Atlantic Council
GEOTECH CENTER

DFRLab

CYBERSECURE THE FUTURE: RANSOMWARE

Trent R. Teyema | Kiran S. Jivnani | David A. Bray

July 2022

ISBN-13: 978-1-61977-241-0

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions. This report is made possible by general support to the Atlantic Council's Middle East Programs.

CYBERSECURE THE FUTURE: RANSOMWARE

Trent R. Teyema | Kiran S. Jivnani | David A. Bray

EXECUTIVE SUMMARY 2

INTRODUCTION 4

BUILDING THIS REPORT AND CONCEPTUALIZING THE RANSOMWARE LIFE CYCLE 5

KEY FINDINGS 6

GLOSSARY 16

ABOUT THE AUTHORS 17

ACKNOWLEDGMENTS 18

EXECUTIVE SUMMARY

This report endeavors to examine key challenges in predicting, safeguarding against, and dealing with ransomware attacks, thereby better informing US and international policy to combat such attacks and their perpetrators. To identify the aforementioned challenges, the Atlantic Council's GeoTech Center, in partnership with the Digital Forensic Research Lab Cyber Statecraft Initiative, held four roundtables that connected government officials from the Department of Justice, the Federal Bureau of Investigation, and the United States Secret Service with executive-level industry experts in cybersecurity and ransomware. The key findings along with the primary observations of the roundtables are listed below.

Summary of Findings and Observations

Summary of Findings

Finding 1.1: Industry is seeing **two parallel trends** when it comes to ransomware models. On the one hand, industry is seeing an increase in independent, skilled hackers, as opposed to established hacker gangs. This shift is resulting in friction in the cybercriminal world and could be positive for law enforcement agencies. Alternatively, some industry members are reporting that there is a lowered barrier of entry for inexperienced or nontechnical cybercriminals, therefore expanding the ransomware criminal industry. More research needs to be done to determine which one of these trends is truly on the rise.

Despite the two opposing trends, all of industry agrees that ransomware groups are learning from their mistakes and continually improving their techniques, tactics, and procedures (TTPs) while actively managing their brands and reputations.

Finding 1.2: Ransomware attacks are opportunistic—targeting organizations with vulnerable online systems and/or during key periods when they have pressure to be up and running.

Finding 2.1: Information sharing between government and the private sector, while integral to tackling ransomware, is inconsistent. Federal law enforcement has made it clear that the legal counsels of private companies have repeatedly raised concerns about constraints that limit the sharing of information that could aid in the detection and reporting of illicit activities.

Finding 2.2: The stigma and consequences of being the victim of a cyberattack present a challenge to information sharing. Oftentimes, victims are reluctant to report incidents to government agencies for fear of negative consequences such as double victimization.

Finding 2.3: Since ransomware attacks are happening at an increasing speed, information sharing between law enforcement and industry should be faster.

Finding 3.1: The establishment of a national law enforcement team to focus specifically on cryptocurrency, which is increasingly used for cybercrime payments, is a step in the right direction.

Finding 3.2: Law enforcement discourages paying a ransom, but encourages prompt reporting regardless of a decision to pay.

Finding 3.3: Federal law enforcement should work to detail appropriate processes for how e-currency or cryptocurrency service providers work with law enforcement to monitor for criminal activities beyond just ransomware, including use of cryptocurrencies for illicit activities such as human trafficking and other transnational criminal offenses.

Summary of observations

Observation 1.1: An international public-private sector partnership needs to be developed to address the transnational nature of ransomware schemes. Such a partnership should focus on helping law enforcement to focus more of its energy on tracing and arresting perpetrators within ransomware groups.

Observation 1.2: It is important to implement stronger defense mechanisms and use updated and secure software to make entering a network more difficult particularly for heavily targeted industries.

Observation 2.1: Better uniform reporting and sharing of information is needed. In particular, standardized timelines, questions, and formats are needed for incident reporting. Even with the Cyber Incident Reporting for Critical Infrastructure Act of 2022, there still remains confusion across government and critical infrastructure entities as to the logistics of reporting incident information. In addition, it is unclear how reported incident information will be shared between departments, government agencies, and the private sector.

Observation 2.2: Safe harbor and shield laws are needed for ransomware reporting; mandated reporting, in particular, requires a safe harbor framework.

Observation 2.3: Establish and strengthen public and private partnerships through joint tabletop exercises and relationship building with law enforcement and the government.

Observation 3.1: The US government and Federal Reserve should work with the National Cryptocurrency Enforcement Team to properly evaluate the strategic implementation of a US central bank digital currency (CBDC).

Observation 3.2: “To pay or not to pay” a ransom is ultimately a business decision. This decision should be made with proposed safe harbor protections in coordination with law enforcement.

INTRODUCTION

In an interconnected world, digital threats have become increasingly common. Chief among them is ransomware, a malware-based cyberattack that encrypts files, rendering data inaccessible. Once an attack has successfully been inflicted, hackers promise to restore systems and data in exchange for a ransom.

Ransomware has existed for over two decades but reached new heights in the last few years.[1] In 2020, known ransomware payments totaled $400 million globally and topped $81 million in the first quarter of 2021.[2] Financial motivations are not the only driver for these cyberattacks. Nation-states, among others, can use ransomware to demonstrate vulnerabilities in the critical infrastructures of their rivals or disguise deliberate destruction of data and information systems. This makes ransomware a potent tool of geopolitical power.[3]

Ransomware incidents have disrupted critical services and organizations of all sizes including schools, banks, hospitals, and transportation. A high-profile example of this is the 2021 Colonial Pipeline hack. This attack targeted Colonial Pipeline's billing system and led to the shutdown of the largest fuel pipeline in the United States, introducing gas shortages across the East Coast. The hackers were affiliated with a Russian-speaking cybercrime group known as DarkSide and received $4.4 million in ransom from Colonial after the attack,[4] part of which was later recovered with the assistance of US law enforcement.[5] One of the criminals associated with this attack was later found and charged on January 14, 2022, as a result of US-Russia collaboration. At the request of the United States, Russia dismantled the ransomware crime group, REvil, in an operation in which it detained and charged the group's members, one of whom was responsible for the Colonial Pipeline attack.[6]

As a harbinger of things to come, costs associated with ransomware are expected to reach new heights by 2031. Cybersecurity Venturesa, a research firm, predicts that there will be a new ransomware attack every two seconds by 2031 and that global costs are expected to exceed $265 billion.[7] Against this backdrop, the Atlantic Council's GeoTech Center and Digital Forensic Research Lab (DFRL) held a series of off-the-record, private conversations. The discussions examined the connections among ransomware, cyber threat intelligence, industry insurance, cryptocurrencies, and adversarial actors. Participants included high-level members of the US Department of Justice, the Federal Bureau of Investigation, the US Secret Service, and industry experts. This report highlights the key findings of these conversations, followed by the observations that emerged as a result of those findings.

[1] Chuck Brooks, "Ransomware on a Rampage; a New Wake-Up Call," *Forbes*, August 21, 2021, https://www.forbes.com/sites/chuckbrooks/2021/08/21/ransomware-on-a-rampage-a-new-wake-up-call/?sh=524d9d822e81.

[2] "FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware," White House Briefing Room (website), October 13, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/.

[3] *Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar, 2019 Public-Private Analytic Exchange Program, Department of Homeland Security,* https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf.

[4] William Turton and Kartikay Mehrotra, "Hackers Breached Colonial Pipeline Using Compromised Password," Bloomberg, June 4, 2021, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

[5] "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," Justice Department Office of Public Affairs, June 7, 2021, https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

[6] Tom Balmforth and Maria Tsvetkova, "Russia Takes Down REvil Hacking Group at U.S. Request: FSB," Reuters, January 14, 2022, https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/.

[7] Steve Morgan, "Top 6 Cybersecurity Predictions and Statistics for 2021 to 2025," *Cybercrime Magazine*, December 30, 2021, https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/#:~:text=The%20frequency%20of%20ransomware%20attacks,exceed%20200%20zettabytes%20by%202025.

BUILDING THIS REPORT AND CONCEPTUALIZING THE RANSOMWARE LIFE CYCLE

In 2021, the Atlantic Council GeoTech Center convened subject matter experts from the cybersecurity industry and federal law enforcement agencies for a series of four off-the-record roundtable conversations. The objective of these roundtables was to convene and allow subject matters experts to speak freely on issues surrounding ransomware and to compile these conversations into a report with concrete findings and corresponding observations. The findings and observations in this report expressly grew out of the views articulated by the private sector and law enforcement officials present for these conversations, and as such not every finding has a corresponding observation. In some cases, findings or observations are supplemented by existing research. Due to the private nature of these conversations, none of these findings or observations will be linked to the specific companies or law enforcement agencies that were present.

Senior executives from the following companies and organizations were in attendance. All participants in these roundtables were given an equal right to participate and share their views and experiences.

Roundtable 1: Ransomware and Cyber Threat Intelligence

Attendance record:

- US Department of Justice
- Federal Bureau of Investigation
- McAfee LLC[8]
- CrowdStrike Services
- Flashpoint
- Accenture
- Intel471
- Atlantic Council

Roundtable 2: Ransomware and Cyber Incident Response

Attendance record:

- US Department of Justice
- Federal Bureau of Investigation
- McAfee LLC
- CrowdStrike Services
- Flashpoint
- Blue Ridge Networks
- Intel471
- Atlantic Council

Roundtable 3: Ransomware and Cryptocurrencies

Attendance record:

- US Department of Justice
- Federal Bureau of Investigation
- US Secret Service
- Flashpoint
- CrowdStrike Services
- Andreessen Horowitz
- Accenture
- SICPA
- Atlantic Council

Roundtable 4: Ransomware and On-the-Horizon Threats

Attendance record:

- US Department of Justice
- Federal Bureau of Investigation
- Flashpoint
- CrowdStrike Services
- Blue Ridge Networks
- McAfee LLC
- Maximus
- Forward Edge-AI
- System 1 Inc.
- DataPolicyTrust
- Accenture

[8] Following the firm's participation in roundtables, McAfee merged with FireEye and is known as Trellix.

KEY FINDINGS

1. Facing Ransomware Realities

Finding 1.1 Industry members are seeing two parallel trends when it comes to ransomware models. On the one hand, some of them see an increase in independent, skilled hackers, as opposed to established hacker gangs. This shift is resulting in friction in the cybercriminal world and could be positive for law enforcement agencies. Alternatively, some industry members are reporting that there is a lowered barrier of entry for inexperienced or nontechnical cybercriminals, therefore easing the expansion of the cybercriminal industry. More research needs to be done to determine which one of these trends is truly on the rise.

Despite the two opposing trends, all of industry agrees that ransomware groups are learning from their mistakes and continually improving their techniques, tactics, and procedures (TTPs) while actively managing their brands and reputations.

According to industry members, ransomware business models are shifting. Historically, ransomware-as-a-service (RaaS) was a hierarchical business model in which established ransomware gangs advertised their RaaS programs and recruited independent hackers to their team by conducting interviews and instituting hiring frameworks. In this model, developers held most of the leverage, as independent hackers were usually less skilled and just needed to generate installations via botnets, exploit kits, or stolen credentials. However, in recent years, some industry members are noting that the skill set for independent hackers has changed as ransomware gangs have shifted their focus from targeting individuals to targeting organizations. As a result, they must now penetrate and compromise entire networks. **This has changed the typical independent hacker profile to one of a highly skilled cybercriminal that is more sought after.** This has given independent hackers the freedom to demand elevated levels of compensation and authority in the group. In many cases, these independent hackers now have the skills and motivation to form their own groups, consisting of equally skilled partners.[9]

According to these industry experts, the onset of the pandemic also exacerbated the asking power of individual hackers as the cybercriminal underground was increasingly looking to identify the skills and talents of individuals.[10] There have been advertisements for people with different language skills, broad technical abilities, marketing abilities, and more. Analysts have also noticed an uptick in freelancers, indicating a change in the original RaaS model. In this new age, potential affiliates are dictating which ransomware groups they will work with.

Predictions from some of industry suggest that the shift in the power dynamic between ransomware gangs and individual hackers will continue to widen.[11] These industry experts believe that increasing friction between independent hackers and ransomware gangs is likely positive for law enforcement as it indicates infighting within the criminal marketplace.[12] According to these experts, independent hackers feel that ransomware gangs are not compensating them enough for their work or independent hackers simply disagree with the tactics of developers. This is exemplified by the recent Conti Crew leak in which a disgruntled affiliate leaked Conti's playbook after alleging underpayment by the group. This move was a huge blow to the group as the leaked Conti documentation could help researchers or law enforcement to better understand the TTPs used by this group of criminals. It also could allow other groups to use the leaked playbook as a guide for their own criminal activities.[13] Similarly, the source code for Babuk ransomware was also leaked on

[9] Max Kersten, John Fokker, and Thibault Seret, "How Groove Gang Is Shaking Up the Ransomware-as-a-Service Market to Empower Affiliates," Trellix (website), blog co-authored with Intel471 and McAfee Enterprise Advanced Threat Research, September 08, 2021, https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/how-groove-gang-is-shaking-up-the-ransomware-as-a-service-market-to-empower-affiliates/.

[10] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Threat Intelligence, September 2021.

[11] Kersten, Fokker, and Seret, "How Groove Gang."

[12] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Threat Intelligence.

[13] Ionut Ilascu, "Translated Conti Ransomware Playbook Gives Insight into Attacks," *Bleeping Computer*, September 2, 2021, https://www.bleepingcomputer.com/news/security/translated-conti-ransomware-playbook-gives-insight-into-attacks/.

a Russian-language hacking forum by an alleged member of the group and, in general, Babuk has had a history of disagreements.[14] Chief among these was the splintering of the group after the attack on Washington's Metropolitan Police Department (MPD) in which the "Admin" wanted to leak MPD data for publicity, but other members of the group were against it. One threat actor from the group commented, **"**We're not good guys, but even for us it was too much.**"**[15] After the MPD data leak, the group fractured and reformed as Babuk V2 without the Admin.[16] Because of these patterns, several industry experts expect that these ransomware groups will become short-lived, and they see this as an opportunity for former gang members to work with law enforcement.[17]

Alternatively, other industry members have flagged a parallel trend in which the traditional RaaS model has lowered the barrier of entry for inexperienced or nontechnical cybercriminals. **This allows for the expansion of ransomware due to a lowered barrier of technical experience, and high-profit margins.** According to these experts, the expansion of ransomware attacks is also being fueled by the fact that more victims are willing to pay a hacker's ransom and the increased media attention around these hacks puts pressure on victims to resolve hostile situations quickly. Not only are more victims willing to pay for decryption of their data, but also, many of them do not want to admit that they were victims of ransomware in the first place because of the negative press surrounding victimization. **There is still a significant hesitancy to report incidents, industry members say**. This hesitancy impedes law enforcement agencies: they cannot get accurate and timely information about the scale of attackers, victims, and ransoms paid.[18]

Despite the two opposing trends, all the industry members present expressed that ransomware groups are learning from their mistakes and are innovating. Ransomware groups are more aware of how they are perceived and are realizing that they need a healthy balance of attention for their business model to succeed. They need to be known and have a reputation to entice a ransom payment out of their victims, but if they get too big or launch a significant attack on critical infrastructure, as seen in the Colonial Pipeline and Kaseya attacks, they face the risk of garnering too much attention and ending up on law enforcement's radar. When this does happen, they often need to recalibrate strategy and possibly reform.[19]

When reforming, industry representatives believe that these cybercrime groups do not spend a lot of time or money. They often use similar TTPs by recycling and leveraging existing malicious code, tools, and techniques, thereby reducing the amount of investment in research and development. Industry members also believe that ransomware actors exert more effort in increasing the speed of their attack—whether that is encrypting networks in record time or rapidly gaining access to a victim and deploying ransomware, as opposed to attacking covertly through reinvention. This preference is because the opportunity for great profit and wealth significantly outweighs the risk of repercussions for their attacks. According to one industry expert in the first roundtable,

> "They are more interested in being up and running fast, than completely obscuring who they are and who they were."[20]

Observation 1.1 An international public-private sector partnership needs to be developed to address and conduct further research on the transnational nature of ransomware schemes particularly as they continue to innovate. Such a partnership should focus on helping law enforcement to focus more of its energy on tracing and arresting perpetrators within ransomware groups.

In October 2021, the White House National Security Council facilitated a Counter-Ransomware Initiative over two days and six sessions, starting with a

[14] Lawrence Abrams, "Babuk Ransomware's Full Source Code Leaked on Hacker Forum," *Bleeping Computer*, September 3, 2021, https://www.bleepingcomputer.com/news/security/babuk-ransomwares-full-source-code-leaked-on-hacker-forum/?&web_view=true.

[15] "The Source Code for the Babuk Ransomware Leaked on a Hacker Forum," *Cyber Intel Magazine, September 7, 2021,* https://cyberintelmag.com/malware-viruses/the-source-code-for-the-babuk-ransomware-leaked-on-a-hacker-forum/.

[16] "The Source Code for the Babuk Ransomware Leaked."

[17] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Threat Intelligence.

[18] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Threat Intelligence.

[19] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Threat Intelligence.

[20] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Threat Intelligence.

plenary.[21] As a result of the sessions in this summit, the ministers and representatives of Australia, Brazil, Bulgaria, Canada, the Czech Republic, the Dominican Republic, Estonia, the European Union, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Lithuania, Mexico, the Netherlands, New Zealand, Nigeria, Poland, Republic of Korea, Romania, Singapore, South Africa, Sweden, Switzerland, Ukraine, United Arab Emirates, the United Kingdom, and the United States recognized that ransomware is an escalating global security threat with serious economic and security consequences.[22] As part of the agenda, four areas of significant importance were identified:

1. Disrupt ransomware infrastructure and actors.
2. Bolster resilience to withstand ransomware attacks.
3. Address the abuse of virtual currency to launder ransom payments.
4. Leverage international cooperation to disrupt the ransomware ecosystem and address safe harbors for ransomware criminals.[23]

Despite these recent efforts, and although government is a primary entity that has the power to act against rogue actors, groups, or nations via diplomatic, intelligence, military, economic, and enforcement actions, industry experts at the roundtable noted that governments cannot act alone on ransomware. They emphasized that there is no law enforcement, government, or private-sector entity that can fully tackle the problem of ransomware themselves, and that the current public-private sector partnerships are limited by the geographic, political, and legal boundaries of the countries in which they reside. **To address the transnational nature of ransomware schemes, industry experts say, there should be public-private partnerships both domestically and internationally, particularly with countries like Russia that serve as safe havens for many of these cybercriminals.**

Interestingly, although the CRI did not involve Russia, the White House has commented that "the U.S.-Kremlin Experts Group, which is led by the White House, was established by President Biden and President Putin." This means that the United States engages directly with Russia on ransomware. The White House further added that they "look to the Russian government to address ransomware criminal activity coming from actors within Russia."[24]

Such a transnational public-private partnership could potentially commence by including the countries that participated in the CRI. It should look at key questions such as:

1. How should this partnership address the transnational nature of ransomware schemes and what actions should be taken internationally?
2. Which nation should lead the organization of this partnership?
3. Why are the existing international cooperative mechanisms to address ransomware insufficient and what can be learned from prior efforts?

Invitations to participate in such an initiative can also be extended to other countries that have demonstrated a sufficient level of action or intent to act against ransomware attacks and the individuals perpetrating them. A key focus of this partnership should be on global law enforcement agencies coming together to focus on tracing and arresting key perpetrators within ransomware groups.

In the aftermath of ransomware incidents, industry feels as though law enforcement does not focus enough on tracing and arresting individual members of ransomware groups. They feel as though some of the attention that law enforcement puts toward identifying the latest TTPs or the victims of the crime could instead be redirected to catching the criminals responsible for the attack.[25]

[21] White House, "Background Press Call on the Virtual Counter-Ransomware Initiative Meeting," Via Teleconference, October 12, 2021, https://www.whitehouse.gov/briefing-room/press-briefings/2021/10/13/background-press-call-on-the-virtual-counter-ransomware-initiative-meeting/.

[22] Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021, https://s3.documentcloud.org/documents/21085090/joint-statement-international-counter-ransomware-initiative.pdf; also available at White House, Briefing Room, Statements and Releases, October 14, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/.

[23] "FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware."

[24] White House, "Background Press Call on the Virtual Counter-Ransomware Initiative Meeting."

[25] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Threat Intelligence.

However, even if more resources such as this proposed partnership went into targeting the individuals that develop, create, and commit crimes with ransomware variants, there would still be challenges in finding and arresting them. One industry expert pointed to an individual who has been underground for a long time and has been an affiliate of six different ransomware variants. Although law enforcement officials know who he is and where he is, he can operate with impunity in Russia as long as he does not target organizations located in the Commonwealth of Independent States. Further, because investigations are naturally reactive, an initial investigation should begin by focusing on the TTP of the attack and on the indicators of compromise provided by the victims. After an initial assessment of the variant and victim, however, law enforcement should make greater efforts to focus their investigations on the individual perpetrators of cybercrimes.[26]

Finding 1.2 Ransomware attacks are opportunistic. They target organizations with vulnerable online systems during key periods when they have pressure to be up and running. The pressure to stay up and running often leads to some victims paying a ransom, creating a flawed system that involves trusting cybercriminals to return data.

Ransomware attacks are essentially attacks of opportunity. According to industry experts, there is a thriving ransomware marketplace and no shortage of individuals or groups called initial access brokers who can sell access into compromised organizations. In fact, industry experts believe that poorly secured remote desk protocol (RDP) endpoints are one of the most common vectors used to get inside an organization and can be acquired relatively cheaply. Therefore, at the end of the day, any sector or organization with online credentials or online systems is vulnerable.[27] Key targeted industries are those that have pressure to be up and running**. Specifically, criminals are looking for organizations that have poor security and that quantify downtime in high dollar amounts, creating pressure to pay the ransom as quickly as possible**. **Heavily targeted sectors that meet these criteria include healthcare, manufacturing, school districts, local governments, technology, media, and telecom services**.[28]

Oftentimes, victim organizations in heavily targeted sectors will pay a ransom to get their data back. However, paying for data and getting a decryptor does not ensure the return of data, according to industry experts. Ransomware criminals might issue a decryptor that simply does not work or takes too long to work. Alternatively, these criminals might simply not respond and disappear with the money. Paying a ransom involves trusting criminals to keep their end of the bargain and this method is flawed.

Observation 1.2 It is important to implement stronger defense mechanisms and use updated and secure software to make entering a network more difficult, particularly for heavily targeted sectors.

Most industry members pointed to one key recommendation to help organizations better prepare and protect themselves from ransomware attacks. **Their primary suggestion was tightening basic defense mechanisms, making it more difficult for an adversary to enter networks.** Security software and cybersecurity company experts that do real-time tracking of potential cyber threats found that initial entry vectors such as weak passwords or poorly protected systems are common in most of the incidents that they deal with.[29]

In many cases, the largest attacks of ransomware have been against companies that work in regulated industries and do not follow the established standards set out by the National Institute of Standards and Technology, the federal government, insurance companies, etc. Such standards include patch management and keeping restorable data backups. The WannaCry attack is a perfect example of this. In this attack, ransomware spread through server message block (SMB) protocol. SMB is used by Windows machines to communicate with file systems over networks. The ransomware in this attack worked by targeting machines that had not gotten the necessary security patch (MS17-010 Security Bulletin) from Microsoft. Once the ransomware was deployed, it spread to all the other devices in the same network that did not have the necessary patch, therefore taking control of their files as well. This attack worked so well that in five

[26] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Threat Intelligence.

[27] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Threat Intelligence.

[28] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Threat Intelligence.

[29] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Threat Intelligence.

days the virus was able to spread to more than 150 countries.[30]

As illustrated by the WannaCry attack, industry experts emphasized that core infrastructure needs to be kept up to date, and incentives or punitive measures need to be put into place to ensure that standards are kept current. Some industry experts took this argument a step further and criticized some software developers. Although there is no such thing as 100 percent secure software, they pointed out that there are a lot of vendors that are very good at responding to vulnerabilities. However, some vendors dismiss vulnerabilities and respond to them by claiming that the product has reached its end of life and an upgrade to a newer model is needed, even if the former model has only been on the market for a short period of time. In these cases, some industry experts believe that software updates and support should be provided for a certain period of time. Once that period of time has passed, only then is it fair to ask the customer to invest in a new product. Another adjustment that needs to be made is the timeline between a patch getting released and it being applied in industry. As of right now, the timeline is 180 days, which industry experts argue is far too long.[31]

2. Information Sharing and Mandated Reporting

Finding 2.1 Information sharing between the government and the private sector, while integral to tackling ransomware, is inconsistent. Federal law enforcement has made it clear that the legal counsels of private companies have repeatedly raised concerns about constraints that limit the sharing of information that could aid in the detection and reporting of illicit activities.

Information sharing and communication between the public and the private sector is key to catching and deterring cybercriminals. Information sharing allows cybersecurity experts in both the public and private sectors to learn about new vulnerabilities in software and about new attack vectors. It also can help to strengthen collective resiliency in and between those sectors. Finally, information sharing allows for the scope of cybercrimes to be defined more accurately and can influence the processes used to anticipate or respond to threats.[32]

Although information sharing is important, in the event of a breach, there is only so much that the government can share with anyone who is not the victim. Sometimes government officials are unable to share specially protected information such as criminal locations or identifying factors such as names with victims. At the same time, the private sector needs a framework to safely share information without waiving corporate and legal protections such as attorney-client privilege in order to increase such sharing.[33] When a company gets hit by a ransomware attack, the first step often is to engage a lawyer.[34]

At the time of the roundtables, industry experts explained that in many cases, information sharing with law enforcement was avoided to protect the company's brand reputation and investor confidence, circumventing the stigma associated with being the victim of a cyberattack. Alternatively, a company might not see any benefit in reporting a crime or sharing any information with law enforcement. **Ultimately, it was a business decision as to whether a company should immediately report the incident to law enforcement or handle the matter internally, especially since there were no contractual, regulatory, or statutory requirements**. A privately held company could decide not to report a ransomware attack and pay the extortionists. A publicly traded company could also decide not to report the cyber incident to law enforcement and wait until its filing with the Securities and Exchange Commission (SEC). Collaborative investigations between public and private partners take time and resources, which sometimes prompts companies to decide to simply tackle the problem themselves.[35]

[30] Samantha Donaldson, "Wannacry Ransomware: Who It Affected and Why It Matters," Red Hat Developer (blog), https://developers.redhat.com/blog/2017/05/19/wannacry-ransomware-who-it-affected-and-why-it-matters#how_was_this_ransomware_stopped.

[31] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Threat Intelligence.

[32] "Why Is Information Sharing Important in Cybersecurity?," nstec.com (website), accessed April 29, 2022, https://www.nstec.com/network-security/cybersecurity/why-is-information-sharing-important-in-cybersecurity/#qa_3.

[33] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Incident Response, September 2021.

[34] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Threat Intelligence.

[35] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Incident Response.

Until recently, there was no legal framework or protections (such as a shield law) for a company to safely share information with law enforcement or other government agencies. The primary method of mandated reporting to the US government for a breach or cybersecurity incident has been through a contractual agreement to follow the Federal Acquisition Regulations (FAR), the Defense Federal Acquisition Regulations (DFAR), or the requirements of the SEC for publicly traded companies.

However, this changed to an extent in the first quarter of 2022 with the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which became law in March. CIRCIA requires "critical infrastructure organizations to report cyberattacks to the Cybersecurity and Infrastructure Security Agency (CISA) within seventy-two hours. The law also creates an obligation to report ransomware payments within twenty-four hours."[36] It addresses in part the following observation of participants of the roundtables, which were conducted by the GeoTech Center prior to CIRCIA becoming law; yet there is still room for confusion across government and critical infrastructure entities as to the logistics of reporting incident information.

Observation 2.1 Better uniform reporting and sharing of information is needed. In particular, standardized timelines, questions, and formats are needed for incident reporting. In addition, it is unclear how reported incident information will be shared between departments, government agencies, and the private sector.

The contours of a US government reporting framework are beginning to form, but much work remains in addressing concerns voiced in roundtable discussion about the specifics of threat reporting and the handling of victim information. While CIRCIA designates CISA as the focal point for all private infrastructure owners and operators to report significant cyber incidents, and requires covered entities to report a covered cyber incident to CISA within 72 hours after it reasonably believes a covered cyber incident has occurred, **this law does not define what constitutes "covered entities," "covered cyber incident," or "reasonably believes." Instead, it requires CISA to fill in these blanks through the rulemaking process.**[37]

Additionally, this law does not cover private companies who do not operate in the critical infrastructure sectors, and it is unclear how CISA will report information to law enforcement for action. Moreover, CISA has up to two years to issue proposed rules, and up to eighteen months thereafter to issue final rules.[38] In this time, CISA should address the inconsistencies of this act in order for it to be truly effective and cover all the necessary parties.

CISA also should consider frustration points that existed prior to the passage of CIRCIA. Industry experts expressed frustration primarily over having to share the same data multiple times with the federal government, often with different units in the same department. They were also frustrated because information sharing did not seem to be a two-way street. Law enforcement in turn explained that not all information gets shared between the different parts of the government and sometimes they should not be shared with each other.

Additionally, victims and relevant incident responders were not always sure what should be shared and why it should be shared. This is because government agencies do not provide a uniform list of questions and sometimes different parts of government require drastically different sets of information**. Therefore, CISA should consider having a defined set of questions and timelines that should be shared irrespective of the case or company that is attacked. Having a set of detailed, clear questions and timelines would make it much easier to coordinate the responses from the victim.**

[36] The Cyber Incident Reporting for Critical Infrastructure Act of 2022 passed Congress as part of an omnibus spending bill in mid-March 2022. For more information about the law, see Scott Carlson and Danny Riley, "President Biden Signs Bill Mandating Cyber Reporting for Critical Infrastructure Entities," **Seyfarth Shaw LLP** (article), JDSupra (website), April 14, 2022, https://www.jdsupra.com/legalnews/president-biden-signs-bill-mandating-1882190/. For the text of the act, see Consolidated Appropriations Act, P.L. No: 117-103 § Division Y (2022), https://www.congress.gov/bill/117th-congress/house-bill/2471/text.

[37] Shardul Desai et al., "Cyber Incident Reporting Requirement for Critical Infrastructure Sectors Signed into Law," Holland & Knight LLP (website), March 16, 2022, https://www.hklaw.com/en/insights/publications/2022/03/cyber-incident-reporting-requirements-for-critical-infrastructure.

[38] Jena M. Valdetero, "Congress Passes 72-hour Federal Breach Reporting Law for Critical Infrastructure," Greenberg Traurig LLP, Lexology (website), March 29, 2022, https://www.lexology.com/library/detail.aspx?g=b70dd100-5026-4494-8b5a-7050ea4b5632.

Finding 2.2 The stigma and consequences of being the victim of a cyberattack presents a challenge to information sharing. Oftentimes, victims are reluctant to report incidents to government for fear of negative consequences such as double victimization.

Prior to the passage of CIRCIA, publicly traded companies and critical infrastructure companies had a fiduciary responsibility to their shareholders to report information that may positively or negatively impact the value of the company and its stock. Since CIRCIA's passage, critical infrastructure companies are now required to also report cybersecurity incidents to the US government. However, noncritical infrastructure companies that are publicly traded are still only bound by fiduciary duty, government regulation, or state law.[39]

Reporting a ransomware attack or the decision to pay a ransom can have regulatory effects and impact stock value and public trust. Privately held companies that are not classified as critical infrastructure organizations, unless required by contract, regulation, or law, will assess the impact on their bottom line in making a decision on whether to report a ransomware attack and/or pay the extortion that is demanded. For these companies, the question of whether to pay a ransom is ultimately a business decision. It is the calculus of the impact on business operation, time to resume operations, the amount of the ransom, impact on brand reputation, and risk. The business decision may be as simple as if a company does not pay, it will go out of business and in fact, according to leading industry members, some companies would be out of business today if they had not paid a hacker's ransom.

Industry also voiced a concern that paying a ransom can cause companies to be unfairly targeted by the US Department of the Treasury's Office of Foreign Assets Control (OFAC). This office "administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy, or economy of the United States."[40] As a result, OFAC maintains lists that often includes cybercriminal groups or individuals involved in the act of cybercrime such as ransomware. However, because the true identities of ransomware gangs or individual extortionists are often unknown and are changed intentionally to hide from law enforcement, it is difficult for a company to know if the gang or individual is specifically prohibited or embargoed by an OFAC list.[41] Therefore, these lists occasionally put victims in a difficult position: in many cases they have to pay the ransom to remain economically viable, and thus cannot share information with the government because they might face ramifications due to paying a criminal group or individual on the OFAC lists.[42]

Despite all of the aforementioned difficulties related to information sharing, it is important to note that law enforcement and the government can be of great assistance to a company whose systems have been encrypted by ransomware. This is because law enforcement and the government may be in possession of the keys to decrypt the encryption pursuant to previous investigations, which can allow a victim company to speedily resume operations without having to pay a ransom.[43]

Observation 2.2 Safe harbor and shield laws are needed for ransomware reporting; mandated reporting, in particular, requires a safe harbor framework.

When asked about the concept of mandated reporting (prior to the passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022), some industry experts already felt that mandated reporting around payments is a good option. However, since getting companies to share proprietary information regarding a cyberattack is challenging (particularly if that information is unfavorable to their reputation or causes financial risk), they stress the need for a safe harbor to report information to the federal government without fear of repercussions from regulators, investors,

[39] Consolidated Appropriations Act, P.L. No: 117-103 § Division Y (2022).

[40] "Office of Foreign Assets Control–Sanctions Programs and Information," US Department of Treasury (website), https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information.

[41] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Incident Response.

[42] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Incident Response.

[43] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Incident Response.

the public, etc. Industry experts also think that there needs to be a fundamental change in how ransomware incident reporting and information sharing is approached.

Specifically, they seek a new safe harbor framework that allows victims to recover their information and get back online as quickly as possible without blocking the government's ability to pursue potential investigatory actions.[44] Such a framework should:

- Be specific about the types of companies, victims, and crimes that it will cover.
- Include safety net assurances for victim organizations where law enforcement agencies can show how to safely share information, how the information is going to be protected, and how it is going to be used.
- Determine what kind of limits on disclosure or federal action the framework is intended to forestall.
- Take into consideration the existing liability protections in the Cyber Information Sharing Act of 2015 and the Cyber Incident Reporting for Critical Infrastructure Act of 2022 to determine where they are insufficient and build on them.

To increase trust further, an industry expert recommended that law enforcement agencies themselves need to put "skin in the game" through this framework and show how they will be held accountable if the information provided is misused in some way.

The speed at which the information can be shared using this new framework is also a critical factor because so far, **the right mechanism to share information at a higher speed does not exist**. One industry expert pointed to the example of the WannaCry attack, which occurred within twenty-four hours. If a company waits twenty-four hours before sharing information with law enforcement, then by the time said information is processed and validated **it is already far too late**. It is integral to find a way to get this information to the relevant parties as quickly as possible because cybercriminals are continually increasing the speed of their operations and are encrypting or stealing data within hours of the initial infection.[45]

On the law enforcement side, the support for mandated reporting and the need for more information, in general, was extremely clear. Experts from the Department of Justice (DOJ) articulated that required sharing already existed in many contexts, often by regulation in certain sectors or state laws even prior to the passage of CIRCIA. With additional information, CISA might be able to better manage risk as the agency shares cybersecurity information across the private sector so that potential victims are aware of new cyberattacks and vulnerabilities. Law enforcement officials also agreed that they needed information through reporting because if victimization is not reported, there is no way for them to determine the true extent of cybercrime or assist in catching cybercriminals**. In particular, law enforcement requires technical indicators of compromise (IOCs) as quickly as possible because sharing IoCs quickly can help other organizations preemptively defend themselves while also allowing government to take action.**[46]

Finding 2.3 Since ransomware attacks are happening at an increasing speed, information sharing between law enforcement and industry should be faster.

From a ransomware incident-response perspective, there has been an increase in the speed and effectiveness of bad actors over the past three years. **Attacks that used to take days, weeks, and sometimes months to execute can now take under an hour and the information sharing between law enforcement and victim companies is not effective enough to keep up with the increasing speed of these attacks.**[47]

Observation 2.3 Establish and strengthen public and private partnerships through joint tabletop exercises and relationship building with law enforcement and the government.

Public and private partnerships need to be strengthened to keep up with the speed of criminals. Companies that have gone through tabletop exercises have worked out their responses ahead of an attack, and have already developed relationships with their local law enforcement offices; as a result, they are typically much more

[44] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Incident Response.

[45] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Incident Response.

[46] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Incident Response.

[47] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Incident Response.

prepared when it comes to information sharing because they have already developed a certain level of trust with law enforcement.[48] A number of such efforts have been initiated and could be further resourced, such as the US Secret Service Cyber Incident Response Simulations series.[49] The federal government also trains state and local law enforcement through, for instance, the National Cyber Forensics Institute's annual Cyber Games.[50]

When a company has not prepared for such an incident ahead of time, information sharing can be quite messy. In those cases, victim firms often wait to report useful information until **weeks to months later**, and by that time it is often too late to effectively disrupt cybercriminals.[51]

3. Ransomware and Cryptocurrencies

Finding 3.1 The establishment of a national law enforcement team to focus specifically on cryptocurrency, which is increasingly used for cybercrime payments, is a step in the right direction.

On October 6, 2021, Deputy Attorney General Lisa O. Monaco announced the formation of a National Cryptocurrency Enforcement Team (NCET). The creation of this new team combines the capabilities of DOJ's Criminal Division Money Laundering and Asset Recovery Section (MLARS), the Computer Crime and Intellectual Property Section (CCIPS), and other criminal division sections. A significant focus for NCET will be understanding how to better stop the usage of cryptocurrency for criminal purposes. Other primary focuses include: crimes committed in virtual currency exchanges, mixing and tumbling services, which attempt to launder the origin of illicit funds with seemingly legitimate sources of funds, and other crimes committed by money launderers.

NCET was created so that the Department of Justice would be able to tackle the criminal misuse of cryptocurrencies and digital assets. It is made up of attorneys from across departments including prosecutors with professional backgrounds in cryptocurrency, cybercrime, money laundering, and forfeiture. The purpose of NCET is to identify, investigate, support, and pursue cases that involve the criminal use of digital assets with an emphasis on virtual currency exchanges, mixing and tumbling services, infrastructure providers, and other entities that are aiding the misuse of cryptocurrency and related technologies to commit or facilitate crimes. NCET will also set strategic priorities on digital asset technologies, classify areas that need higher investigative and prosecutorial focus, and lead the initiatives to coordinate with domestic and international law enforcement partners, regulatory agencies, and private industry to overcome the criminal usage of digital assets. Finally, NCET will improve the DOJ Criminal Division's current efforts to deliver support and training to federal, state, local, and international law enforcement for the purpose of building capacity to investigate and prosecute cryptocurrency and digital asset crimes in the United States and globally.[52]

Observation 3.1 US government agencies and the Federal Reserve should work with the National Cryptocurrency Enforcement Team to properly evaluate the strategic implementation of a US central bank digital currency (CBDC).

In March President Biden signed an executive order, Ensuring Responsible Development of Digital Assets, directing the US government to "assess the technological infrastructure and capacity needs for a potential US CBDC in a manner that protects Americans' interests." It also calls on the Federal Reserve to continue to research, develop, and assess efforts for a potential US CBDC.[53]

Increasingly, victim payments resulting from ransomware attacks are being facilitated using

[48] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Incident Response.

[49] US Secret Service, "Secret Service Hosts Cyber Incident Response Simulation," Media Relations News Release, July 2, 2021, https://www.secretservice.gov/newsroom/releases/2021/07/secret-service-hosts-cyber-incident-response-simulation-0.

[50] US Secret Service, "U.S. Secret Service Announces the Winner of the Nationwide Cyber Games," Media Relations News Release, October 21, 2021, https://www.secretservice.gov/newsroom/releases/2021/10/us-secret-service-announces-winner-nationwide-cyber-games.

[51] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Cyber Incident Response.

[52] Department of Justice, "Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team," Office of Public Affairs News Release, October 6, 2021, https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team.

[53] White House, "FACT SHEET: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets," White House Briefing Room (website), March 9, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/fact-sheet-president-biden-to-sign-executive-order-on-ensuring-responsible-innovation-in-digital-assets/.

cryptocurrencies. Therefore, evaluating the implementation of a US CBDC should be a top priority for the federal government and law enforcement, in consultation with industry experts.[54]

Finding 3.2 Law enforcement discourages paying a ransom and encourages prompt reporting regardless of a decision to pay.

While many companies that are hit with ransomware attacks end up paying their attackers using cryptocurrencies, law enforcement strongly discourages paying a ransom for several reasons. There is no way to track what the ransom money is being used for. In many cases, ransomware groups operate like organized crime. The revenues are so substantial that even if a significant part of a group's operations is disrupted, it is still making millions of dollars. Those funds can be used to invest in infrastructure, to pay people off, and to buy assets.[55]

Observation 3.2 "To pay or not to pay" is ultimately a business decision. This decision should be made with proposed safe harbor protections in coordination with law enforcement.

If victim organizations stop paying ransom demands, cybercriminals have substantially less incentive to keep launching attacks. Furthermore, paying a ransom can make a company even more of a target for future attacks. According to law enforcement**, it might be more effective to rebuild and secure networks and systems than to pay a ransom.**

However, this is an overly simplistic view when you balance the amount of the ransom demanded and the cost of rebuilding an entire network. **Ultimately, the decision to pay or not pay a ransom resulting from a cyberattack is a business decision and companies should not be penalized for doing what is best for the company financially**. [56]

Finding 3.3 Federal law enforcement should work to detail appropriate processes for how e-currency or cryptocurrency service providers work with law enforcement to monitor for criminal activities beyond just ransomware, including use of cryptocurrencies for illicit activities such as human trafficking and other transnational criminal offenses.

The first rule of any criminal investigation is to follow the money. This is also the case when it comes to cybercrime involving digital currency. It is important to understand how bad actors are using cryptocurrency as a method of payment for all kinds of criminal activities, and how to disrupt or block this system.

According to industry experts, one of the ways to do this is to make sure that cryptocurrency cannot be converted to fiat currency through blockchain technology. However, to truly make this method of interruption effective, there should be a better partnership between the government and digital asset service providers. In fact, there is a better chance of being able to track bitcoin as opposed to cash because right now most ransomware is quite traceable and most payments are still being made through bitcoin, the largest cryptocurrency by market capitalization.[57]

[54] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Ransomware and Cryptocurrencies, October 2021.

[55] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Ransomware and Cryptocurrencies.

[56] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Ransomware and Cryptocurrencies.

[57] Atlantic Council, GeoTech Center, Cybersecure the Future Roundtable, Ransomware and Cryptocurrencies.

GLOSSARY

Babuk ransomware: A ransomware threat discovered in 2021 that currently targets the transportation, healthcare, plastic, electronics, and agriculture sectors. Similar to other ransomware variants, this one is deployed in the network of enterprises that criminals target and compromise.

Blockchain: Blockchain is a distributed digital ledger which works as a chain that stores individual blocks of data. It is used to support nearly all cryptocurrencies and is unique in that it is decentralized.

Colonial Pipeline: In 2021, Colonial Pipeline (the largest fuel pipeline in the United States) was the target of a cyberattack by the DarkSide group. Attackers infiltrated Colonial's network through a virtual private network and held 100 gigabytes of data hostage, posting a $4.4 million ransom. Within an hour, the entire pipeline was shut down for the first time in fifty-seven years to assess the threat. Colonial ultimately paid the ransom to DarkSide—part of which was later recovered by law enforcement.

DarkSide: A Russia-linked cybercrime group first seen in August 2020 that inflicted ransomware attacks in more than fifteen countries and targeted multiple industry sectors, including financial services, legal services, manufacturing, professional services, retail, and technology.

Decryptor: A tool that transforms data that has been rendered unreadable through encryption back to its unencrypted form.

Indicator of compromise (IoC): An indicator of compromise is described as evidence on a computer that indicates a security breach on networks. IoC data is gathered after the discovery of a suspicious incident.

Kaseya attack: Russian ransomware organization REvil carried out a ransomware attack on information technology management software company Kaseya in July 2021. The managed service provider attack paralyzed as many as 1,500 organizations.

OFAC lists: The US Office of Foreign Assets Control (OFAC) publishes lists of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country specific.

WannaCry attack: A ransomware that contains a worm component, or a self-replicating program that is able to copy and spread itself without the help of any other program. These attacks can slow down network traffic, delete files on a system, or send infected documents by email.

CBDCs: Central bank digital currencies are virtual currencies backed and issued by a central bank.

ABOUT THE AUTHORS

Trent R. Teyema is a former FBI special agent and Senior Executive Service retiree who is an independent consultant advising governments and companies on cybersecurity, infrastructure protection, national security, and technology. His firm specifically focuses on blockchain, cyber physical systems, and space security. Most recently, he was the chief information security officer for Novavax Inc., a COVID-19 biotechnology company; the global head of Cyber Threat Management; a business information security officer for the insurance giant AIG; and the senior vice president and chief technology officer in charge of research and development (R&D) and chair of the Intellectual Property Council for Parsons Corp.

Throughout his thirty-three-year investigative career, he served in numerous senior leadership positions including director of cybersecurity policy for the White House's National Security Council under President Barack Obama, and was detailed under President George W. Bush. He was the special agent in charge of the Cyber and Counterintelligence Divisions for the FBI field office in Los Angeles, and served as the FBI Cyber Division's chief operating officer. In addition, Mr. Teyema founded and led the National Cyber Investigative Joint Task Force, which is one of the US government's seven national cybersecurity centers.

Mr. Teyema is a doctoral candidate in cybersecurity at Marymount University and holds a Master of Forensic Science from The George Washington University. He holds numerous professional certifications in cybersecurity, forensics, and risk.

Kiran S. Jivnani is an assistant director at the Atlantic Council's GeoTech Center. She manages projects at the intersection of geopolitics, security, climate, health, and agriculture. Prior to joining the Atlantic Council, she worked for the United Nations Academic Impact and Millennium Campus Network Millennium Fellowship, where she managed student leaders globally through mentorship on United Nations Sustainable Development Goal-based projects. She later worked for a former member of European Parliament and the Social Democrat Party vice president, Dr. Miriam Dalli. In this role she worked on legislative dossiers of the European Parliament's Environment, Public Health, and Food Safety Committee; Industry, Research, and Energy Committee; and the Beating Cancer Committee. She holds a bachelor's degree from Northeastern University in Boston, where she studied criminal justice, international affairs, and law and public policy.

David A. Bray, PhD, is a distinguished fellow with the Atlantic Council. He is the founding principal at LeadDoAdapt Ventures and has served in a variety of leadership roles in turbulent environments, including bioterrorism preparedness and response with the Centers for Disease Control and Prevention and the broader US government from 2000 to 2005; executive director for a bipartisan US intelligence community commission on R&D; nonpartisan leadership as a federal agency senior executive; work with the US Navy and Marines on improving organizational adaptability; and efforts with US Special Operations Command on the challenges of countering disinformation online. He has received the Joint Civilian Service Commendation Award, Roger W. Jones Award for exceptional federal executive leadership, and the National Intelligence Exceptional Achievement Medal.

He also provides strategy to both boards and start-ups espousing human-centric principles to technology-enabled decision making in complex environments. He was named a senior fellow with the Institute for Human-Machine Cognition, starting in 2018. *Business Insider* named him one of the top "24 Americans Who Are Changing the World" under 40, and he was named a Young Global Leader by the World Economic Forum. He has served in roles such as president, chief strategy officer, and strategic adviser for twelve different start-ups. He has been an invited keynote speaker before audiences of CEOs and world leaders and at events with more than three thousand participants in India, Vietnam, Australia, Taiwan, Dubai, South Africa, Brazil, Colombia, Mexico, Canada, Belgium, Sweden, Switzerland, and the United Kingdom.

ACKNOWLEDGMENTS

The GeoTech Center would like to extend its thanks to the panelists, reviewers, and teammates whose expert insights and support proved invaluable to this project.

Editorial acknowledgments:

Stephanie Wander, *Director of Programs*, GeoTech Center, Atlantic Council

Trey Herr, *Director*, Cyber Statecraft Initiative, Digital Forensic Research Lab, Atlantic Council

Safa Shahwan Edwards, *Deputy Director*, Cyber Statecraft Initiative, Digital Forensic Research Lab, Atlantic Council

Olivia Rowley, *Assistant Director*, Cyber Statecraft Initiative, Digital Forensic Research Lab, Atlantic Council

Emily Sepisco, *Project Assistant*, GeoTech Center, Atlantic Council

Recognition of industry and government panelists:

- US Department of Justice
- Federal Bureau of Investigation
- US Secret Service
- McAfee LLC
- CrowdStrike Services
- Flashpoint
- Accenture
- Intel471
- Blue Ridge Networks
- CrowdStrike Services
- Andreessen Horowitz
- SICPA
- Maximus
- Forward Edge-AI
- System 1, Inc.
- DataPolicyTrust
- Mandiant

Atlantic Council Board of Directors

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org