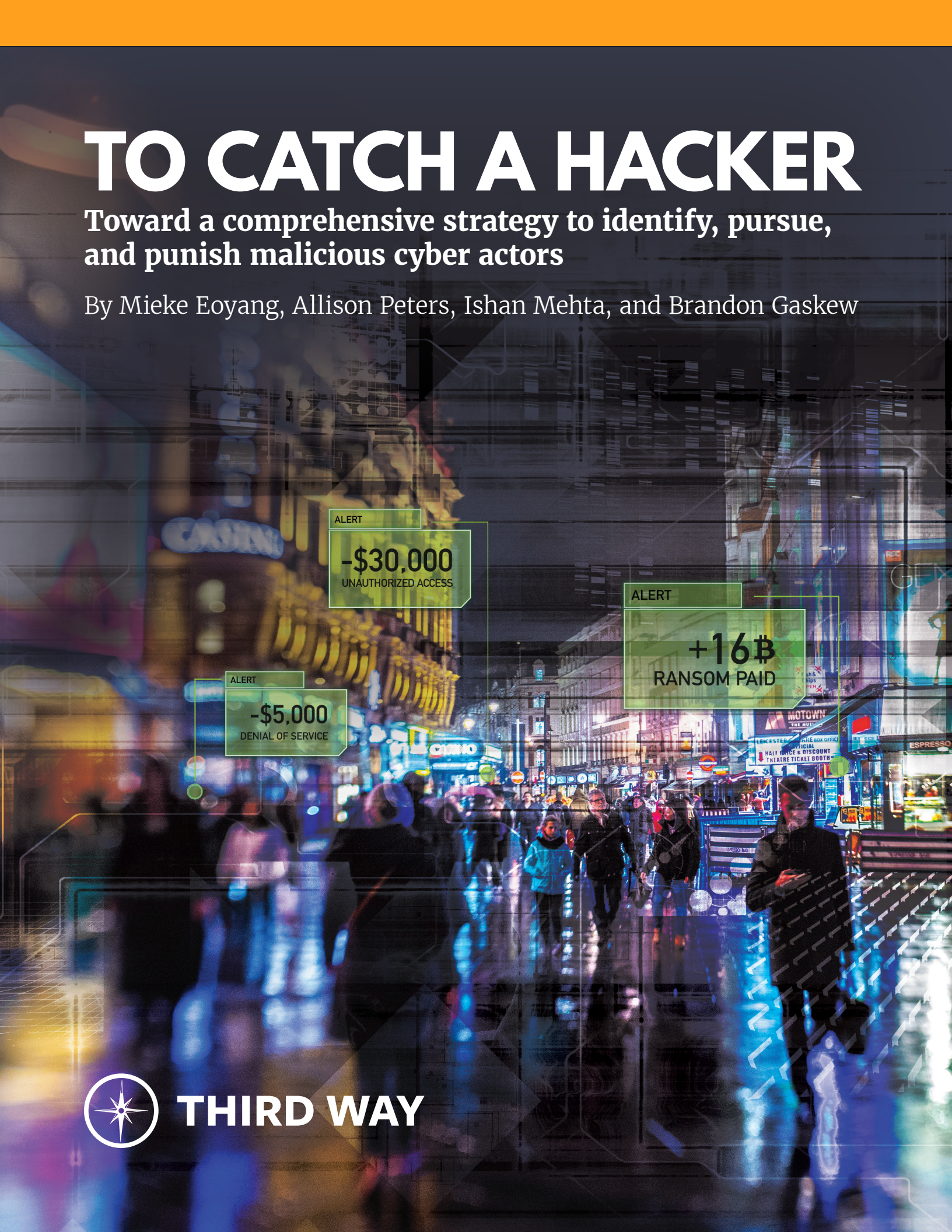
TO CATCH A HACKER

Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors

By Mieke Eoyang, Allison Peters, Ishan Mehta, and Brandon Gaskew



THIRD WAY

THIRD WAY

Acknowledgments

We would like to acknowledge and thank the many people who have contributed to this report and shared their perspectives on the cyber enforcement gap. The support, expertise, and guidance that has been provided to us has been invaluable in steering the direction of this report.

In particular, we would like to thank our former fellows Jayati Dev and Adam Twardowski for their incredible research support without which this report would not be possible. We would also like to thank Third Way's Founders Jim Kessler and Jonathan Cowan for their endless support and strategic guidance.

Additionally, we are grateful to the members of the Advisory Board of Third Way's Cyber Enforcement Initiative for their continued inputs and support. Each brings a wealth of diverse experience and expertise to the Advisory Board and we are thankful for their partnership. However, the views expressed in this paper should be viewed as the authors' alone and not presumed to be endorsed by the Cyber Enforcement Initiative's Advisory Board:

Gina Abercrombie-Winstanley
James Baker
Cassandra Chandler
Jennifer Daskal
Rajesh De
Mary DeRosa
Judith Germano
Orin Kerr
Andrew McLaughlin
Christopher Painter
Chan Park
Gregory Rattray
Paul Rosenzweig
Ari Schwartz
Ben Wittes

Finally, we would like to thank the many individuals we have spoken to throughout the development of the Third Way Cyber Enforcement Initiative who have provided critical ideas, data, and feedback to us. In particular, we are grateful to Eli Sugarman, Michael Woods, Taxpayers for Common Sense, the Consumer Bankers Association, Kathryn Rosen, Matthew Waxman, Jonah Force Hill, Kevin Bankston, Joshua Alexander, David Lieber, Jeff Ratner, Bruce Schneier, Suzanne Spaulding, Matt Tait, Allan Friedman, and Jing de Jong-Chen. We are thankful to the many other representatives of industry and civil society groups who have provided us with their thoughts on this Initiative.

To Catch a Hacker: Policy Recommendations

Cybercriminals operate with a sense of impunity as only 0.3% of malicious cyber incidents see an arrest, according to our analysis of FBI reported data. What that means is that the United States is facing a massive cyber enforcement gap just as the cybercrime wave continues and malicious cyber activity that threatens our national security is becoming more common. To close the cyber enforcement gap, we call for a comprehensive, strategic approach to identify, stop, and punish malicious cyber actors. The US maintains robust efforts to secure existing computer networks, but heavily relying on air tight systems and mistake-less human users can only accomplish so much. In our new paper, we call for ten US policy actions (some that build off existing efforts) that can form the contours of such a strategy to go after human attackers.

Domestic Enforcement Reform

1. **A Larger Role for Law Enforcement:** Strengthen capacity building efforts so that law enforcement, enabled by diplomacy, can target the humans behind cyberattacks.
2. **A Cyber Enforcement Cadre:** Address not only workforce shortages, but the way the cyber enforcement workforce is trained, incentivized, and retained.
3. **Better Attribution Efforts:** Increase investments in research and development for attribution technology, better digital forensics, and prioritize efforts to build international alliances that improve timeliness and impact of attribution efforts.
4. **A Carrot and Stick Approach to Fugitives:** Adopt a broader reward-based system to incentivize information sharing that can lead to arrests of malicious cyber actors balanced with the smart use of targeted sanctions.

International Cooperation and Coordination Reform

5. **An Ambassador-level Cyber Quarterback:** Institute an ambassador-level cyber coordinator position at the State Department with a clear mandate and resources on cyber enforcement.
6. **Stronger Tools in the Diplomacy Arsenal:** Expand the number and streamline processes for agreements with other countries that help bring cyber attackers to justice and continue to utilize the multilateral Budapest Convention.
7. **Better International Capacity for Enforcement:** Support efforts to build the capacity of other countries on cybercrime investigations, while ensuring cybercrime and cybersecurity efforts are not used to suppress civil liberties and human rights.

Structural and Process Reform

8. **Better Success Metrics:** Establish mechanisms to measure the scope of the cyber enforcement problem and the effectiveness of government efforts.
9. **Organizational Changes and Interagency Cooperation:** Evaluate further needed policy changes to de-conflict the missions of the agencies responsible for cyber enforcement.
10. **Centralized Strategic Planning:** Institute an overarching, comprehensive strategy for US cyber enforcement led by a senior official at the White House.

The lack of an overarching strategy to deal with this growing threat is ominously analogous to the pre-9/11 US government approach to terrorism. We need a strategy that doesn't just focus on building a better safe, but focuses on catching the safecracker.

To Catch a Hacker:

Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors

By Mieke Eoyang, Allison Peters, Ishan Mehta, and Brandon Gaskew

Introduction

On February 21, 2018, computer monitors in Colorado's Department of Transportation went gray. In simple red and black text, an ominous message: "All your files are encrypted." For three bitcoin, or what was then $27,000, the department could have the decryption keys.[1] They refused.[2] Soon after, the department lost use of 150 servers and shut down 2,000 employee computers.[3] Two weeks later the department was hit a second time, by another strain of the same ransomware, hampering already costly recovery efforts.[4] One month following this attack, Atlanta's municipal computer systems came to a slow crawl. Again, a message appeared on the city's network demanding ransom in exchange for the decryption of their files. One-third of all city services were sidelined and critical data, including police files and evidence, was lost.[5] In Indiana this past January, the Hancock Health Hospital system was hit with the same type of ransomware. The attackers took hostage of more than 1,400 files on their networks, which included medical records of current patients, only releasing them once a ransom was paid.[6]

Each of these incidents were part of the same ransomware attack known as SamSam. SamSam may be thought of as just a series of ones and zeroes but behind SamSam is a person or a set of people. They could be a member of a terrorist group, a criminal organization, or an agent of a nation-state, seeking to exploit computer vulnerabilities to advance their agenda. They may simply be a cyber thief – finding clever ways of breaking into systems and collecting ransoms through hard-to-trace cryptocurrencies. But whoever it is they have collected payments totaling an estimated $6 million since 2015,[7] and they have cost their victims even more millions of dollars in recovery costs. Atlanta alone could reportedly spend $17 million in incident response and mitigation.[8] This attack was technically sophisticated, both in its invasion and its execution, and hit victims across many different jurisdictions. The person or persons behind SamSam are still at large, and as this report will show, it is safe to assume that they believe they will never be caught. This must change.

In this paper, we argue that the United States currently lacks a comprehensive overarching strategic approach to identify, stop and punish cyberattackers. We show that:

1. **There is a burgeoning cybercrime wave:** A rising and often unseen crime wave is mushrooming in America. There are approximately 300,000 reported malicious cyber incidents per year, including up to 194,000 that could credibly be called individual or system-wide breaches or attempted breaches.[9] This is likely a vast undercount since many victims don't report break-ins to begin with.[10] Attacks cost the US economy anywhere from $57 billion to $109 billion annually and these costs are increasing.[11]
2. **There is a stunning cyber enforcement gap:** Our analysis of publicly available data shows that cybercriminals can operate with near impunity compared to

their real-world counterparts. We estimate that cyber enforcement efforts are so scattered that less than 1% of malicious cyber incidents see an enforcement action taken against the attackers.

3. **There is no comprehensive US cyber enforcement strategy aimed at the human attacker:** Despite the recent release of the *National Cyber Strategy*, the United States still lacks a comprehensive strategic approach to how it identifies, pursues, and punishes malicious human cyberattackers and the organizations and countries often behind them. We believe that the United States is as far from this human attacker strategy as the nation was toward a strategic approach to countering terrorism in the weeks and months before 9/11.

In order to close the cyber enforcement gap, we argue for a comprehensive enforcement strategy that makes a fundamental rebalance in US cybersecurity policies: from a heavy focus on building better cyber defenses against intrusion to also waging a more robust effort at going after human attackers. We call for ten US policy actions that could form the contours of a comprehensive enforcement strategy to better identify, pursue and bring to justice malicious cyber actors that include building up law enforcement, enhancing diplomatic efforts, and developing a measurable strategic plan to do so.

This rebalance can only be achieved if we increase the emphasis on, and resources in, US cybersecurity efforts to include a greater focus on identifying, stopping, and punishing the human attacker. This means:

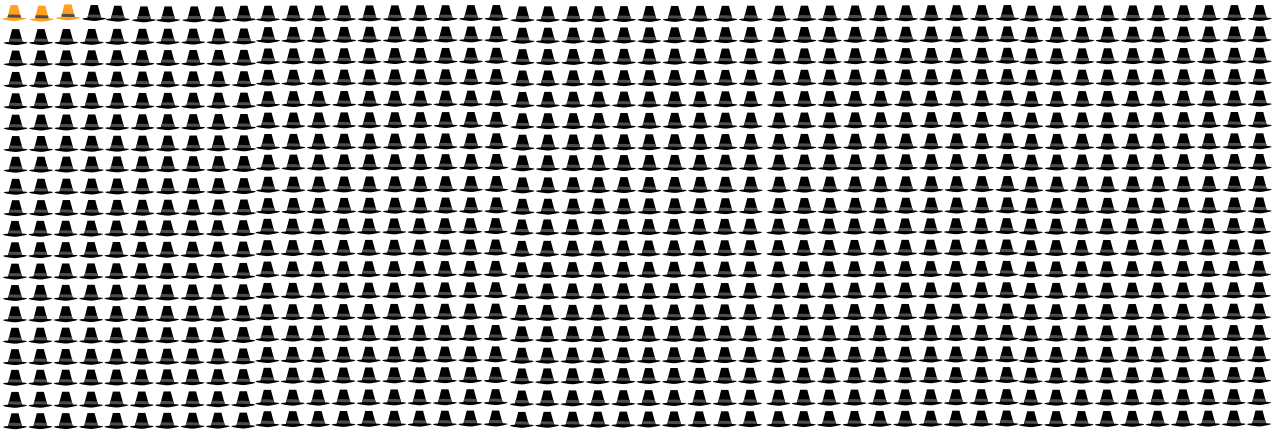
- Shedding a blame-the-victim mentality that drives the defensive approach in favor of one of shared responsibility that invigorates a catch-the-hacker approach, and
- Creating a more balanced approach that places more emphasis on law enforcement and diplomacy to prevent an overreliance on the military.

SamSam is only one of thousands of attacks affecting Americans, and it is just a matter of time before another malicious actor aims at bigger targets for reasons far more nefarious than SamSam. While system and network owners and operators have obligations to provide the best security they can, we have seen time after time that a determined attacker will eventually get through. By putting the human attacker in the crosshairs of America's cybersecurity efforts we can instead raise the costs of their actions to not only bring attackers to justice, but also to deter future attacks—whether they come from criminals, organizations, or hostile governments.

The Enforcement Gap and the Burgeoning Cybercrime Wave

Calculating the scope of the cyber enforcement gap is a challenging if not impossible task due to the lack of comprehensive public data across agencies. Based on our analysis of the publicly available data that does exist from federal, state, and local sources, we estimate the chance of arresting a cybercriminal is less than 1% of the total number of malicious cyber incidents reported annually to the federal government. We define this enforcement rate as the ratio of arrests to the number of incidents reported, as data on indictments and prosecutions is not consistently reported at all levels. In other words, this enforcement rate may be optimistic as arrests do not mean conviction.

Only 3 in 1,000 cyber incidents see an arrest



Note: every 'black hat' represents one cyber incident

By comparison, the clearance rate for property crimes was approximately 18% and for violent crimes 46%, according to the Federal Bureau of Investigation's (FBI) Uniform Crime Report (UCR) for 2016. The clearance rate is the number of cases where at least one person has been arrested, charged with the commission of an offense, and referred for prosecution.[12] Those numbers in comparison to a less than 1% rate for just arrests for computer crimes is a drastic difference in the rate of enforcement.

What happens when there is a criminal, terrorist, or other malicious actor engaging in destabilizing activity in which the likelihood of getting caught and punished is close to zero? In this section, we lay out some of the dimensions of the cybercrime wave in the United States and globally. The burgeoning cybercrime wave is the result of both the ubiquity of technology and the one-sided nature of our defenses: a reliance on building systems that are harder and harder to breach, training lay users to be harder and harder to fool, and faced with hackers who are harder and harder to catch.

Malicious cyber actors are rarely caught and the effort to do so is uncoordinated, under-resourced, and under-prioritized.

The ubiquity of technology means every critical infrastructure sector in the United States—from nuclear power plants to water facilities— utilizes some form of computer-enabled system for their operations that, if attacked successfully, could have devastating impacts on Americans. That is why the US Department of Treasury has designated cybersecurity incidents as one of the biggest threats to the stability of the entire US financial system.[13]

Nearly every US citizen's personal, financial, and sensitive information is stored on a connected device in some form. There are now more active mobile phones, which store sensitive information on them, than the number of people on the planet, and Cisco predicts 27.1 billion up from 17.1 billion in 2016 connected devices by 2021 or roughly 3.5 per person.[14] Each device is

potentially an attack vector that a malicious actor could exploit. Each device has applications, operating systems, and network connections, which all have potential vulnerabilities for an attacker to exploit.

And as we discovered and noted above, the effort to catch malicious cyber actors is uncoordinated, under-resourced, and under-prioritized— just a handful of reasons why those actors are rarely caught.

The Cybercrime Wave

There's a rising and often unseen crime wave happening in America. The FBI received 298,728 self-reported cybercrime complaints in the United States in the year 2016 alone through its Internet Crime Complaint Center (IC3).[15] Of those, as many as 193,700 cybercrimes could credibly be described as serious attempts at individual or systemic cyber breaches, including such activities as identity theft (16,878 reported incidents), personal data breach (27,573), ransomware (2,673), and malware (2,783), according to the IC3 database.[16] This is only part of the picture, as the FBI estimates that fraud victims report only 15 percent of crime nationwide to law enforcement.[17] That may mean there are 2 million cybercrimes per year, or roughly equal to 1.4 million burglaries in a given year, if underreporting estimates are accurate.[18]

The IC3 is an FBI center established in May 2000 to serve as a central hub for Internet crime victims to alert federal, state, and local authorities to suspected criminal Internet activity.[19] From 2013 to 2017, the IC3 has received over 1.4 million complaints.[20] While IC3's methodology tabulates each individual's complaint as a separate entry, the Verizon Data Breach Investigations Report states that there have been over 53,000 incidents targeted at organizations.[21] And America isn't alone. The International Police Organization (INTERPOL), the multilateral organization that facilitates global law enforcement cooperation to fight international crime, states that cybercrime is one of the fastest growing areas of crime.[22]

What do we mean by "cybercrime?"

While this paper refers to the more general term "malicious cyber activity" in certain places, or "cyberattack" for high-impact incidents, we're primarily focused on cybercrime or crimes that use or target computer networks. This includes data theft, fraud, distributed denial-of-service (DDoS) attacks, worms, ransomware, and viruses.[23] We recognize the concerns raised with the term "cyberattack,"[24] but considering its widespread adoption and lack of global consensus on overall terminology, we continue its use in certain places to describe significant cyber incidents.

Cybercriminals come in all shapes and sizes. The FBI assesses that these threats can come from attackers with a host of different motivations and affiliations.[25] High-level intrusions usually stem from attackers affiliated with global organized crime syndicates or state-sponsored attackers.[26] Hacker-rings or lone actors typically run mid-level identity fraud or carding schemes for financial gain.[27] Finally, privacy crimes, such as doxing, are targeted crimes usually committed by lone actors with malicious personal or political motivation.[28]

However, that landscape is changing fast. Nation-states like North Korea have attacked systems for a variety of reasons. Sony was hacked to prevent reputational harm, the Bank of Bangladesh heist was for financial gain, and the WannaCry attack was motivated by a desire to cause economic chaos.[29] Terrorists have also continued to use the Internet as a key operational tool, including launching malicious cyberattacks against targets in the United States.[30] Many of these crimes threaten the stability of systems, either intentionally or through the way they spread.

There are also a few categories of malicious cyber activity that, while extremely serious, do not threaten to disrupt the stability of systems. While critically important, our recommendations will not focus on what the Department of Justice refers to as "cyber-enabling crimes threatening personal privacy," such as cyber-enabled stalking, non-consensual pornography, and cyber-enabled harassment.[31] The recommendations also do not cover issues related to child pornography. These devastating crimes involve potentially very different motivations than other forms of cybercrime and deserve dedicated research related to government responses to these crimes.

The rewards from a successful cyberattack are high, and the costs (in terms of risk) low, which has incentivized malicious actors to develop more effective hacking techniques. Some examples of those techniques and their costs are as follows:

- Ransomware attacks, where an attacker encrypts the victim's data and typically only frees it when a ransom is paid, doubled in frequency between 2016 and 2017 with incidents affecting a diversity of targets and disrupting the operations of public services and large corporations around the country and globe.[32]
- Malware attacks on mobile devices have now surged with an increase in 54% globally from 2016 to 2017.[33]
- Software update supply chain attacks in which malware is implanted into software packages to infect computer systems has increased by 200 percent globally in 2017 from the year prior.[34]
- The Ponemon Institute estimates the average total cost of a data breach at $3.62 million.[35]
- IC3 calculated that reported crimes, such as identity theft and online fraud, cost victims more than $1.42 billion.[36]
- In 2016, the White House Council of Economic Advisors estimated in 2016 that malicious cyber activity costs the United States economy between $57 billion and $109 billion per year.[37] Other estimates put the number as high as $3 trillion for the global economy annually.[38]

The targets that malicious cyber actors are hitting with their attacks span a wide spectrum of sectors with the healthcare, public, accommodation, and manufacturing bearing the brunt of security incidences and data breaches.[39] For example, the Mirai Botnet attack in October 2016 led to some of the world's most popular websites going offline for up to twelve hours—including

Netflix, Twitter, Reddit, PayPal, The New York Times, and The Wall Street Journal—costing these companies millions of dollars in lost revenue.[40]

Criminal use of technology is creating entirely new categories of crime that never existed before the digital age.[41] It is ending the notion of "good neighborhoods" and "bad neighborhoods" when it comes to crime because cyberspace is both ubiquitous and borderless. New types of crime from carding schemes, to ransomware, to crypto mining have made investigations even more complex where the victim and perpetrator may be unknown to each other and may be in different countries. Technologies like Virtual Private Networks (VPNs), the Tor browser,[42] and cryptocurrencies like Bitcoin lend anonymity, or at least perceived anonymity, to the malicious cyber actor.

These technologies also help make attacks more effective and easier to execute. Tools created using machine learning allow malicious cyber actors to perform reconnaissance, or information-gathering efforts, more efficiently and to a much higher degree of accuracy. For attackers, the more information they have about the systems and the operators of the system, the more effective the attack. Attackers can assess information regarding potential vulnerabilities, unpatched systems, and exploits much quicker through the advanced technology available to them. Marketplaces and discussion forums on the dark web have made buying and using cyber-exploits as easy as shopping for shoes online.[43]

Cybercrime has hit victims across the United States in every single state and territory. California, Florida, Texas, New York, and Pennsylvania—states with very different demographics, corporate representation, and cybersecurity laws—make up the highest number of victims.[44] These states have been hit by devastating economic losses as a result of the cybercrime wave.[45]

Cybercrime's impact is so broad that it has security implications for the entire nation and globe. A single incident like the WannaCry cyberattack in 2017 affected more than 200,000 computer systems in 150 countries and potentially cost the world economy $4 billion.[46] Malicious cyber actors have attacked health care systems and critical infrastructure in the United States, such as Industrial Control Systems (ICS), the electric grid, and dams. A successful attack executed on these systems can threaten life, property and cause large scale destruction. In March of this year, the Department of Homeland Security (DHS) and the FBI issued an alert that the Russian government was targeting the electric grid and other critical energy systems.[47] In 2015, malicious actors managed to access the ICS software at a water treatment plant and tampered with the controls related to water flow and the amount of chemicals used to treat the water.[48]

The cybercrime wave is so big it should be setting off alarm bells at every level of law enforcement. And yet, the response from the enforcement community is a drop in the bucket compared to the sheer volume of crimes occurring.

Beyond financial harm, some cyberattackers, at the behest of nation states, are doing real damage to US national security. US defense contractors have become targets for adversaries seeking to steal national security secrets. Recently, Chinese government hackers infiltrated the network of a US Navy contractor, stealing data on undersea warfare and secret plans for US submarine anti-ship missiles.[49] China and others are hacking US companies to steal intellectual property, at an estimated cost of $225 billion to $600 billion annually.[50] Hostile nations are also using cyber operations to affect US national security personnel directly. In 2014 and 2015,

the Office of Personnel Management[51] suffered a massive data breach exposing the sensitive information of up to 22 million people, including personal information in their security clearance forms. And, of greatest concern, Russia's malicious cyber activities aimed at trying to affect the outcome of the 2016 US presidential election have been well-documented in indictment after indictment.[52]

The cybercrime wave is so big it should be setting off alarm bells at every level of law enforcement. And yet, the response from the enforcement community is a drop in the bucket compared to the sheer volume of crimes occurring.

The Enforcement Gap

We know how big the problem is, but assessing the adequacy of the response to the problem is tougher. Not only are we in a cybercrime wave, but we also have a hidden enforcement crisis.

Third Way's analysis estimates that the enforcement rate for reported incidents of the IC3 database is 0.3%. Taking into account that cybercrime victims often do not report cases, the effective enforcement rate estimate may be closer to 0.05%.

How did we calculate the cyber enforcement rate?

There were significant challenges to estimating an aggregate cyber enforcement rate for the purpose of this research. Most significantly, there are currently no public databases which specifically report enforcement metrics on computer crime across all localities in the same way that exists for other categories of crime. We analyzed close to two dozen public and private databases to calculate the cyber enforcement rate. There were numerous discrepancies and inconsistencies across the different datasets that estimated the number of cyber incidents. Additionally, none of the datasets had comprehensive attribution information. To calculate the enforcement rate, we therefore decided to use Department of Justice (DOJ), FBI, and Secret Service self-reported numbers on incidents and arrests. This data is not perfect and includes categories of crimes that we do not directly address in our recommendations, such as privacy crimes, and the number of incidents relies on reports by victims to the federal government. Yet, these are the best datasets publicly available that give a picture of the enforcement gap rate for the United States. This is precisely why we call for better comprehensive reporting in our recommendations later in this report.

The FBI IC3 received 298,728 complaints in 2016.[53] By analyzing a variety of official US government reporting databases, we determined that there were fewer than 1,000 arrests that year between federal, state, and local law enforcement agencies for reported cybercrimes.

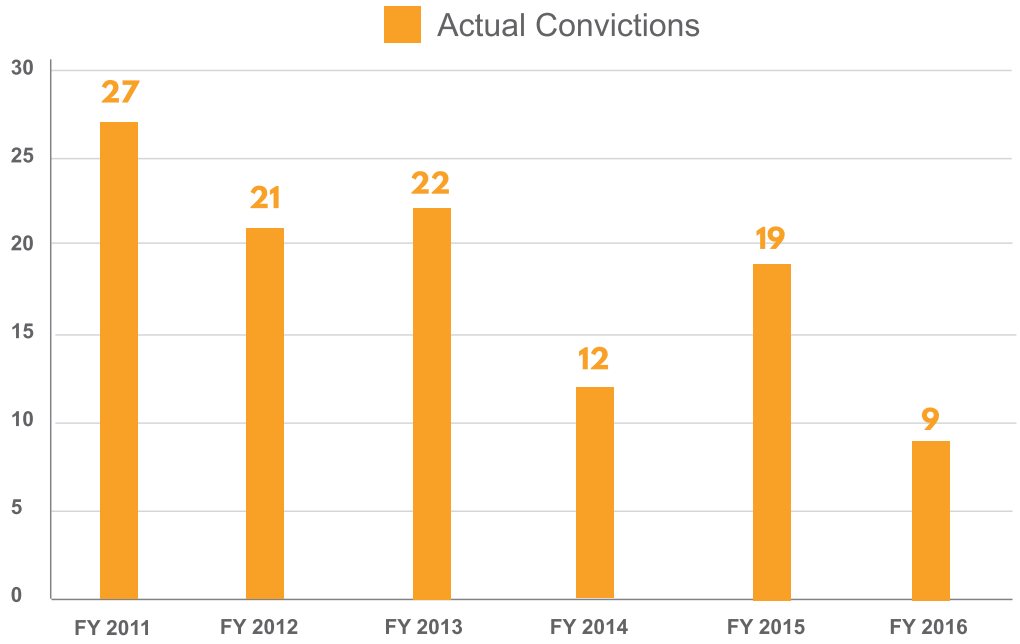
Specifically, to determine the number of enforcement actions we looked at various reports of the number of cybercrime arrests. In 2014 and 2015, through the FBI's Uniform Crime Reporting (UCR) Program, the Bureau reported the number of individuals arrested for "criminal computer intrusion" by each FBI field office. The total number was 105 for 2014 and 49 for 2015.[54] In 2016, UCR transferred to

the National Incident-Based Reporting System (NIBRS) and no longer separates out the arrest numbers for computer crime in their reporting. However, in 2016, the arrest numbers for computer crime by state and local law enforcement were included through NIBRS for the first time. The number reported under "hacking/computer invasion" crime was 581 for 2016, the most recent year reported, which includes reporting from 6,849 state and local agencies.[55] The Secret Service reported 251 cybercrime arrests in 2016.[56] If we assume the FBI field offices made a similar number of arrests as in the previous two years in 2016 combined, we arrive at the total federal, state, and local computer crime arrests to be between 871 and 927 for 2016, barring a significant increase in federal arrests.

To determine a denominator, we looked at various reports that tabulate the number of cyber incidents and cybercrime. The FBI IC3 report for 2016 notes 298,728 complaints received that year.[57]

Based on these numbers, we estimate the enforcement rate at 0.31%. Considering only one in six victims of cybercrime report to law enforcement,[58] the *effective* enforcement rate estimate may be closer to 0.05%.

Number of Convictions for Internet Fraud



Source: justice.gov

The number of convictions reported by the FBI alone is even lower than the number of arrests used to calculate the cyber enforcement rate. The only DOJ document that Third Way has found that reports prosecution numbers is the FBI Congressional Budget Justification document, which lists them as "Internet Fraud." The FBI reports that using the IC3 data to develop law enforcement referrals, it only secured nine convictions in 2016, down from nineteen cases the previous year.[59]

While these cases are important and meaningful in punishing cyber attackers, they represent a very small drop in a very large bucket. And the low enforcement rate for cybercrime has consequences. Cybercriminals are operating with near impunity compared to their real-world counterparts. Given the increasing ease of committing these crimes and the unlikely chance of being caught, it is no wonder that this category of crime is on the rise.[60]

In the face of such a small response from law enforcement, some believe the private sector should take matters into their own hands and go on the offense. A widely-perceived enforcement failure will lead victims to eventually say "enough is enough" and act on their own.

This offensive approach is not to deter attackers but to disrupt their capabilities, including rendering useless their devices, locking accounts, and blocking server access.[61] Proponents of so-called "hacking back" will acknowledge that the impulse comes from a recognition of an enforcement failure and a frustration about the inability to do anything to stop the attacker.[62] But hack back exposes the counter-hacker to their own liability for unauthorized access to someone else's system and malicious action. Additionally, malicious cyber actors use proxy systems that are tough to identify and retaliations may target systems of innocent individuals. In a well-functioning system, victims have confidence that law enforcement is doing their best to catch the attacker and have a reasonable chance of doing so.

The Cyber Enforcement Gap: Third Way's analysis estimates that the enforcement rate for reported incidents of the IC3 database is 0.3%. Taking into account that cybercrime victims often do not report cases, the effective enforcement rate estimate may be closer to 0.05%.

Furthermore, America's enforcement gap has been largely hidden because there are no good metrics to assess law enforcement response. The number of reported crimes is proportionally miniscule in comparison to the number of actual crimes. Anecdotal data on high profile incidents and prosecutions do not provide a full picture of what's at stake. The traditional crime statistics also do not reflect the kinds of new computer enabled crimes that are happening today.[63] And, the lack of clarity in how to report crimes means that state, local, and federal agencies do not report cybercrime in a clear or consistent manner.

There is a clear enforcement gap in cybercrime that must be urgently addressed. The problem is right in front of us, but policymakers are largely not paying any attention to it. The recent indictments against Russian and North Korean state cyber actors may be perceived as progress, but they do not address the large number of crimes that go unnoticed.[64] The lack of action, the rising costs as a result, and the apparent impunity of these malicious actors would not be tolerated in any other domain. But it often seems like an afterthought in the realm of cyber.

Closing the enforcement gap will also require understanding the motivation of the human attacker and their relationship to foreign states or other non-state actors that might harbor or support them. This is an essential factor in crafting an effective policy solution to compel behavioral change. There are four reactions the state can take toward the attacker: passive, ignore or abet, or order or conduct.[65] Depending on the nature of the nation state and the cyber attacker(s) and their motivations, the tools used to target a change in behavior of both the state and attackers will vary. It's important to deeply understand the nature of this relationship to employ the most effective solution once the human attacker has been identified.

The Spectrum of State Responsibility

Passive	Ignoring or Abetting		Ordering or Conducting	
1. State-prohibited. The national government will help stop the third-party attack	**3. State-ignored.** The national government knows about the third party attacks, but is unwilling to take any official action	**5. State-shaped.** Third parties control and conduct the attack, but the state provides some support	**7. State-ordered.** The national government directs third-party proxies to conduct the attack on its behalf	**9. State-executed.** The national government conducts the attack using cyber forces under their direct control
2. State-prohibited-but-inadequate. The national government is cooperative but unable to stop the third-party attack	**4. State-encouraged.** Third parties control and conduct the attack, but the national government encourages them as a matter of policy	**6. State-coordinated.** The national government coordinates third party attackers such as by "suggesting" operational details	**8. State-rogue-conducted.** Out-of-control elements of cyber forces of the national government conduct the attack	**10. State-integrated.** The national government attacks using integrated third-party proxies and government cyber forces

Source: Jason Healey, Atlantic Council

Working with states that prohibit attacks may require increased cooperation or capacity building to be able to coordinate efforts to bring enforcement actions against the attackers. If the state is ignoring or abetting the attacker, diplomatic pressure will need to be brought to bear to change the state's attitude about its complicity in the attacks. This may in some cases bring a different set of more coercive tools to bear. Finally, if the state has direct responsibility for the attacks and is encouraging or conducting them as part of the attacking state's foreign policy, then the victimized nation may have to consider the full spectrum of actions available, beyond law enforcement and diplomacy, against the attacking nations.

Ultimately, if malicious cyber actors are working at the behest of nation-states to advance their objectives through cyberattacks, they are likely to be much more difficult to punish or change their behavior at all. Even if you are able to do so either by sanctioning or arresting them in another country, it is likely that the foreign government sponsor would just recruit others to take up the banner and continue the attacks.

Importantly, although there are a number of nation-states that are using cyberattacks as a tool to advance their objectives, this does not in any way mean the United States can ignore the massive cybercrime wave that is occurring, granting impunity to the large number of malicious cyber actors that may be able to be identified, stopped, and punished. Regardless of whether the behavior is the decision of an individual or the state, whether it's the fingers on the keyboard or the ones signing the order, it is still a human whose decision-making process can be impacted, and who can (and should) feel real consequences.

Rebalancing the US Cyber Approach

Given the magnitude both of the cybercrime wave and the enforcement gap the nation faces, it's clear that the current approach is insufficient. As the number and intensity of cyberattacks has increased, robust efforts at cyber defense are necessary, but not nearly sufficient. A determined attacker will get through even the most heavily defended system. Focusing on making the most secure target possible to the exclusion of a substantial focus on also getting the attacker allows malicious actors to continue to multiply and operate with a sense of impunity. And while there are an infinite number of vulnerabilities and a growing number of attacks, there are a finite number of attackers. To stop those attackers, we must transform both the way we think about cybersecurity and rebalance our efforts to include a greater focus on going after the human attacker.

To be sure, there has been a growing emphasis under the Obama and Trump Administrations in going after malicious cyber actors through law enforcement actions and imposing other types of costs to change their behavior. This includes the number of actions that have been taken against malicious cyber actors working on behalf of adversarial nation-states. However, as the enforcement rate makes clear, these efforts are not nearly enough. Nor have they been sufficiently resourced and given the political leadership necessary to make progress.

We need to change the calculation of malicious cyber actors by balancing defense of systems with an offense designed to stop and deter the human.

Most of the cybersecurity efforts are currently defensive in orientation, focused on protecting systems and networks. Building better firewalls against attacks, creating better passwords, and educating users are all critical. But a strategy primarily developed around building impregnable cyber walls and mistake-proof human users cannot succeed. We need to create a more robust parallel effort around how we identify, stop, and punish the human attacker. We need to change the calculation of malicious cyber actors by balancing defense of systems with an offense designed to stop and deter the human.

It's no surprise that thus far the American government has had a heavy focus on defending systems and networks. This approach has been, in part, driven by a blame-the-victim mentality in cybersecurity. When there is a major cyber breach of a company they are often hauled up before Congress and made to apologize for their lapses, their holes in security, and their failure to have the most up-to-date defenses. To be sure, some of these companies deserve criticism for not taking proper precautions. For example, Equifax, a consumer reporting agency, which holds millions of Americans personally identifiable information, was hacked in 2017

because they failed to update their software after knowing about the risk for months. This led to hackers exploiting the vulnerability, exposing the information of 143 million Americans.[66] This was preventable and companies that similarly fail to address known vulnerabilities should be held accountable. Corporations in America fear the losses and reputational harm that come from a major breach, and thus focus their efforts on defending their networks and data.

Beyond the private sector, the government's own approach to cybersecurity has also been primarily defensive in nature. In 2008, the Bush Administration adopted a new approach to securing the internet, the Comprehensive National Cybersecurity Initiative (CNCI),[67] which established a broad series of policies aimed at trying to secure the United States in cyberspace.[68] Later declassified by President Obama, it was a call to arms establishing and modernizing the government's role in defending networks, sharing information, and increasing cyber-education. The CNCI established the basic parameters of the debate which focused on: network security, securing critical infrastructure, and global supply chain risk mitigation.[69] This overarching focus on defense is one that has continued in the cybersecurity debate to this day, including the Trump Administration's recently released the *National Cyber Strategy*.[70] While the Strategy is an important conceptual framework for strengthening law enforcement efforts at home and abroad and imposing consequences on cyberattackers and nation-state sponsors, the Strategy still heavily centers on cyber defense with only a few short sections committed to pursuing hackers. It proposes no advances to how the government will assess its progress on enforcement and has few innovative, new solutions to address the number of tremendous challenges that exist in closing the enforcement gap.

Yet, the government is the only institution with the authority to do anything about the human attacker and the capability to bring them to justice. The government's abilities in this area are quite broad, but in our assessment, priorities and resourcing have been improperly aligned to go after the attacker. When there is a conversation about how the government is going after hackers it is often framed in military terms, which is inapplicable against most of the attackers we see today.

Military leaders have been debating how large a cyberattack must be in order to make it an act of war since the massive Russian denial of service attacks that crippled Estonia in 2007.[71] Those attacks were largely the inspiration for the North Atlantic Treaty Organization's (NATO) efforts to develop the Tallinn Manual, an attempt to set the rules for cyber war.[72] Multiple efforts have been made to define the rules of cyberwar and to develop Digital Geneva Conventions.[73] Given the vast amount of funding the military has to invest in cybersecurity, and the over-militarization of US foreign policy generally, it is no surprise that the debate around when a cyberattack will trigger a kinetic response is robust.

For example, the elevation of US Cyber Command to a unified combat command shows the political consensus in the Executive Branch and in Congress to embrace a military approach. On August 18, 2017, the administration elevated Cyber Command to a unified command, and according to a White House statement, this "... demonstrates our increased resolve against cyberspace threats and will help reassure our allies and partners and deter our adversaries." [74] This military priority is reflected in Cyber Command's request of approximately $647 million for fiscal year 2018, a 16% increase over the previous year.[75] Additionally, in August 2018, the Trump administration relaxed the rules in Presidential Policy Directive 20, which governs the use of US offensive and defensive cyber operations, especially those to "deter foreign election influence and thwart intellectual property theft by meeting such threats with more forceful responses."[76]

Yet, until that threshold is crossed, all of those military cyber-weapons are limited to cyberspace and cannot physically touch the human cyber attacker. While the Pentagon is developing weapons that may deny the attacker access to their tools, these responses may have collateral consequences and are limited in their ability to impose consequences on the individual human attacker. Given the range of types of attacks and attackers, cyber weapons may not be the best response in a particular situation. There are other tools besides military action that can be used to stop the attacker.

Rather than responding with military force, the government can use its Title XVIII authorities to bring law enforcement to bear against the attacker at any time. Unfortunately, the current prioritization undervalues and underinvests in that response. We can only stop this cybercrime wave and close the cyber enforcement gap by transforming law enforcement, enabled by diplomacy, to go after the attacker.

America needs a comprehensive cyber enforcement strategy aimed at identifying, stopping, and punishing cyberattackers, which it currently lacks. This strategy would need both domestic and international components to it as well as the structure and process in place to achieve its objectives. We lay out elements of that strategy below.

Toward a Comprehensive Cyber Enforcement Strategy

In this section we lay out the contours of what a comprehensive cyber enforcement strategy could look like. These broad recommendations are aimed at achieving the fundamental rebalance we aim to see in America's cybersecurity approach to dramatically improve the country's security. Over a multi-year initiative, Third Way will develop more detailed policy proposals to advance these efforts.

Below we detail our recommendations for areas of priority that require urgent attention by policymakers. Some of these recommendations are aimed at building upon existing streams of efforts while others propose new reforms. These recommendations fall into three general categories of those that deal with: 1) domestic enforcement reform, 2) international coordination and cooperation reform, and 3) internal US government reform efforts to put in place the structure and process to lead all of these efforts.

Domestic enforcement reform

Recommendation #1: A Larger Role for Law Enforcement

Absent a state of war, the primary US government agencies with the authority and ability to identify, stop, and punish the humans responsible for these attacks are law enforcement—enabled by our diplomats and allies. Law enforcement is how we deal with people who have broken our laws in peacetime. Recent high-profile enforcement actions demonstrate what is possible when law enforcement and diplomats target individual attackers and point to a new way forward.

For example, in 2015, after a series of cyber espionage attacks on intellectual property in the US private sector, the Obama administration exerted diplomatic pressure on China. Under

the threat of sanctions, the Chinese government arrested individuals accused of commercial cyberespionage.[77] Experts believe the individuals arrested to have ties to the cyber offense unit of the People's Liberation Army (PLA).[78]

The US Government was able to investigate and indict twelve Russian GRU (Main Intelligence Directorate, abbreviated GRU) agents for hacking the Democratic National Committee and the Clinton Campaign during the 2016 election. The indictment detailed the methods and technologies used by the GRU to execute the hack. The investigators were also able to obtain the names of individuals responsible for executing, coordinating, and ordering the hack.[79] Even against the most sophisticated nation-state actors it is possible to identify and bring indictments against the individuals who launch the attacks.

In cyber policy circles, there are many who have argued that enforcement actions cannot have an impact when it comes to America's adversaries who use cyberattacks to target our country. But enforcement actions taken against malicious cyber actors even in the most difficult cases can still have a substantial impact. Deputy Attorney General Rod Rosenstein recently laid out the Department of Justice's view on this very issue, arguing that indictments and prosecutions are an important tool in these cases for a number of reasons, including: 1) the defendants may one day face a trial if there is a change in their government's calculus or they travel to another nation that cooperates with the United States in these efforts; 2) public indictments can provide some level of deterrence by raising the risk that these individuals will be held accountable, making them less attractive for future attacks; 3) these actions demonstrate the ability of US law enforcement to attribute attacks and charge hackers, which may deter others; 4) federal indictments in the US criminal justice system given its evidentiary standards are often taken seriously by other countries, which could impact their relationship with the offending countries; and 5) victims deserve justice for the attacks that were perpetrated against them.[80]

But it's not enough to just bring indictments leaving the hackers on the loose in foreign lands. The ultimate goal is to take them off the field completely, and law enforcement, enabled by diplomats, does that too.

It's time to rebalance cyber resources, beefing up the capacity of law enforcement and diplomats to focus on bringing to justice those people who are stealing Americans' hard-earned money, ideas, and personal data for nefarious purposes.

Unfortunately, American law enforcement and diplomatic efforts are severely under-resourced to address the growing cyber-crime wave. In fiscal year 2017, the Department of Defense spent $7.2 billion on cybersecurity broadly, nearly ten times the cybersecurity resources of the Department of Justice.[81]

As the recent CSIS report highlighted, America needs better cyber forensic capabilities and training.[82] These resources must be committed to:

- Forensics Training for Law Enforcement: In 2018, the National Computer Forensic Institute (the nation's only federally-funded training center dedicated to instructing state and local law enforcement officers, prosecutors, and judges in digital/cybercrime investigations) was only provided $18.9 million for its training efforts.[83] This 2018 funding level is only enough to train approximately 1,200

students even though the Institute has the capacity to train over 3,000 students annually if fully funded.[84] Yet some law enforcement officials are receiving just 12 hours of digital evidence training a year.[85]

- Technical Assistance for Local Law Enforcement: Even in the best of circumstances, not every officer in the country will be able to become an expert on digital evidence collection, so better forensic capabilities will require technical help for local law enforcement. For example, the New York County District Attorney's office only has 15 forensic specialists on staff to support 550 prosecutors handling over 100,000 cases annually.[86] State and local law enforcement rarely have the same level of technology available as the federal government. The costs of running a cybercrime division are simply too high for many local offices. New York City built a digital forensic lab in 2016 that cost $10 million— a price tag well beyond what most cities can spend.[87]
- Improve Crime Labs: Just 79 of the 409 publicly funded crime labs in the United States offered dedicated digital evidence support services according to a DOJ report.[88]

Without these resources, law enforcement officials cannot confront the new challenges posed by the cyber domain. In particular, digital evidence collection is a core component of most cyber investigations, yet federal, state, and local law enforcement have been hampered by their lack of training on such evidence collection and a lack of expert personnel that can be called upon to provide technical assistance in cyber investigations.[89]

It is time to rebalance these resources, beefing up the capacity of law enforcement and diplomats to focus on bringing to justice those people who are stealing Americans' hard-earned money, ideas, and personal data for nefarious purposes.

Recommendation #2: A Cyber Enforcement Cadre

In order to transform the government's enforcement efforts, we must be willing to address not only cybersecurity workforce shortages, but the way that workforce is trained, incentivized, and retained to hunt and catch cybercriminals.

There are 299,000 unfilled cybersecurity positions in the United States and the gap is expected to reach 1.8 million by 2022, according to a 2018 report authored jointly by the Department of Commerce and DHS.[90] The gap in unfilled cybersecurity positions covers both the private and public sector and vacancies range from information technology (IT) specialists to law enforcement cyber investigators. The large vacancy in positions affects the government and companies' ability to improve their cybersecurity and law enforcement's ability to go after cybercriminals. There is also a severe lack of diversity in this workforce, which could vastly improve the effectiveness of the workforce as a whole.[91]

The ways that law enforcement personnel are trained to be able to handle digital forensics of these crimes will need broad transformation.

One of the central issues the US government is confronting is recruiting capable cyber talent and this has had a direct impact on US enforcement agencies. A 2015 Department of Justice

Office of the Inspector General (OIG) report highlighted a need to increase pay for cybersecurity professionals, particularly those that serve in cyber investigation roles working within the National Cyber Investigation Joint Task Force, a multi-agency cyber coordinating entity within the federal government.[92] Additionally, the report notes challenges with the lengthy security clearance process, prohibiting the use of marijuana in the past 3 years, and prohibiting illegal drug use in the past 10 years, posing a challenge in recruiting a younger generation used to a more permissive environment.[93] Once recruited, there are challenges in retention and promotion that must be addressed. The recent departure of four senior FBI cyber officials on top of an additional 20 FBI cybersecurity officials in the past five years for high-paying corporate positions that can exceed $300,000 highlights the challenges of retaining senior talent in the face of lucrative private sector positions.[94]

There are also challenges with ensuring that law enforcement is properly trained to conduct cyber investigations. Preparing law enforcement personnel to handle cybersecurity cases will require increasing the technical capability of multiple specialties: detectives who investigate crime, specialized forensic technicians who analyze digital devices and signatures, and first responders who secure crime scenes.[95] A recent report by the Center for Strategic and International Studies (CSIS) surveyed law enforcement personnel and discovered that many don't know how to make basic requests to technology companies for data that they need to investigate crimes in general, not just computer-enabled crimes.[96] The ways that law enforcement personnel are trained to be able to handle digital forensics of these crimes will need broad transformation.

Recommendation #3: Better Attribution Efforts

Attribution, or identifying the origin and individuals responsible for a cyberattack, is difficult and time consuming, but not impossible.

It often requires teams of investigators comprised of forensic experts, law enforcement officials, and cybersecurity professionals.[97] Technologies like VPNs, the Tor network, and advanced encryption used by malicious cyber actors add to the difficulty by masking identifying information. Tools created using machine learning allow malicious actors to perform reconnaissance, or information-gathering efforts, efficiently and to a much higher degree of accuracy.[98] The solutions offered by law enforcement often raise serious civil liberties concerns and the issue remains a challenge for local, state, and federal officials, and the private sector—as was apparent in the Apple-FBI dispute regarding the San Bernardino case in 2016.[99]

Attribution often requires close cooperation between law enforcement and other government entities and victims of cyberattacks for evidence collection and sharing of threat intelligence. Law enforcement is unable to pursue cases against cybercriminals if victims of cyberattacks do not report these attacks and share evidence with the proper authorities. Intelligence agencies are also unable to collect and analyze cyber-threat intelligence if there is not an effective mechanism in place for information sharing from the private sector and government entities. While law enforcement and intelligence agencies do and should face restrictions on accessing data for attribution without due process, it is worth assessing whether the current systems and processes in place allow for the most effective and efficient sharing of cybercrime information between victims, particularly in the private sector, and government enforcement entities.

Because of a lack of physical evidence, cyber attribution has to deal in degrees of certainty rather than absolutes.[100] Most attribution reports from cybersecurity organizations will refrain from

making an outright accusation. Instead, they use subjective levels such as low, medium, or high confidence.[101] Translating this into evidence that a prosecutor could present in court in front of judge and jury can be an onerous task.[102]

However, considerable progress has been made on attribution in cyber investigations. The indictments against nation-state actors like China's PLA and Russia's GRU show that attribution is possible against even the most sophisticated actors.[103] The change in the attitude of cybersecurity experts to the US government attribution of the Sony attack to North Korea shows the evolution of attribution mechanisms in the last few years.[104]

Attribution made by or against a nation-state may require human sources or information obtained through technologies the victim government does not wish to reveal. In the investigation into Russian hacking during the 2016 presidential election, many individuals were critical of the initial DHS report for not containing enough information and were suspicious of the attribution made to Russia.[105] After the government disclosed more information regarding the hack and other offensive operations, most analysts and experts accepted that Russian actors hacked the Democratic National Committee (DNC).[106]

Further, given the international nature of many of these crimes, attribution by the United States will also have to be sufficiently credible to convince foreign partners to take action. Rising distrust of the United States in the global space, especially in areas related to intelligence, have heightened the need to be able to provide transparent and credible attribution for cyberattackers. Attributing attacks is the first stage in a process that allows for enforcement actions to be taken against malicious cyber actors, whether that be law enforcement action or sanctions. US diplomatic officials have taken a leading role in building up coalitions of countries that can coordinate on attribution issues, providing determinations on who perpetrated an attack that have more diplomatic might on the global stage than the United States standing alone.[107]

Progress has been made in this direction with US attribution efforts having been closely coordinated with partner nations on some recent cases. For example, this month, officials from the United States, United Kingdom, and the Netherlands released coordinated announcements attributing the targeting of the Organization for the Prevention of Chemical Weapon to the GRU.[108]

The Trump Administration's newly proposed Cyber Deterrence Initiative is a potential avenue for such a coalition.[109] But to ensure this Initiative is most effective, it must also address the issues that have impeded joint attribution in the past, including significant delays caused by bureaucratic processes and challenges in information sharing between the United States and partner countries. These joint attribution efforts will involve more than just collecting, analyzing, and sharing digital evidence. In the end, the decision by governments to publicly identify malicious cyber actors, particularly nation-state actors, will be a political decision by their leaders. If all of these international efforts are to be effective and coordinated, the State Department needs a senior-level person resourced and empowered to ensure that our diplomatic efforts are consistent with the goal of increasing our ability to identify, stop, and punish the attacker.

All of these challenges can begin to be met or at least mitigated by:

- More resources for technological advances in cyber investigations dedicated to enhancing cyber attribution efforts at federal and state levels. Systems and processes for cyber attribution are currently in their infancy when compared

to physical crime and often they are too costly for many states and localities to pursue on their own.

- The federal government advising system operators of the tools and best procedures to use when breached so they can gain the maximum forensic evidence.
- Building alliances, substantially improving information sharing processes and mechanisms between partner nations, and streamlining bureaucratic processes to improve the timeliness and impact of joint attribution efforts.

Recommendation #4: A Carrot and Stick Approach to Fugitives

In some cases, the criminals may be difficult to find or hiding in countries that provide them safe haven. The United States need not give up just because a criminal is beyond the arm of the law. It can reinvigorate enforcement tools used to impose consequences on cyber fugitives— both in offering rewards for their apprehension or imposing sanctions while they're at large.

A comprehensive strategy to deter and apprehend cybercriminals requires the use of a "carrot and stick" approach. The "carrot" could be the use of a reward-based system to incentivize the sharing of information that can lead to an arrest of malicious cyber actors. The "stick" is the use of targeted sanctions on cybercriminals and their possible nation-state or organizational sponsors.

The United States can reinvigorate enforcement tools used to impose consequences on cyber fugitives—both in offering rewards for their apprehension or imposing sanctions while they're at large.

Current "Most Wanted" programs can be expanded to incentivize the capture of cybercriminals. The FBI currently maintains what is known as the "Cyber's Most Wanted" list to raise public attention on cyber-fugitives and it should be evaluated if the use of rewards to incentivize information on cybercriminals can be expanded even further. As of September 2018, this list includes 42 malicious cyber actors from many different countries but additional individuals have been listed and then delisted once they have been captured.[110] The FBI also maintains a most wanted list for criminals involved in others types of crimes. The most well-known use of a criminals list is the FBI's "Ten Most Wanted Fugitives" list. The FBI has used a "Ten Most Wanted Fugitives" list for various crimes since the 1950s, and over the years over 519 fugitives have been on the list with the majority eventually being apprehended.[111] According to the FBI, "one hundred and sixty-two of the 'Ten Most Wanted Fugitive' apprehensions have been the result of citizen recognition of 'Ten Most Wanted Fugitive' publicity."[112] The lists are designed to help law enforcement garner public attention to apprehend criminals who otherwise might not receive attention and often tie rewards that are offered to the reporting of information that leads to arrest or apprehension.[113] The FBI in the past has applied the same incentive-based reporting approach to the "Cyber's Most Wanted" list with rewards for certain criminals being as high as $100,000.[114] However, there are currently very few cybercriminals listed that are tied to a reward. The rewards-based system for information on certain crimes has been an important tool in apprehending criminals and policymakers must evaluate whether incentives for information on cybercriminals can be expanded even further.

As we expand the use of incentives, we can also use punitive tools to impose consequences on cyber fugitives. Where the foreign nation is unwilling or unable to assist the United States in the prosecution of a cybercriminal, individual sanctions can be used by the US government to punish individuals responsible for malicious cyber-enabled activities who remain outside of the United States. The Department of Treasury can impose economic and financial sanctions. These may include such things as asset freezes and travel bans on individuals. The United States has many existing sanctions regimes, but the use of sanctions for cyber enforcement is a relatively recent development. [115]

The Department of Treasury Office of Foreign Asset Control's (OFAC) cyber-related sanctions program was instituted in April 2015 with President Obama's Executive Order 13694 to block the property and interests in property of persons who are responsible or complicit in malicious cyber-enabled activities.[116] These sanctions were expanded by President Obama in December 2016 and now allow for the sanctioning of individuals or entities whose activities either directly or indirectly present a "significant threat to the national security, foreign policy, or economic health or financial stability of the United States."[117]

Sanctions can also be issued against persons or organizations when we suspect a link to a nation-state sponsor. For example, the United States has a specific set of sanctions targeting cyber-enabled malicious activity and nation-state sanctions regimes such as those placed on North Korea and Iran.[118] In addition, the "Countering America's Adversaries Through Sanctions Act" was enacted in 2017 to authorize sanctions against any person who engaged in malicious cyber activity against a person or democratic institution on behalf of the Russian government.[119]

Key partner nations and multilateral organizations like the European Union and the United Nations have sanctions regimes that can be equally, or in some cases more, effective in punishing hard to reach malicious cyber actors and their nation-state sponsors.[120]

By revisiting a carrot and stick approach to apprehending cyber-fugitives as part of an overarching strategy, US enforcement agencies can begin to impose consequences even when the perpetrator is at large.

International cooperation and coordination reform

Recommendation #5: Ambassador-level Cyber Quarterback

Not only must law enforcement transform itself domestically, but it must also transform the ways it works across international borders. Since the early days of the internet, attempts to identify hackers have faced bureaucratic hurdles caused by the multiple jurisdictions involved, the most complex of which require international cooperation.[121] For many law enforcement agencies, the difficulties of getting international cooperation to trace or arrest a malicious actor are extremely daunting.[122]

The global nature of the cyber threat requires dedicated and deliberate leadership and coordination at the highest echelons of the US government to enhance international coordination and cooperation on closing the enforcement gap. Given the scope of countries that are impacted in a cybercrime investigation, little progress can be made in these efforts if America's cyber diplomacy and development efforts are not expanded and diplomatic ties to partner nations around the globe are not strengthened. To catch international cybercriminals, we'll need a

coordinated international effort, cooperation on building the case, and cooperation on bringing the criminals into custody.

Effective engagement with other countries on cyber threats requires a coordinated international effort as we make catching cybercriminals a top priority for the United States. To have an effective offense, we need a strong quarterback. Unfortunately, the State Department's cyber coordinator being downgraded under the Trump Administration leaves US international efforts without a leader.[123]

Effective engagement with other countries on cyber threats requires a coordinated international effort as we make catching cybercriminals a top priority for the United States. To have an effective offense, we need a strong quarterback.

Congressional efforts to raise the level of the State Department's Coordinator for Cyber Issues to a Senate-confirmed ambassador position are an important step in ensuring the United States has the leadership it needs to strengthen international cooperation and coordination.[124] The Office of the Coordinator for Cyber Issues has played an important role in enhancing the vital operational-level cooperation that occurs between US law enforcement and federal agencies, including the Departments of Homeland Security and Defense, and their foreign counterparts. But a Congressional authorization to elevate the Office of the Coordinator for Cyber Issues is not enough. The Office must also be provided with a clear mandate to include a focus on closing the enforcement gap in its work, including strengthening its efforts on attribution and diplomatic training programs, and the necessary resources and personnel by Congress to be able to do so. This is critical to drive forward a rebalance in America's cybersecurity approach to one that puts the State Department front and center as a key entity for progress.

America's diplomats are key to making a dent in international cybercrime and changing the malicious cyber behavior of nation states and non-state actors more broadly. To make progress, the United States cannot go at these missions alone. It must build a posse of like-minded countries that will complement and enhance our efforts. This means that strengthened international cooperation and alliance building to collectively respond to shared cyber threats, including those posed by nation states, must be a top priority for the US government. The United States must also work to strengthen its leadership in international organizations that deal with these issues, such as the UN, the Group of Seven (G7), NATO, and others, to play a leading role in decision-making and not work to weaken and attack these alliances as President Trump has done on a number of occasions.[125]

Recommendation #6: Stronger Tools in the Diplomacy Arsenal

To catch cybercriminals, we'll need international assistance in building the evidence against them. Bilateral agreements facilitate cooperation between the United States and other governments in cybercrime investigations.

Mutual legal assistance treaties (MLATs) and mutual legal assistance agreements (MLAAs) are one such tool to facilitate cooperation on cyber-enabled crime investigations and prosecutions. These binding treaties and agreements are typically bilaterally signed between the United States and other countries to formalize the parameters of their criminal justice cooperation.[126] These treaties can be critical tools for sharing data and digital evidence in cyber investigations

and prosecutions.[127] Right now the process under these agreements can be very lengthy and administratively burdensome. Congress has taken some action to try to help make this process more efficient. For example, they have worked to facilitate cross-border data sharing directly between US technology companies and foreign governments.[128] The recently enacted "CLOUD Act" allows the United States to enter into agreements with other countries to provide direct access to data held by technology companies while also raising the standards of civil liberties.[129] Congress must continue to perform its oversight function in evaluating the effectiveness of any "CLOUD Act" agreements and assessing whether any further legislative changes to these legal assistance processes are needed.

Treaties can be critical tools for sharing data and digital evidence in cyber investigations and prosecutions.

Once the United States has ultimately built cases against these cybercriminals, it will need help bringing them into custody. Once they have an arrest warrant, American authorities can ask INTERPOL, the global police cooperation body, to issue a Red Notice, which asks foreign authorities to locate and provisionally arrest an individual pending their extradition.[130] Once a Red Notice is issued for a cybercriminal, these persons are placed on lookout lists and, if they come to the attention of police in other countries the United States can request that they be provisionally arrested or file a request for extradition.[131] Extradition treaties allow US authorities to ask other countries to hand over an individual for prosecution or to serve a sentence following a conviction in American courts. The United States has signed extradition treaties with over 100 countries.[132]

Additionally, the United States should continue to utilize the Council of Europe's 2001 Convention on Cybercrime (also known as the Budapest Convention) to facilitate cooperation on cybercrime. This treaty was the first binding international treaty that sets common standards on investigations and criminal justice cooperation on cybercrime and electronic evidence. It remains the most wide-reaching cybercrime treaty there is and has now been ratified or acceded by the United States and 60 other countries.[133] Expanding the number of countries that ratify or accede to the Budapest Convention is critical to ensure it can have far-reaching impact because it can be a diplomatic tool to push member countries to uphold their obligations. However, if this treaty is to be most effective, it must not just be adopted by like-minded countries. This will require sustained US leadership in pushing countries who have previously opposed its provisions to come on board. Yet, even in countries that have ratified or acceded to the Convention, changes in national laws to comply with the treaty obligations and capacity building for criminal justice actors in the standards of the Convention remain big gaps in certain nations that need to be addressed. As one of the only binding agreements that exists globally on cybercrime, America's diplomats can work to expand the number of countries that ratify this treaty.

Underneath the frameworks established by international agreements, American authorities are able to take advantage of multilateral tools that exist to try to locate these actors overseas in specific cases and either prosecute them in the United States or the country they are apprehended in. However, these initiatives require resources, personnel, and political leadership from the United States to remain effective.

Recommendation #7: Better International Capacity for Enforcement

US law enforcement has a long way to go to make a dent in the cybercrime wave. But many other nations require far greater capacity building to be able to complement these US efforts.[134]

To strengthen the capability of partner nations, the US government must assess and expand its support to global cyber enforcement capacity building. It must help foreign authorities understand and address the threat as it transforms itself. Currently, the United States provides capacity building assistance on cybersecurity and cybercrime to countries through US diplomatic, development, and international judicial programs.[135] US enforcement agencies also have personnel and agents posted in key countries who help facilitate cooperation and support capacity-building efforts on cybersecurity and cybercrime.[136]

It is clear that the current levels of funding and manning for capacity building efforts are not adequate to meet the challenge. As the Trump Administration has continued to deprioritize America's diplomatic and development efforts, requesting to gut funding to critical global initiatives[137] and decimating the workforce;[138] Congress must push back and ensure adequate, and in some cases expanded, funding is provided to bilateral and multilateral cyber capacity building efforts. The United States cannot say it prioritizes cybercrime capacity building, as the new *National Cyber Strategy* proclaims, without ensuring the resources are provided to support this.[139]

However, the United States does not have to go at this capacity-building alone. There are capacity-building efforts being undertaken for criminal justice actors around the globe, many supported by the United States, by entities like the United Nations,[140] INTERPOL,[141] the Organization for Security and Co-operation in Europe,[142] and others in the private sector.

Capacity-building efforts are also an opportunity to strengthen international support for rule of law, privacy, civil liberties, and human rights.

These capacity-building efforts are also an opportunity to strengthen international support for rule of law, privacy, civil liberties, and human rights. As governments around the globe have strengthened their cybersecurity laws, these laws and strengthened cyber capabilities have been used as a tool in certain countries to crackdown on dissidents, opposition figures, and activists.[143] These laws may help to strengthen efforts to go after cyberattackers but, if used for nefarious reasons, they can be powerful tools to stifle dissent and restrict powerful forces needed for democratization and social change.[144] As the United States works to strengthen its international cooperation on cyber enforcement, this work must match with calls to respect privacy, civil liberties and human rights, and criticism for actions that do not do so.

Structural and process reform

Recommendation #8: Better Success Metrics

To begin to make improvements in the government's ability to bring enforcement actions against cybercriminals, there must be a comprehensive assessment of current government efforts across all agencies with a role in cyber enforcement to determine what is working, what might need to be amplified, and what might need to change. At a minimum, without baseline statistics it is difficult to measure government efforts, develop budget estimates for current levels of effort, and

make an informed case for budget increases necessary to support increased enforcement levels. This baseline does not currently exist.

It's difficult for outside researchers to assess the level of enforcement activity taken by the US government, as we discovered. But even the government's own analysis indicates there's no reliable measurement of the problem. In July 2016, the Department of Justice's Inspector General found that the process that the FBI uses to prioritize cyber threats was subjective and open to interpretation, and that the Bureau lacked a system that would allow it to determine whether cyber threats were appropriately prioritized.[145] Without accurate data on cybercrime, law enforcement cannot make reasoned policy decisions to best deal with the issue.[146] The Uniform Federal Crime Reporting Act of 1988 requires all federal agencies to report federal crime offenses to the FBI, yet there are agencies that have never reported crime data to the FBI.[147] The National Academies of Science has recommended a data collection framework modeled off of one utilized by United Nations entities that would provide reliable and comparative data on crime beyond what is currently available.[148] Better reporting measures would also assist in lowering the number of unreported crimes.[149]

Without accurate data on cybercrime, law enforcement cannot make reasoned policy decisions to best deal with the issue.

In addition to the lack of a process to determine prioritization of the cyber threat, the FBI lacks comprehensive performance metrics that set case targets for cyber fraud, a large and growing category of criminal activity.[150] The lack of comprehensive performance metrics stands in stark contrast to the targets set for white collar crime, mortgage fraud, and criminal enterprises and gangs.[151]

A baseline assessment on the government's cyber enforcement efforts will allow for the eventual setting of targets for agency performance on a number of different metrics. For example, the US Secret Service (USSS) sets targets for each year, reported to Congress, on a number of cyber-related measures. This includes the amount of dollar-loss prevented by Secret Service cyber investigations as well as the number of law enforcement officials trained in cybercrime and cyber forensics. In fiscal year 2017 alone, the USSS set a target to prevent $600 million in the public financial loss that was prevented due to the agency's cyber investigations. It far exceeded that target.[152] However, these targets do not appear to include targets set for arrests and prosecutions and nor do the targets set by other enforcement agencies.[153] Assessing the government's efforts now on cyber enforcement will allow for the setting of targets on enforcement actions taken moving forward.

Recommendation #9: Organizational Changes and Interagency Cooperation

Cybercrime remains pervasive and the US government's enforcement efforts to counter this threat must be made as efficient and effective as possible. This must include necessary reforms to de-conflict the often overlapping mandates of the numerous US government agencies involved in enforcement. The many federal agencies with special agents that all have a role in cyber investigations and the number of state and local law enforcement agencies also leading investigations has led to similar or overlapping responsibilities between these entities. At the federal level in particular, this can lead to inefficiencies, redundancies, and difficulties in

ensuring congressional oversight efforts are tied to an overarching strategic cyber enforcement approach across agencies. [154]

Efforts have been undertaken already to enhance coordination between these various agencies. For example, the National Cyber Investigative Joint Task Force (NCIJTF) was established in 2008 to serve as focal point for government coordination and information sharing on cyber investigations. The FBI-led NCIJTF serves as the national focal point for coordinating cyber threat investigations and allows for information sharing across over 20 member agency representatives from law enforcement, the intelligence community, and the military.[155] FBI also leads state and local task forces out of its field offices to coordinate domestic cyber threat investigations at the state and local level.[156] In addition, the USSS coordinates a network of Electronic Crimes Task Forces to strengthen its efforts to prevent, detect, and investigate various types of electronic crimes.[157]

However, even with the creation of these task forces, there's continued confusion on which agency has the lead to investigate certain types of cybercrime. A 2015 congressional report found that the similar or overlapping missions of enforcement agencies has continued to cause confusion on which agency has the lead on investigating certain crimes, particularly when multiple agencies are involved in an investigation. This also creates confusion among the American people on what agency they should even report to if they become victim of a cybercrime.[158]

Reforms need to focus on de-conflicting the missions of the agencies responsible for cyber enforcement, focusing on streamlining efforts, reducing duplication, and clarifying jurisdiction. Without these reforms, issues will remain on how to accurately assess the progress of each of these agencies and link that progress to an overarching strategic approach tied to resources and personnel. To ensure these investigations are as efficient and effective as possible, investigators working on complicated and multi-jurisdictional cybercrimes need clarity on which agency is taking the lead on coordinating the effort.

Recommendation #10: Centralized Strategic Planning

All of these areas of focus must be supported by an overarching, comprehensive strategy for US cyber enforcement aimed at identifying, stopping, and punishing global cyberattackers. That overarching strategy must include a plan to transform the interagency cooperation on cyber enforcement, both domestically and internationally. No single agency can tackle this behemoth of a challenge alone. A comprehensive domestic strategy would require unparalleled cooperation between the myriad federal agencies that have a role in cyber investigations.

A recent assessment by the non-partisan Government Accountability Office (GAO) underscores that the government still lacks a comprehensive cybersecurity strategy that allows for effective oversight.[159]

And the Trump Administration's recently released *National Cyber Strategy* does not meet the benchmarks for an effective strategic approach that allows for proper oversight.[160] This document does contain priorities for strengthening cyber enforcement and is an important first step. However, there remains little detail, at least publicly available, as to how federal, state, and local agencies plan to implement it. This document echoes some of the concerns expressed by the 9/11 Commission in its critical assessment of the US counterterrorism strategic approach before these catastrophic terrorist attacks.[161] The Commission noted that while the US government cannot promise that a terrorist attack will never happen on American soil again "the American people

are entitled to expect that officials will have realistic objectives, clear guidance, and effective organization. They are entitled to see standards for performance so they can judge, with the help of their elected representatives, whether objectives are being met."[162] In order to achieve the necessary transformation, we will have to develop these standards and benchmarks.

The US government needs a position to oversee and coordinate a national cyber strategy to ensure that there is proper attention and resources dedicated for this pervasive national crisis, benchmarks for progress are tracked and evaluated, and there is clarity in mission of different agencies to avoid duplication.

A strategy will be most effective when there is White House leadership managing and coordinating a whole-of-government response. When the country has faced tremendous threats in the past, "czar" positions were created within the executive branch to mobilize and coordinate resources, streamline processes, and work to coordinate the efforts of the numerous government agencies involved.[163] Most recently, the Obama Administration created the position of Ebola response coordinator, known as the Ebola Czar, to coordinate the federal government's ability to combat Ebola.[164] Similarly, the US government needs a position to oversee and coordinate a national cyber strategy to ensure that there is proper attention and resources dedicated for this pervasive national crisis, benchmarks for progress are tracked and evaluated, and there is clarity in mission of different agencies to avoid duplication.

The Trump administration has taken the opposite approach. The Trump White House has actually scaled back cybersecurity coordination not strengthened it,[165] eliminating the White House Cyber Coordinator position within the National Security Council (NSC) and leaving coordination to two senior director-level NSC officials.[166] NSC officials often operate with little resources and support personnel. In comparison, the operating budget of the Office for National Drug Control Policy, the office of the Drug Czar, in fiscal year 2018 alone was $18.4 million for operating costs,[167] which has been even higher in years past.[168] The county is facing a national cybersecurity crisis and there is no senior official empowered with the resources to coordinate a comprehensive cyber strategy that includes a significant focus on closing the cyber enforcement gap.

What are the federal agencies involved in cyber enforcement?

Many federal agencies have a role in cyber investigations, including the FBI, the Secret Service (USSS), the Immigration and Customs Enforcement's Homeland Security Investigations (HSI), and others.[169] State and local law enforcement agencies also lead on many cybercrime investigations. While each of these agencies has a vital role in cyber enforcement, there are also some similar or overlapping responsibilities between them. At the federal level in particular, this can lead to inefficiencies, redundancies, and difficulties in ensuring congressional oversight efforts are tied to an overarching strategic cyber enforcement approach across agencies.[170]

The descriptions provided by the Secret Service, Homeland Security Investigations, and the FBI concerning the scope of their mandate on cybercrime demonstrates the lack of clarity in their investigation jurisdictions:

USSS: "Cybercrime, including computer intrusions or attacks, transmissions of malicious code, password trafficking, or theft of payment card of other financial payment information."[171]

HSI: "Cyber-based domestic or international cross-border crime, including child exploitation, money laundering, smuggling, and violations of intellectual property rights."[172]

FBI: "Cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity."[173]

Conclusion

Before 9/11 the US government lacked a strategic approach to the threat of terrorism. While the 9/11 Commission documented enormous efforts that were undertaken by the US government to detect and disrupt the terrorist threat, it also found tremendous barriers to progress, including a lack of prioritization of the threat, competing priorities and immense bureaucratic challenges.[174] Some of the challenges they found also stymie a strategic approach to cybersecurity. They noted that a comprehensive approach to counterterrorism was limited by: law enforcement priorities guided by local FBI field offices as opposed to by an overarching national approach;[175] a lack of a significant shift in resources at the FBI to meet the threat;[176] insufficient training for law enforcement;[177] the minimization of the important diplomatic role of the State Department;[178] and the failure of Congress to adjust itself to address the rise of the transnational terrorism threat and conduct proper oversight.[179] The state of the US government's cybersecurity efforts today draw alarming parallels to these pre-9/11 challenges.

To transform the US government's ability to improve its ability to identify, stop, and punish the attacker, we will need a strategy that doesn't just focus on building a better safe, but focuses on catching the safe-cracker.

We have enough examples of successful prosecutions to know that while finding and punishing the attacker is hard, it's not impossible. Today, we lay the cornerstone of that foundation, and dedicate ourselves to building a more complete cyber enforcement architecture.

ENDNOTES

1 Chuang, Tamara. "Pay Us Bitcoin or Never See Your Files Again: Inside the Highly Profitable Underworld of Ransomware." The Denver Post, The Denver Post, 8 Mar. 2018, www.denverpost.com/2018/03/04/computer-ransomware/. Accessed 19 Oct. 2018.

2 Chuang, Tamara, and David Migoya. "SamSam Virus Demands Bitcoin from CDOT, State Shuts down 2,000 Computers." The Denver Post, The Denver Post, 22 Feb. 2018, www.denverpost.com/2018/02/21/samsam-virus-ransomware-cdot/. Accessed 19 Oct. 2018.

3 Colorado Department of Transportation. "CDOT Cyber Incident After-Action Report." 17 July 17, 2018, pp 3. https://www.colorado.gov/pacific/dhsem/atom/129636. Accessed 3 Oct. 2018.

4 Chuang, Tamara. "Ransomware Strikes CDOT for Second Time Even as Agency Still Recovering from First SamSam Attack." The Denver Post, The Denver Post, 2 Mar. 2018, www.denverpost.com/2018/03/01/cdot-samsam-ransomware-attack/. Accessed 19 Oct. 2018.

5 Kearney, Laila. "Atlanta Officials Reveal Worsening Effects of Cyber Attack." Reuters, Thomson Reuters, 6 June 2018, www.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-idUSKCN1J231M. Accessed 19 Oct. 2018

6 Quinn, Samm. "Hospital Pays $55,000 Ransom; No Patient Data Stolen." Daily Reporter, Daily Reporter, 16 Jan. 2018, www.greenfieldreporter.com/2018/01/16/01162018dr_hancock_health_pays_ransom/. Accessed 19 Oct. 2018.

7 Sophos. "SamSam : The (Almost) Six Million Dollar Ransomware." 19 July 2018, pp. 8. https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf. Accessed 19 Oct. 2018.

8 Deere, Stephen. "CONFIDENTIAL REPORT: Atlanta's Cyber Attack Could Cost Taxpayers $17 Million." Ajc, The Atlanta Journal-Constitution, 2 Aug. 2018, www.ajc.com/news/confidential-report-atlanta-cyber-attack-could-hit-million/GAljmndAF3EQdVWlMcXS0K/. Accessed 19 Oct. 2018.

9 This number includes 2016 incidents that involved a systemic or targeted breach of a system and does not include privacy crimes, online harassment, or crimes against children. See: Federal Bureau of Investigation. "2016 Internet Crime Report." 22 June 2017, pp. 17. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 3 Oct. 2018. The authors welcome a robust discussion on how these metrics could be improved and have made recommendations for the same in this report.

10 Newman, Craig A. "When to Report a Cyberattack? For Companies, That's Still a Dilemma." The New York Times, The New York Times, 5 Mar. 2018, www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html. Accessed 19 Oct. 2018.

11 "CEA Report: The Cost of Malicious Cyber Activity to the U.S. Economy." The White House, The United States Government, 16 Feb. 2018, www.whitehouse.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/. Accessed 19 Oct. 2018.

12 "Clearances." FBI, Federal Bureau of Investigation, 25 Aug. 2017, ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/topic-pages/clearances. Accessed 19 Oct. 2018.

13 Office of Financial Research. "2017 Annual Report to Congress." 29 Sept. 2017, pp. 6. https://www.financialresearch.gov/annual-reports/files/office-of-financial-research-annual-report-2017.pdf. Accessed Oct. 3, 2018.

14 Cisco. "VNI Complete Forecast Highlights Global Internet Users: % of Population Devices and Connections per Capita Average Speeds Average Traffic per Capita per Month Global -Device Growth Traffic Profiles 2021 Forecast," 2016, pp. 6–7..https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Global_Device_Growth_Traffic_Profiles.pdf. Accessed 21 Oct. 2018.

15 Federal Bureau of Investigation. "2016 Internet Crime Report." 22 June 2017, pp. 14. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 3 Oct. 2018.

16 This number includes incidents that involve a systemic or targeted breach of a system and does not include privacy crimes, online harassment, or crimes against children. See: Federal Bureau of Investigation. "2016 Internet Crime Report." 22 June 2017, pp. 2. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 3 Oct. 2018.

17 Federal Bureau of Investigation. "2016 Internet Crime Report." 22 June 2017, pp. 17. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 3 Oct. 2018.

18 Federal Bureau of Investigation. "2017 Crime in the United States," 2017. https://ucr.fbi.gov/crime-in-the-u.s/2017/crime-in-the-u.s.-2017/topic-pages/burglary. Accessed 24 Sept. 2018.

19 Federal Bureau of Investigation. "Filing a Complaint with the IC3." https://www.ic3.gov/about/default.aspx. Accessed 3 Oct. 2018.

20 Federal Bureau of Investigation. "2017 Internet Crime Report." 7 May 2018, pp. 4. https://pdf.ic3.gov/2017_IC3Report.pdf. Accessed 3 Oct. 2018.

21 Verizon. "2018 Data Breach Investigations Report (DBIR)." Verizon Bus. J., 10 April 2018, pp. 4. https://www.verizonenterprise.com/verizon-insights-lab/dbir/. Accessed 9 Oct. 2018.

22 INTERPOL. "Crime Areas | Cybercrime." INTERPOL, 2018. https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime. Accessed 9 Oct. 2018

23 United States Department of Justice, Office of Legal Education, "Prosecuting Computer Crimes," 1 Jan. 2015, pp. V. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf. Accessed 3 Oct. 2018.

24 Wolff, Josephine. "Why We Need to Be Much More Careful About How We Use the Word Cyberattack." Slate Magazine, Slate Magazine, 30 Mar. 2017, www.slate.com/blogs/future_tense/2017/03/30/we_should_be_careful_when_we_use_the_word_cyberattack.html. Accessed 9 Oct. 2018.

25 Federal Bureau of Investigation, "WHAT WE INVESTIGATE; Cyber Crime." https://www.fbi.gov/investigate/cyber. Accessed 3 Oct. 2018.

26 Wray, Christopher. "Statement Before the Senate Homeland Security and Government Affairs Committee," 27 Sept. 2017. https://www.fbi.gov/news/testimony/current-threats-to-the-homeland. Accessed 3 Oct. 2018.

27 United States Department of Justice, "Report of the Attorney General's Cyber Digital Task Force." 2 July 2018, pp. 31. https://www.justice.gov/ag/page/file/1076696/download. Accessed 3 Oct. 2018.

28 Ellis, Emma Grey. "Doxing Is a Perilous Form of Justice-Even When It's Outing Nazis." Wired, Conde Nast, 18 Aug. 2017, www.wired.com/story/doxing-charlottesville/. Accessed 21 Oct. 2018.

29 Sanger, David E., and Katie Benner. "U.S. Accuses North Korea of Plot to Hurt Economy as Spy Is Charged in Sony Hack." The New York Times, The New York Times, 6 Sept. 2018, www.nytimes.com/2018/09/06/us/politics/north-korea-sony-hack-wannacry-indictment.html. Accessed 3 Oct. 2018.

30 Coats, Daniel R. "WORLDWIDE THREAT ASSESSMENT of the US INTELLIGENCE COMMUNITY." Office of the Director of National Intelligence, Office of the Director of National Intelligence,13 Feb. 2018, www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf. Accessed 21 Oct. 2018.

31 United States Department of Justice. "Report of the Attorney General's Cyber Digital Task Force." July 2, 2018, pp. 32-33. https://www.justice.gov/ag/page/file/1076696/download. Accessed 3 Oct. 2018.

32 Accenture. "2017 Cost of Cyber Crime Study." 26 Sept. 2017, pp. 23. https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017. Accessed 3 Oct. 2018.

33 Symantec. "2018 Internet Security Threat Report." 20 March 2018. https://www.symantec.com/security-center/threat-report. Accessed 3 Oct. 2018.

34 Symantec. "2018 Internet Security Threat Report." 20 March 2018. https://www.symantec.com/security-center/threat-report. Accessed 3 Oct. 2018.

35 Ponemon Institute LLC. "2017 Cost of Data Breach Study, Global Overview." IBM, June 2017, pp. 1. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN. Accessed 3 Oct. 2018.

36 Federal Bureau of Investigation. "2017 Internet Crime Report." 7 May 2018, pp. 17. https://pdf.ic3.gov/2017_IC3Report.pdf. Accessed 3 Oct 2018.

37 United States White House, The Council of Economic Advisers. "The Cost of Malicious Cyber Activity to the U.S. Economy." February 2018, pp. 1. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf. Accessed 3 Oct 2018.

38 Sterling, Bruce. "Global Cybercrime. Costs a Trillion Dollars. Maybe 3." Wired, Conde Nast, 19 July 2017, www.wired.com/beyond-the-beyond/2017/07/global-cybercrime-costs-trillion-dollars-maybe-3/. Accessed 3 Oct. 2018.

39 Verizon. "2018 Data Breach Investigations Report (DBIR)." Verizon Bus. J., 10 April 2018, pp. 25. https://www.verizonenterprise.com/verizon-insights-lab/dbir/. Accessed 9 Oct. 2018.

40 Thielman, Sam, and Chris Johnston. "Major Cyber Attack Disrupts Internet Service across Europe and US." The Guardian, Guardian News and Media, 21 Oct. 2016, www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service. Accessed 3 Oct. 2018.

41 Wexler, Chuck. "New National Commitment Required: The Changing Nature of Crime and Criminal Investigations." Police Executive Research Forum, January 2018, pp. 4. https://www.policeforum.org/assets/ChangingNatureofCrime.pdf. Accessed 3 Oct. 2018.

42 Tor is a special kind of web browser commonly used to access the dark web designed for user anonymity. Inc. "Tor." Tor Browser. www.torproject.org/projects/torbrowser.html.en. Accessed 22 Oct. 2018.

43 The dark web is content on the Internet that requires special anonymizing software to access. Websites may additionally require specific authorization from administrators and are commonly used by individuals who seek privacy for a variety of reasons. Eddy, Max. "Inside the Dark Web." PCMAG, PCMAG, 4 Feb. 2015, www.pcmag.com/article2/0,2817,2476003,00.asp. Accessed 22 Oct. 2018.

44 Federal Bureau of Investigation. "2017 Internet Crime Report." 7 May 2018, pp. 19. Accessed Oct. 3, 2018. https://pdf.ic3.gov/2017_IC3Report.pdf. Accessed 3 Oct. 2018.

45 Federal Bureau of Investigation. "2017 Internet Crime Report." 7 May 2018, pp. 19. Accessed Oct. 3, 2018. https://pdf.ic3.gov/2017_IC3Report.pdf. Accessed 3 Oct. 2018.

46 Berr, Jonathan. "'WannaCry' Ransomware Attack Losses Could Reach $4 Billion." CBS News, CBS Interactive, 16 May 2017, www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/. Accessed 3 Oct. 2018.

47 United States Department of Homeland Security. "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." 15 March 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A. Accessed Oct. 3 2018.

48 Verizon. "Data breach digest." pp 39.http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf. Accessed 10 Oct. 2018.

49 Nakashima, Ellen, and Paul Sonne. "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare." The Washington Post, WP Company, 8 June 2018, www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?utm_term=.49f1d1da664. Accessed 9 Oct. 2018.

50 The Commission on the Theft of American Intellectual Property. "The Report of the Commission on the Theft of American Intellectual Property." The National Bureau of Asian Research, Feb. 2017, pp.1 http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf. Accessed 10 Oct. 2018.

51 Nakashima, Ellen. "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say." The Washington Post, WP Company, 9 July 2015, www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/. Accessed 22 Oct. 2018.

52 Mazzetti, Mark, and Katie Benner. "12 Russian Agents Indicted in Mueller Investigation." The New York Times, The New York Times, 13 July 2018, www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html. Accessed 9 Oct. 2018.

53 The enforcement rate was calculated using 2016 IC3 data instead of the most recent for 2017 due to the fact that is the most recent year of reported UCR statistics. Federal Bureau of Investigation. "2016 Internet Crime Report." 22 June 2017. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 3 Oct. 2018.

54 Federal Bureau of Investigation. "2015 Crime in the United States: federal Crime Data." 26 Sept. 2016. https://ucr.fbi.gov/crime-in-the-u.s/2015/crime-in-the-u.s.-2015/additional-reports/federal-crime-data/federal_crime_data_-2015. Accessed 3 Oct. 2018; Federal Bureau of Investigation. "2014 Crime in the United States: Federal Crime Data, 2014." 28 Sept. 2015. https://ucr.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2014/crime-in-the-u.s.-2014/additional-reports/federal-crime-data/federal-crime-data.pdf. Accessed 3 Oct. 2018.

55 "2016 NIBRS Crime data Released." Federal Bureau of Investigation, 11 Dec. 2017. https://www.fbi.gov/news/stories/2016-nibrs-data-released. Accessed 3 Oct. 2018.

56 United States Secret Service. "Presidential Campaign 2016 Annual Report." pp. 14. https://www.secretservice.gov/data/press/reports/USSS_FY2016AR.pdf. Accessed 10 Oct. 2018.

57 Federal Bureau of Investigation. "2016 Internet Crime Report."22 June 2017, pp. 2. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed Oct. 3, 2018

58 Baker, Al. "An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported." The New York Times, The New York Times, 5 Feb. 2018, www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html. Accessed 10 Oct. 2018; Wexler, Chuck. "New National Commitment Required: The Changing Nature of Crime and Criminal Investigations." Police Executive Research Forum, Jan. 2018. https://www.policeforum.org/assets/ChangingNatureofCrime.pdf Accessed Oct. 3, 2018.

59 Federal Bureau of Investigation. "FY 2018 Authorization and Budget Request to Congress." May 2017, pp 4-31. https://www.justice.gov/file/968931/download. Accessed 5 Oct. 2018.

60 Federal Bureau of Investigation. "FY 2018 Authorization and Budget Request to Congress." May 2017, pp 4-31. https://www.justice.gov/file/968931/download. Accessed 5 Oct. 2018.

61 Sulemeyer, Michael. "Why the U.S. Should witch from Cyber-Deterrence to Playing Cyber-Offense." Foreign Affairs, 22 March 2018. https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense. Accessed 5 Oct. 2018.

62 Baker, Stewart, and Victoria Muth. "Should Companies Risk Going on the Cyber Offensive?" Brink – The Edge of Risk, Marsh & McLennan Companies' Global Risk Center, 22 July 2016, www.brinknews.com/should-companies-risk-going-on-the-cyber-offensive/. Accessed 5 Oct. 2018.

63 National Academies of Sciences. "Modernizing Crime Statistics: Report 1: Defining and Classifying Crime." The National Academies Press, 16 May 2016. doi.org/10.17226/23492. Accessed 22 Oct. 2018.

64 Mazzetti, Mark, and Katie Benner. "12 Russian Agents Indicted in Mueller Investigation." The New York Times, The New York Times, 13 July 2018, www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html. Accessed 5 Oct. 2018; Starks, Tim. "U.S. Indicts North Korean National for Sony Hack, Massive Cyberattacks." POLITICO, POLITCO Magazine, 6 Sept. 2018, www.politico.com/story/2018/09/06/justice-department-north-korea-sony-hack-771212. Accessed 5 Oct. 2018.

65 Healey, Jason. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks." The Atlantic Council, pp. 2-4. January 2012. https://www.fbiic.gov/public/2012/mar/National_Responsibility_for_CyberAttacks,_2012.pdf. Accessed 10 Oct. 2018.

66 Mathews, Lee. "Equifax Data Breach Impacts 143 Million Americans," Forbes Magazine, 7 Sept. 2017. https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#6f153672356f. Accessed 9 Oct. 2018.

67 Nakashima, Ellen. "White House Declassifies Outline of Cybersecurity Program." The Washington Post, WP Company, 3 Mar. 2010. www.washingtonpost.com/wpdyn/content/article/2010/03/02/AR2010030202113.html. Accessed 5 Oct. 2018.

68 United States White House. "The Comprehensive National Cybersecurity Initiative." 15 July 2015. https://web.archive.org/web/20100715223803/www.whitehouse.gov/sites/default/files/Cybersecurity.pdf. Accessed 5 Oct. 2018.

69 United States White House. "The Comprehensive National Cybersecurity Initiative." 15 July 2015. https://web.archive.org/web/20100715223803/www.whitehouse.gov/sites/default/files/Cybersecurity.pdf. Accessed 5 Oct. 2018.

70 United States White House, National Security Council. "President Trump Unveils America's First Cybersecurity Strategy in 15 Years." 20 Sept. 2018. https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/. Accessed Oct. 9, 2018.

71 Maclellan, Stephanie, and Naomi O'Leary. "Doing Battle in Cyberspace: How an Attack on Estonia Changed the Rules of the Game." Centre for International Governance Innovation, Centre for International Governance Innovation , 26 Oct. 2017, www.cigionline.org/articles/doing-battle-cyberspace-how-attack-estonia-changed-rules-game. Accessed 27 Oct. 2018; United States, Congress, House, Armed Services Committee. "Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities." Government Printing Office, 1 March 2017. 115th Congress, 1th session, House Report [115-8]. https://www.gpo.gov/fdsys/pkg/CHRG-115hhrg24680/pdf/CHRG-115hhrg24680.pdf. Accessed 9 Oct. 2018.

72 NATO Cooperation Cyber Defence Center of Excellence. "Tallinn Manual Process." https://ccdcoe.org/tallinn-manual.html. Accessed 10 Oct. 2018.

73 Smith, Brad. "The need for a Digital Geneva Convention," RSA Conference, San Francisco, CA, 14 Feb. 2017. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/. Accessed 10 Oct. 2018.

74 United States White House. "Statement by President Donald J. Trump on the Elevation of Cyber Command." 18 Aug. 2017. https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/. Accessed Oct. 9, 2018.

75 Pomerleau, Mark. "CYBERCOM elevation at heart of budget increase." Defense News, 24 May 2017. https://www.defensenews.com/2017/05/24/cybercom-elevation-at-heart-of-budget-increase/. Accessed 9 Oct. 2018.

76 Volz, Dustin. "Trump, Seeking to Relax Rules on U.S. cyberattacks, Reverses Obama Directive." The Wall Street Journal, 15 Aug. 2018. https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721. Accessed 9 Oct. 2018.

77 Nakashima, Ellen, and Adam Goldman. "In a First, Chinese Hackers Are Arrested at the Behest of the U.S. Government." The Washington Post, WP Company, 9 Oct. 2015. www.washingtonpost.com/world/national-security/in-a-first-chinese-hackers-are-arrested-at-the-behest-of-the-us-government/2015/10/09/0a7b0e46-6778-11e5-8325-a42b5a459b1e_story.html?postshare=9811444395972124&utm_term=.dfca74bada27. Accessed 9 Oct. 2018.

78 Leyden, John. "China Cuffs Hackers at US Request to Stave off Sanctions." The Register® - Biting the Hand That Feeds IT, The Register, 9 Oct. 2015, www.theregister.co.uk/2015/10/09/china_cuffs_hackers_at_us_request/. Accessed 9 Oct. 2018.

79 United States District Court for the District of Columbia. "United States of America v. Viktor Borisovich Netykscho Et Al." New York Times, 13 July 2018, int.nyt.com/data/documenthelper/80-netyksho-et-al-indictment/ba0521c1eef869deecbe/optimized/full.pdf?action=click&module=Intentional&pgtype=Article. Accessed 22 Oct. 2018.

80 Deputy Attorney General Rod J. Rosenstein. "Remarks at the Aspen Security Forum," Aspect Security Forum. "19 July 2018. https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-aspen-security-forum. Accessed 9 Oct. 2018.

81 "Federal Budget Cyber Security Spending." White House, 2016. https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf. Accessed 9 Oct. 2018.

82 Carter, William A. and Jennifer C. Daskal. "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge." Center for Strategic & International Studies, July 2018. https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge. Accessed Oct. 9, 2018.

83 Carter, William A. and Jennifer C. Daskal. "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge." Center for Strategic & International Studies, July 2018, pp. 5. https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge. Accessed Oct. 9, 2018; United States Secret Service. "2017 Annual Report." 2017, pp. 21. https://www.secretservice.gov/data/press/reports/CMR-2017_Annual_Report_online.pdf. Accessed 9 Oct. 2018.

84 Carter, William A. and Jennifer C. Daskal. "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge." Center for Strategic & International Studies, July 2018, pp. 5. https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge. Accessed Oct. 9, 2018.

85 Carter, William A. and Jennifer C. Daskal. "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge." Center for Strategic & International Studies, July 2018, pp. 14. https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge. Accessed Oct. 9, 2018.

86 Carter, William A. and Jennifer C. Daskal. "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge." Center for Strategic & International Studies, July 2018, pp. 9. https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge. Accessed Oct. 9, 2018.

87 Taylor, Michelle. "New York City Opens its $10 Million Cybercrime Lab." Forensic Magazine, 17 Nov. 2016. https://www.forensicmag.com/news/2016/11/new-york-city-opens-its-10-million-cybercrime-lab. Accessed 10 Oct. 2018.

88 Carter, William A. and Jennifer C. Daskal. "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge." Center for Strategic & International Studies, July 2018, pp. 12. https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge. Accessed 9 Oct. 2018.

89 Digital evidence is "information stored or transmitted in binary form that may be relied on in court." It can be found on such things as a computer hard drive or a mobile phone and is used to prosecute a wide spectrum of crimes. United States Department of Justice, Office of Justice Programs. "Digital Evidence and Forensic." National Institute of Justice, 14 April 2016. https://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx. Accessed 9 Oct. 2018.

90 Secretary of Commerce Wilbur Ross and Acting Secretary of Homeland Security Elaine Duke. "A Report to the President on Supporting the Growth and Sustainment of the nation's Cybersecurity Workforce: Building the foundation for a More Secure American Future." 30 May 2018, pp. 1. https://www.dhs.gov/sites/default/files/publications/eo_wf_report_to_potus.pd_.pdf. Accessed 9 Oct. 2018.

91 Hurley, Deborah. "Improving Cybersecurity: The Diversity Imperative." Forbes. Forbes Magazine, 7 May 2017. https://www.forbes.com/sites/ciocentral/2017/05/07/improving-cybersecurity-the-diversity-imperative/#1fb6a9011e30. Accessed 19 Oct. 2018.

92 United States Department of Justice, Office of the Inspector General. "Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative." July 2015, pp. ii. https://oig.justice.gov/reports/2015/a1529.pdf. Accessed 9 Oct. 2018.

93 United States Department of Justice, Office of the Inspector General. "Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative." July 2015, pp. 8. https://oig.justice.gov/reports/2015/a1529.pdf. Accessed 9 Oct. 2018.

94 Geller, Eric. "FBI Struggles to Retain Top Cyber Talent." POLITICO, POLITICO Magazine, 3 Aug. 2018, www.politico.com/story/2018/08/03/fbi-cyber-security-talent-drain-hacking-threat-russia-elections-760740. Accessed 10 Oct. 2018.

95 Wexler, Chuck. "New National Commitment Required: The Changing Nature of Crime And Criminal Investigations." Police Executive Research Forum, January 2018, pp. 59. https://www.policeforum.org/assets/ChangingNatureofCrime.pdf. Accessed 9 Oct. 2018.

96 Carter, William A. and Jennifer C. Daskal. "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge." Center for Strategic & International Studies, July 2018, pp.4. https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge. Accessed 9 Oct. 2018.

97 Berghel, Hal. "On the Problem of (Cyber) Attribution." Computer, vol. 62, no. 47, 2017, pp. 84–89. https://ieeexplore.ieee.org/document/7888425. Accessed 22 Oct. 2018.

98 "Machine Learning: Practical Applications for Cybersecurity." Recorded Future, 14 Mar. 2018, www.recordedfuture.com/machine-learning-cybersecurity-applications/. Accessed 22 Oct. 2018.

99 Zetter, Kim. "Apple's FBI Battle Is Complicated. Here's What's Really Going On." Wired, Conde Nast, 3 June 2017, www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/. Accessed 19 Oct. 2018.

100 Newman, Lily Hay. "Why Is It So Hard to Prove Russia Hacked the DNC?" Wired, Conde Nast, 3 June 2017, www.wired.com/2016/12/hacker-lexicon-attribution-problem/. Accessed 19 Oct. 2018.

101 Wheeler, David A., and Gregory N. Larsen. "Techniques for Cyber Attack Attribution." Institute for Defense Analysis, Jan. 2003, pp 2, doi.org/10.21236/ada468859. Accessed 19 Oct. 2018.

102 Tran, Delbert. "The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack." Yale Journal of Law & Technology, vol. 20, no. 376, May 10 2017, pp. 3–4., www.yjolt.org/sites/default/files/20__yale__j.__l.__tech.__376.pdf. Accessed 19 Oct. 2018.

103 "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." The United States Department of Justice, 22 July 2015, www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor. Accessed 19 Oct. 2018; "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations." The United States Department of Justice, 4 Oct. 2018, www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and. Accessed 19 Oct. 2018.

104 Collier, Kevin. "The Indictment Of North Korea For The Sony Hack Shows How Cybersecurity Has Evolved." BuzzFeed News, BuzzFeed, 10 Sept. 2018, www.buzzfeednews.com/amphtml/kevincollier/the-indictment-of-north-korea-for-the-sony-hack-shows-how. Accessed 19 Oct. 2018.

105 Biddle, Sam. "Here's the Public Evidence Russia Hacked the DNC - It's Not Enough." The Intercept, 14 Dec. 2016, www.theintercept.com/2016/12/14/heres-the-public-evidence-russia-hacked-the-dnc-its-not-enough/. Accessed 19 Oct. 2018.

106 Apuzzo, Matt, and Sharon Lafraniere. "13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign." The New York Times, The New York Times, 16 Feb. 2018, www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html. Accessed 19 Oct. 2018.

107 Lynch, Justin. "America Could Protect Cyberspace like WMDs." Fifth Domain, Fifth Domain, 1 Aug. 2018, www.fifthdomain.com/civilian/2018/08/01/america-could-protect-cyberspace-like-wmds/. Accessed 19 Oct. 2018.

108 Crerar, Pippa, et al. "Russia Accused of Cyber-Attack on Chemical Weapons Watchdog." The Guardian, Guardian News and Media, 4 Oct. 2018, www.theguardian.com/world/2018/oct/04/netherlands-halted-russian-cyber-attack-on-chemical-weapons-body. Accessed 19 Oct. 2018.

109 The Office of the President of the United States. National Cyber Strategy of the United States of America. The White House, September, 2018. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Accessed 19 Oct. 2018.

110 "Most Wanted." FBI, Federal Bureau of Investigation, 3 May 2016, www.fbi.gov/investigate/cyber/most-wanted. Accessed 19 Oct. 2018.

111 "Ten Most Wanted Fugitives FAQ." FBI, Federal Bureau of Investigation, 17 Sept. 2010, www.fbi.gov/wanted/topten/ten-most-wanted-fugitives-faq. Accessed 19 Oct. 2018.

112 "Ten Most Wanted Fugitives FAQ." FBI, Federal Bureau of Investigation, 17 Sept. 2010, www.fbi.gov/wanted/topten/ten-most-wanted-fugitives-faq. Accessed 19 Oct. 2018.

113 "Ten Most Wanted Fugitives FAQ." FBI, Federal Bureau of Investigation, 17 Sept. 2010, www.fbi.gov/wanted/topten/ten-most-wanted-fugitives-faq. Accessed 19 Oct. 2018.

114 "New Top Ten Fugitive." FBI, Federal Bureau of Investigation, 27 Sept. 2018, www.fbi.gov/news/stories/new-top-ten-fugitive-greg-alyn-carlson-092718. Accessed 19 Oct. 2018.

115 "Sanctions Related to Significant Malicious Cyber-Enabled Activities." U.S. Department of the Treasury, www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx. Accessed 19 Oct. 2018.

116 OFAC administers and enforces an extensive range of US trade and economic sanctions that target individuals, entities, and entire governments. Office of Foreign Assets Control. "Cyber-Related Sanctions Program," U.S. Department of the Treasury, 3 July 2017, pp 6. https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber.pdf. Accessed 19 Oct. 2018.

117 Executive Order. No. 13757 , 2016, p. 1. https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber2__eo.pdf. Accessed 19 Oct. 2018.

118 "Sanctions Programs and Country Information." U.S. Department of the Treasury, www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx. Accessed 19 Oct. 2018.

119 United States Congress, House, "Countering America's Adversaries Through Sanctions Act." Congress.gov, https://www.congress.gov/bill/115th-congress/house-bill/3364. 115th Congress, 1st session, House Resolution 3364, passed Aug. 02, 2017.

120 Masters, Jonathan. "What Are Economic Sanctions?" Council on Foreign Relations, Council on Foreign Relations, 7 Aug. 2017, www.cfr.org/backgrounder/what-are-economic-sanctions. Accessed Oct. 9, 2018.

121 See generally, Stoll, Cliff. Cuckoos Egg. Doubleday, 1989.

122 Carter, William A. and Jennifer C. Daskal. "Low-Hanging Fruit: Evidence Based Solutions to the Digital Evidence Challenge." Center for Strategic & International Studies, July 2018, pp. 5. https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge. Accessed Oct. 9, 2018.

123 Chalfant, Morgan. "State Dept. to Eliminate Cyber Office: Report." TheHill, 19 July 2017, thehill.com/policy/cybersecurity/342698-state-dept-to-eliminate-cyber-office-report. Accessed 19 Oct. 2018.

124 Johnson, Derek B. "Senate Panel Votes to Revive State Cyber Office." FCW, fcw.com/articles/2018/06/26/cyber-state-senate-office.aspx. Accessed 19 Oct. 2018.

125 Cohen, Zachary, et al. "Trump's Attacks Leave NATO Allies in Disbelief." CNN, Cable News Network, 12 July 2018, www.cnn.com/2018/07/11/politics/trump-nato-diplomats-reaction/index.html. Accessed 19 Oct. 2018.

126 The full list of countries that the United States has signed MLATs and agreed upon MLAAs with can be found here: "Treaties and Agreements." U.S. Department of State, U.S. Department of State, 7 Mar. 2012, www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm. Accessed 19 Oct. 2018.

127 Mulligan Stephen, "Cross-Border Data Sharing Under the CLOUD Act," Congressional Research Service, 23 Apr., 2018, pp 15-23. https://fas.org/sgp/crs/misc/R45173.pdf. Accessed 19 Oct. 2018.

128 Mulligan Stephen, "Cross-Border Data Sharing Under the CLOUD Act," Congressional Research Service, 23 Apr., 2018, pp 15-23. https://fas.org/sgp/crs/misc/R45173.pdf. Accessed 19 Oct. 2018.

129 United States Congress, House, "CLOUD Act." Congress.gov,https://www.congress.gov/bill/115th-congress/house-bill/4943 115th Congress. 2nd session, House Resolution 4934, introduced Feb. 6, 2018. as included in United States Congress, House, "Consolidated Appropriations Act, 2018," Congress.gov, https://www.congress.gov/bill/115th-congress/house-bill/1625. 115th Congress, 2nd session, House Resolution 1625, passed March 3, 23, 2018.

130 United States Department of Justice, "Interpol Red Notices," Sept. 19, 2018. Accessed Oct. 10, 2018. Available at: https://www.justice.gov/jm/criminal-resource-manual-611-interpol-red-notices; "Red Notices." Red Notices / Notices / INTERPOL Expertise / Internet / Home - INTERPOL, www.interpol.int/INTERPOL-expertise/Notices/Red-Notices.

131 "Interpol Red Notices." Criminal Resource Manual, The United States Department of Justice, 19 Sept. 2018, www.justice.gov/jm/criminal-resource-manual-611-interpol-red-notices. Accessed 19 Oct. 2018.

132 Doyle, Charles. "An Abridged Sketch of Extradition To and From the United States.", Congressional Research Service, 4 Oct. 2016. RS22702, fas.org/sgp/crs/misc/RS22702.pdf. Accessed 19 Oct. 2018.

133 "Convention on Cybercrime." Treaty Office, Council of Europe, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Accessed 19 Oct. 2018.

134 The Office of the President of the United States. National Cyber Strategy of the United States of America. The White House, September, 2018, pp 26. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Accessed 19 Oct. 2018.

135 Office of the Coordinator For Cyber Issues. "Cybercrime Factsheet." United States Department of State, A/GIS/GPS, Aug. 2015, 2009-2017.state.gov/documents/organization/255007.pdf. Accessed 19 Oct. 2018.

136 For example, the International Criminal Investigative Training Assistance Program (ICITAP) at the US Department of Justice provides technical assistance and training to foreign governments to fight transnational cybercrime. "Terrorism and Transnational Crime." The United States Department of Justice, 10 Feb. 2016, www.justice.gov/criminal-icitap/subject-matter-expertise/terrorism-transnational-crime. Accessed 19 Oct. 2018.

137 Norris, John. "A Bad Budget for America's Place in the World." Center for American Progress, 13 Feb. 2018, www.americanprogress.org/issues/security/news/2018/02/13/446557/bad-budget-americas-place-world/. Accessed 19 Oct. 2018.

138 Corrigan, Jack, and Government Executive. "The Hollowing Out of the State Department Continues." The Atlantic, Atlantic Media Company, 11 Feb. 2018, www.theatlantic.com/international/archive/2018/02/tillerson-trump-state-foreign-service/553034/. Accessed 19 Oct. 2018.

139 The Office of the President of the United States. National Cyber Strategy of the United States of America. The White House, September, 2018. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Accessed 19 Oct. 2018.

140 See for example, Data Protection and Cybercrime Division, Council of Europe. "Capacity Building on Cybercrime." Council of Europe, 2013, doi:10.1017/CBO9781107415324.004. Accessed 19 Oct. 2018.

141 "Activities." Capacity Building / Activities / Cybercrime / Crime Areas / Internet / Home – INTERPOL, INTERPOL, www.interpol.int/Crime-areas/Cybercrime/Activities/Capacity-building. Accessed 19 Oct. 2018.

142 "Capacity Building for Criminal Justice Practitioners Combating Cybercrime and Cyber-Enabled Crime in South-Eastern Europe." OSCE POLIS, Organization for Security and Co-Operation, polis.osce.org/node/9381. Accessed 19 Oct. 2018.

143 See for example "Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy." Freedom House, 31 Aug. 2018, www.freedomhouse.org/report/freedom-net/freedom-net-2017; Waterman, Shaun. "Freedom House: Governments Are Turning Cyberweapons on Their Own People." Cyberscoop, 14 Nov. 2017, www.cyberscoop.com/freedom-house-repression-fotn-cyberweapons-ddos-dissidents/. Accessed 19 Oct. 2018

144 For example, Egypt recently passed a new cybercrime law that human rights groups argue allows broad scope for the Egyptian government to prosecute journalists, activists, and government critics for any criticism of the government: "Egypt Internet: Sisi Ratifies Law Tightening Control over Websites." BBC News, BBC, 18 Aug. 2018, www.bbc.com/news/world-middle-east-45237171. Accessed 19 Oct. 2018

145 Finklea, Kristin, "Justice Department's Role In Cyber Incident Response," Congressional Research Service, August 23, 2017, pp 8-9. https://fas.org/sgp/crs/misc/R44926.pdf. Accessed 19 Oct. 2018

146 Baker, Al. "An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported." The New York Times, 5 Feb. 2018. https://www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html. Accessed 19 Oct. 2018.

147 Baker, Al. "An 'Iceberg' of Unseen Crimes: Many Cyber Offenses Go Unreported." The New York Times, 5 Feb. 2018. https://www.nytimes.com/2018/02/05/nyregion/cyber-crimes-unreported.html. Accessed 19 Oct. 2018.

148 Lauristen, Janet and Cork, Daniel. "Expanding Our Understanding of Crime: The National Academies Report on the Future of Crime Statistics and Measurement." Criminology and Public Policy, vol. 16, no. 4, 2017, pp. 1075–98, doi:10.1111/1745-9133.12332.

149 Lauristen, Janet and Cork, Daniel. "Expanding Our Understanding of Crime: The National Academies Report on the Future of Crime Statistics and Measurement." Criminology and Public Policy, vol. 16, no. 4, 2017, pp. 1075–98, doi:10.1111/1745-9133.12332.

150 Federal Bureau of Investigation. FY 2018 Authorization and Budget Request to Congress. Department of Justice. May 2017, pp 4-31. https://www.justice.gov/file/968931/download. Accessed 19 Oct. 2018.

151 Federal Bureau of Investigation. FY 2018 Authorization and Budget Request to Congress. Department of Justice. May 2017, pp 4-31. https://www.justice.gov/file/968931/download. Accessed 19 Oct. 2018.

152 United States Secret Service. US Secret Service Budget Overview FY 2019 Congressional Justification. Department of Homeland Security, May 2017, pp 4. https://www.dhs.gov/sites/default/files/publications/U.S.%20Secret%20Service.pdf. Accessed 19 Oct. 2018.

153 Federal Bureau of Investigation. FY 2018 Authorization and Budget Request to Congress. Department of Justice. May 2017, pp 4-31. https://www.justice.gov/file/968931/download. Accessed 19 Oct. 2018.

154 United States, Congress, Cong. House, Committee on Oversight and Government Reform. "United States Secret Service: an Agency in Crisis", 9 Dec. 2015. 114th Congress, 1st session, report, oversight.house.gov/wp-content/uploads/2015/12/Oversight-USSS-Report.pdf. Accessed 19 Oct. 2018.

155 "National Cyber Investigative Joint Task Force." FBI, Federal Bureau of Investigation, 13 June 2016, www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force. Accessed 19 Oct. 2018.

156 "Cyber Task Forces: Building Alliances to Improve the Nation's Cybersecurity." FBI, Federal Bureau of Investigation, 31 May 2016, www.fbi.gov/file-repository/cyber-task-forces-fact-sheet.pdf/view. Accessed 19 Oct. 2018.

157 "The Investigative Mission." United States Secret Service, www.secretservice.gov/investigation/#field. Accessed 19 Oct. 2018.

158 United States Congress, House, "Consolidated Appropriations Act, 2018," Congress.gov, Page 201, https://www.congress.gov/115/bills/hr1625/BILLS-115hr1625enr.pdf. 115th Congress, 2nd session, House Resolution 1625, passed March 23, 2018.

159 Dorado, Gene L. "Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation." 2018, pp. 14–18. https://www.gao.gov/assets/700/693405.pdf. Accessed 19 Oct. 2018.

160 The Office of the President of the United States. National Cyber Strategy of the United States of America. The White House, September, 2018. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Accessed 19 Oct. 2018.

161 National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report. 22 July 2004. www.9-11commission.gov/report/. Accessed 19 Oct. 2018.

162 National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report. 22 July 2004, pp 365. www.9-11commission.gov/report/. Accessed 19 Oct. 2018.

163 "Office of National Drug Control Policy." Office of National Drug Control Policy, The White House, www.whitehouse.gov/ondcp/. Accessed 19 Oct. 2018.

164 Eilperin, Juliet. "Obama May Appoint an Ebola Czar, He Says." The Washington Post, 16 Oct. 2014, https://www.washingtonpost.com/news/post-politics/wp/2014/10/16/obama-may-appoint-an-ebola-czar-he-says/. Accessed 19 Oct. 2018.

165 Perloth, Nicole, and David Sanger. "White House Eliminates Cybersecurity Coordinator Role." The New York Times, 15 May 2018, https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html. Accessed 19 Oct. 2018.

166 Perloth, Nicole, and David Sanger. "White House Eliminates Cybersecurity Coordinator Role." The New York Times, 15 May 2018, https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html. Accessed 19 Oct. 2018.

167 United States Congress, House, "Consolidated Appropriations Act, 2018," Congress.gov, Page 201, https://www.congress.gov/115/bills/hr1625/BILLS-115hr1625enr.pdf. 115th Congress, 2nd session, House Resolution 1625, passed March 23, 2018.

168 Lisa N. Sacco and Kristin Finklea, "The Role of the Office of National Drug Control Policy (ONDCP)," CRS Insight, Congressional Research Service, June 1, 2018, pp 1. https://fas.org/sgp/crs/misc/IN10912.pdf. Accessed 19 Oct. 2018.

169 "Law Enforcement Cyber Incident Reporting." Department of Justice, www.justice.gov/usao-ct/page/file/906222/download. Accessed 19 Oct. 2018.

170 United States, Congress, Cong. House, Committee on Oversight and Government Reform. "United States Secret Service: an Agency in Crisis", 9 Dec. 2015. 114th Congress, 1st session, report, oversight.house.gov/wp-content/uploads/2015/12/Oversight-USSS-Report.pdf. Accessed 19 Oct. 2018.

171 "Law Enforcement Cyber Incident Reporting." Department of Justice, www.justice.gov/usao-ct/page/file/906222/download. Accessed 19 Oct. 2018.

172 "Law Enforcement Cyber Incident Reporting." Department of Justice, www.justice.gov/usao-ct/page/file/906222/download. Accessed 19 Oct. 2018.

173 "Law Enforcement Cyber Incident Reporting." Department of Justice, www.justice.gov/usao-ct/page/file/906222/download. Accessed 19 Oct. 2018.

174 National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report. 22 July 2004. www.9-11commission.gov/report/. Accessed 19 Oct. 2018.

175 National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report. 22 July 2004, pp 74. www.9-11commission.gov/report/. Accessed 19 Oct. 2018.

176 National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report. 22 July 2004, pp 76. www.9-11commission.gov/report/. Accessed 19 Oct. 2018.

177 National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report: Executive Summary. 22 July 2004, pp 15-16. www.9-11commission.gov/report/. Accessed October 19, 2018.

178 National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report. 22 July 2004, pp 93-94. www.9-11commission.gov/report/. Accessed 19 Oct. 2018.

179 National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report. 22 July 2004, pp 15-16. www.9-11commission.gov/report/. Accessed 19 Oct. 2018.

THIRD WAY

About Third Way

Third Way is a nonprofit organization headquartered in Washington, DC. The think tank champions modern center-left ideas and its work is grounded in the mainstream American values of opportunity, freedom, and security.

Third Way's agenda is ambitious, aspirational, and actionable. It is built on the bedrock belief that for political movements to succeed in the US political system, they must relentlessly re-imagine their policies, strategies, and coalitions.

Third Way's advantage lies in its high-impact advocacy campaigns that combine rigorous policy research with a unique and incisive understanding of the vast American middle—the people who ultimately decide majorities and provide mandates for change. The work is designed to persuade elected officials, intellectuals, advocates, the media, and others with political influence.

The Third Way National Security Program is focused on protecting Americans from 21st century global threats by moving forward bold and pragmatic new ideas. The National Security Program works hand in hand with diverse coalitions of civil society groups, academics, and others on all sides of the political spectrum to develop and promote smart and tough policy ideas and educate policymakers to make America strong and safe, while preserving American values. The Program's Cyber Enforcement Initiative is non-partisan and is not associated with any specific US political party.