Joint PIJIP/TLS Research Paper Series

2023

Combating Ransomware: One Year On

V. Gerard Comizio

Gary Corn

William Deckelman

Karl Hopkins

Mark Hughes

See next page for additional authors

Authors

V. Gerard Comizio, Gary Corn, William Deckelman, Karl Hopkins, Mark Hughes, Patrick McCarty, Sujit Raman, Kurt Sanger, Ari Schwartz, Melanie Teplinsky, and Jackson Colling

AMERICAN UNIVERSITY
WASHINGTON
COLLEGE OF LAW

TECH, LAW & SECURITY
PROGRAM

Combating Ransomware: One Year On

V. Gerald Comizio, Gary Corn, William Deckelman,
Karl Hopkins, Mark Hughes, Patrick McCarty,
Sujit Raman, Kurt Sanger, Ari Schwartz, Melanie Teplinsky,
and
Jackson Colling (TLS Student Fellow)

Tech, Law & Security Program
American University, Washington College of Law
January 2023

The Tech, Law & Security Program (TLS)

is a rapidly expanding initiative at the American University Washington College of Law that tackles the challenges and opportunities posed by emerging technologies—offering innovative solutions, engaging our students, and training the leaders of tomorrow.

Working across three key focus areas – Content Regulation in the Digital Age; Privacy, Transparency, and Security; and Cyber & Information Conflict – TLS digs deep into concrete issues through focused projects led by team members with directly relevant experience and expertise. TLS engages closely with the private and public sectors, both domestic and international, to develop impactful, workable solutions to today's most difficult security challenges while ensuring the protection of fundamental rights.

For more information about current TLS initiatives, please visit our website at https://www.wcl.american.edu/impact/initiatives-programs/techlaw/projects/.

Support:

This report was made possible with generous support from Denton's and DXC Technology Company. The content of this report reflects the views of its authors alone. TLS maintains strict intellectual independence and sole editorial discretion and control over its intellectual property, ideas, projects, publications, events and other research activities.

Contents

I. Executive Summary

Ransomware attacks pose a serious risk to businesses, individuals, critical infrastructure, and national security. In the fall of 2021, TLS sponsored "Combating Ransomware," a three-part webinar series that brought together leading experts from government, industry, and academia to discuss the ransomware threat and what should be done about it. The series offered an in-depth look at the ransomware problem, with a specific focus on:

(1) private sector efforts to combat ransomware;
(2) cryptocurrency as a ransomware driver; and
(3) national security aspects of counter-ransomware initiatives.

This paper revisits key ideas from the "Combating Ransomware" webinar series in view of ransomware's evolution over the past year; identifies progress that has been made in the fight against ransomware; and identifies actionable recommendations for the future. These include recommendations designed to strengthen cyber defense, cyber offense, law enforcement efforts, the U.S. cyber incident reporting regime, cryptocurrency efforts, and international efforts.

II. Introduction

"Ransomware" has only recently entered the popular lexicon as operations steadily have become more sophisticated and as certain high-profile operations have grabbed the public's attention. Ransomware blocks access to a computer system, or the files therein, until a ransom has been paid. Although the first known instance of ransomware dates to 1989, ransomware attacks have expanded in scope and complexity over the past decade, becoming a costly threat to the public and private sector alike.[1] New data from the U.S. Department of the Treasury shows that U.S. banks paid out nearly $1.2 billion in 2021 as a result of ransomware attacks.[2] Notably, U.S. critical infrastructure has emerged as a particularly compelling target, with the FBI receiving nearly 650 reports in 2021 alone indicating that organizations belonging to a critical infrastructure sector were victims of a ransomware attack.[3]

In the summer of 2021, the American public experienced the real-world effects of ransomware on critical infrastructure when the cybercriminal group 'DarkSide' targeted Colonial Pipeline, the largest pipeline for refined oil products in the U.S. DarkSide "locked" Colonial's business-side computers and demanded US$4.4 million in Bitcoin to "unlock" them. In response, Colonial, which supplies nearly half of the East Coast's fuel, temporarily shut down its operational technology (OT) systems, halting all pipeline operations. The resulting panic-buying, fuel shortages, and price spikes along the East Coast highlighted the vulnerability of U.S. critical infrastructure to ransomware attacks.

The Colonial shutdown had two important implications. First, it underscored the need for the private sector (particularly private sector owners and operators of critical infrastructure) to be prepared for, and resilient in the face of, a ransomware attack. Second, it prompted a shift in the prevailing mindset. Ransomware operations, once

[1] Kim Grauer, Will Kueshner & Henry Updegrave, THE 2022 CRYPTO CRIME REPORT 38 (2022), https://theblockchaintest.com/uploads/resources/Chainalysys%20-%20Crypto%20Crime%20Report%20-%202022%20Feb.pdf.

[2] FINCEN, U.S. DEP'T OF TREASURY, Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between July 2021 and December 2021 4 (Nov. 1, 2022), (noting that the $1.2 billion figure only reflects data filed with FinCEN and is "not a complete representation of all ransomware attacks or payments").

[3] FBI, U.S. DEP'T OF JUSTICE, 2021 INTERNET CRIME REPORT 15 (2021).

largely considered the province of law enforcement, are now more broadly understood to pose a potential national security threat, as well. This shift has triggered the devotion of additional attention and resources to the problem.

Ransomware operations have continued to evolve since the Colonial incident, and they continue to pose a serious threat to U.S. economic and national security. In the year that has passed since TLS's "Combating Ransomware" webinar series, important steps have been taken to combat ransomware, but much work remains to be done. While the ransomware threat is unlikely to be completely eliminated, there are a number of additional steps that government and private actors can take to effectively combat it.

This paper will (1) introduce the concept of ransomware (Section III) and identify current ransomware trends (Section IV); (2) explore ransomware from a private sector (Section V) and national security perspective (Section VI); (3) provide a brief snapshot of current government actions (Section VII); and (4) offer concrete recommendations for action (Section VIII).

III. What is Ransomware?

Ransomware is targeted malicious software used to "lock up" a computer system, or the files thereon, rendering the computer unusable or its information inaccessible until a ransom is paid. Ransomware operations primarily are conducted by criminal actors for financial gain. However, some nation-states are known to use them as well, in an effort to seek geopolitical advantage. In some cases, these nations even harbor or provide support to criminal groups as part of a "blended" threat combining state resources with criminal expertise. Whatever the background circumstances, the actor tends to be jurisdictionally dislocated from target computers or systems and often uses the infrastructure of third-party nation-states to launch the ransomware, further complicating both the attribution analysis and the response framework. Russia, in particular, serves as a hotbed for criminal ransomware organizations, such as DarkSide and Conti, that target Western companies and governments.

Ransomware operations typically follow a particular sequence, although there are some deviations. First, the ransomware operator must obtain access to the victim's network. This can be achieved in a variety of ways, including through phishing, malware, or exploitation of stolen credentials.[4] Once access is gained, the actor probes the victim organization's system(s) to find, access, encrypt (and in some cases, exfiltrate) high-value data. Traditionally, the threat actor demands a ransom in exchange for restoring the victim's access to the encrypted data. Increasingly, ransomware operators threaten to sell or leak the stolen data if their ransom demand is not met. Criminal ransomware operators generally demand ransom be paid in cryptocurrency because cryptocurrency transactions are fast, cheap, liquid and are perceived, sometimes erroneously, to be difficult to trace—features that can make it easier to collect and launder ransom payments. Indeed, over $600 million in cryptocurrency have been tied to 2021 ransomware payments,[5] representing a fraction of the overall ransomware payments effected with cryptocurrencies.

IV. Trends in Ransomware Operations

Overview

Today's ransomware landscape has continued to evolve since TLS's "Combating Ransomware" webinar series one year ago. In 2021, notable ransomware trends included increased frequency and sophistication of attacks; extortion; targeting of high-profile entities (including critical infrastructure); and increased payouts.

Over the past year, new trends have also emerged. As discussed in more detail below, attack frequency reportedly has decreased; the rapidly growing cyber insurance market has seen increasing premiums and reduced coverage; the types of attacks and the entities most regularly targeted have shifted; and the payout system has been impacted by a number of factors, including increased regulatory attention and the spring 2022 crypto market crash.

[4] Some ransomware groups reportedly recruit insiders in order to deploy malware more quickly and with a greater chance of evading detection. *See* Vilius Petkauskis, Cybercriminals Push to Recruit Insiders for Ransomware Attacks, CyberNews (Mar. 14, 2022); Bill Toulas, Ransomware Gangs Increase Efforts to Enlist Insiders for Attacks, BLEEPING COMPUTER (Jan. 24, 2022).

[5] *See* Adam Janofsky, Ransomware victims paid more than $600 million to Cybercriminals in 2021, THE RECORD BY RECORDED FUTURE (Feb. 10, 2022); (Conti, the top grossing ransomware operator in 2021, extorted $180 million from victims, including "9-1-1 dispatch centers, municipalities, and emergency medical services." That same year, Darkside, the group alleged to have perpetrated the Colonial Pipeline attack, brought in $85 million).

Moreover, as explained in more detail below, domestic and international events——
particularly Russia's invasion of Ukraine and new legislation and policy in the U.S.——
have presented new challenges and opportunities.
Despite these shifts, ransomware remains a serious threat to American businesses and national security.

Specialization

In line with recent trends, ransomware operations continue to become increasingly specialized and segmented. Often, they are conducted not by one individual, but by a syndicate comprised of actors either working in tandem or contributing piecemeal to the overall operation. These actors are increasingly specialized in their ability to conduct specific stages of ransomware operations. Some create, market, and sell ransomware tools. Others, known as 'initial access brokers,' broker access to victim networks by, for example, selling stolen credentials or conducting reconnaissance to identify vulnerable networks and then selling cybercriminals access to those networks. [6] This specialization allows individuals to build their expertise and market their products and services, leading to larger, more sophisticated, and more effective ransomware operations.

> *"ransomware trends include increased …sophistication of attacks; [multi-extortion ransomware] … and increased payouts"*

Cyber-criminal organizations recruit individuals who specialize in specific aspects of ransomware operations to maximize impacts.[7] They recruit individuals who specialize in malware writing, infiltration, encryption, maintaining access to systems, negotiation, and more.[8] Fragmentation and specialization make it easier and faster for cybercriminals to carry out ransomware operations as the tools are readily available and more effective, resulting in a faster pace of attack and higher payouts. Fragmentation and specialization also have led to the proliferation of "Ransomware-as-a-Service" (RaaS), [9] a criminal business model in which ransomware is packaged and sold for use. RaaS is a subscription-based revenue model (similar to "Software as a Service") in which

[6] Nicole Sette, et al., Initial Access Brokers: Fueling the Ransomware Threat, KROLL (Sept. 23, 2021),

[7] Matthew J. Schwartz, Eyeing Bigger Targets, Ransomware Gangs Recruit Specialists, BANK INFO SECURITY (Sept. 9, 2020),

[8] Alex Scroxton, Ransomware Gangs Seek People Skills For Negotiations, COMPUTER WEEKLY (Jul. 9, 2021),

[9] Kurt Baker, Ransomware As A Service (RAAS) Explained, CROWDSTRIKE (Feb. 27, 2022),

affiliates pay a fee[10] to launch ransomware attacks developed by ransomware operators. The RaaS market is intensely competitive and functions like a legitimate market would, mirroring the fact that RaaS organizations are adopting the processes of legitimate businesses: recruiting talent, paying salaries and bonuses, and evaluating the performance of employees.

Moreover, RaaS is a resilient and internally diverse ecosystem. Ransomware groups often rebrand by deploying new ransomware strains or, like the elite ransomware group Conti, break up and work with other groups, thereby bolstering and diversifying their capabilities.[11] Indeed, cutting-edge groups like Conti have shown an ability not only to adapt to, but also to shape, emerging labor-market trends. According to blockchain analytics firm TRM Labs, "unlike most ransomware syndicates, Conti implements a model of wage-based employees [different from] the percentage-based affiliate model used by traditional RaaS groups."[12] It appears Conti can do this because it has successfully built up an operation on "an industrial scale, bringing things like gaining [unauthorized network] access and distribution of malware in-house,"[13] which has netted the group hundreds of millions of dollars in total victim payments. Thus, unlike "several other ransomware groups [that] have struggled to keep up with all of the entities they have gained access to or to develop an effective pipeline of accesses"[14]—which therefore requires those groups to partner with affiliates and to share significant percentages of their illicit profits—Conti's superior business organization allows the group to pay salaries that are "nearly two times higher than the average salary in the IT industry in Russia,"[15] while still allowing its core members to keep the vast percentage of ransom payments for themselves.

Prevalence of Attacks

2021: Ransomware attacks increased significantly in 2021. A range of factors contributed to the rise in attacks, including: (1) a marked increase in cyber insurance uptake with insured businesses becoming prime targets for cybercriminals (see 'Cyber Insurance' section below); (2) cybercriminals' increased specialization in the stages of ransomware operations, which facilitated

[10] The fee can take one of several forms, including a monthly subscription fee, a monthly subscription fee with profit sharing (in which part of the ransom proceeds are paid to the ransomware operators), or a one-time license fee. *Id.*

[11] Emilio Iasiello, Is the Conti Ransomware Gang Stronger Apart Than Together?, OodaLoop (May 23, 2022),

[12] TRM Analysis Corroborates Suspected Ties Between Conti and Ryuk Ransomware Groups and Wizard Spider, TRM Insights, (Apr. 6, 2022)

[13] *Id.*

[14] *Id.*

[15] *Id.*

a faster pace of attacks and higher payouts (discussed above); and (3) a strong uptick in remote work spurred by the coronavirus pandemic, which dramatically increased the range of targets for cybercriminals as a significant portion of the workforce labored from home without adequate cyber defenses (by, for instance, working on their own devices without the safeguards of a corporate network).

2022: Reports suggest ransomware attacks on U.S. entities declined in 2022 as compared with 2021.[16] Reports indicate that the first quarter of 2022 saw more ransomware attacks than the same period in 2021; the second quarter of 2022 experienced a drastic decline compared to the same period in 2021;[17] and the number of ransomware attacks in the third quarter of 2022 fell by 8% compared with the same period in 2021.[18]

Among the potential factors driving the seeming decline in ransomware attacks are (1) the Russian invasion of Ukraine and enhanced sanctions on states friendly to cybercriminals; (2) the crypto market crash; and (3) a lack of reporting.

1. Russia's Invasion of Ukraine/Enhanced Sanctions

The vast majority of ransomware attacks emanate from Russia and are perpetrated by groups that have pledged their allegiance to Russia. With Russia's invasion of Ukraine in February 2022, these cybercriminals may have shifted attention away from Western targets and focused on supporting the Russian war effort.

Another element of Russia's invasion is the Western sanctions regime placed on Russia. As discussed in more detail below, these sanctions have made it much harder for Western entities to pay ransoms as the ransomware operators are likely sanctioned, thus creating great disincentives for Western entities to facilitate such payments in the first place.

2. Crypto Market Crash

The recent crash in the cryptocurrency market also may be playing a role in the seeming decline in ransomware attacks. Cybercriminals tend to utilize cryptocurrency to facilitate ransomware payouts as opposed to cash or dollar transactions due, among other things, to the perception that cryptocurrency is difficult to trace. However, with crypto's rapid devaluation, cybercriminals are likely having to shift tactics and reevaluate their operations.

[16] Tim Starks, Is the Drop in Ransomware Numbers An Illusion, WASHINGTON POST (Aug. 17, 2022).

[17] Crystal Kim, Ransomware Attacks Decline Amid Crypto Downturn, AXIOS (Jul. 27, 2022).

[18] Third Quarter of 2022 Reveals Increase in Cyberattacks, CHECK POINT RESEARCH.

3. Lack of Reporting

Finally, some posit that only the *reporting* of ransomware attacks has declined, not the actual number of attacks. As will be discussed in the next section, cybercriminals appear to be shifting from high visibility, high impact targets to targets that can be hit with less societal impact and less government scrutiny.

These targets may be less likely to report ransomware attacks and simply may pay the ransom and continue operations instead of involving the government. Reporting is only as good as the information that supports it. Thus, our understanding of ransomware's prevalence in certain sectors may be based on incomplete data, which may not be wholly accurate and could even be misleading.

In our experts' views, ransomware is here to stay. Any decline in the prevalence of ransomware attacks is likely only a temporary reprieve from the onslaught experienced in 2021. Ransomware has steadily increased over the years as the world has become ever-more digitized, and that overall trend is likely to continue.

Cyber Insurance

"Cyber insurance is the fasting growing product segment in the U.S. property/casualty (P/C) insurance market."[19] Between 2016 and the end of 2020, businesses opting for cyber insurance nearly doubled.[20] While such insurance helps to protect businesses, it also makes them prime targets for cybercriminals, who often use insurance policies as bargaining chips to obtain a payout. Given the massive increase in ransomware attacks in 2021, businesses have seen cyber insurance premiums rise sharply and policy coverages shrink, especially for high-risk entities in academia, healthcare, and the public sector.[21]

However, recent reporting suggests that the federal government may be wading into the cyber insurance market. The U.S. Department of the Treasury and the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) have been probing industry stakeholders about the need for a federally-backed cyber insurance program to deal with "catastrophic" cyber incidents.[22] The Treasury Department officially published a request for comment on September 29,

[19] U.S. Cyber Insurance Sees Rapid Premium Growth, Declining Loss Ratios, FitchRatings (Apr. 13, 2022).

[20] Rising Cyberthreats Increase Cyber Insurance Premiums While Reducing Availability, GAO (Jul. 19, 2022).

[21] *Id.*

[22] Ines Kagubare, Federal Government Considers Sharing Costs for 'Catastrophic' Cyber Incidents, The Hill (Oct. 9, 2022).

2022 to solicit feedback about a potential federal insurance response to ransomware.[23] With the rising costs of premiums and the increasing difficulty for some entities to obtain cyber insurance due to the likelihood of a cyber incident, a federally backed cyber insurance program may provide a necessary backstop. However, implementation challenges include: defining the parameters of a qualifying cyber incident, avoiding moral hazard (e.g., by mandating minimum cyber hygiene practices), and potentially determining an entity's importance to overall U.S. economic health and security.[24] The extent to which a state-sponsored ransomware attack is considered an "act of war" excluded from cyber insurance coverage (a question made ever more pressing by Russia's invasion of Ukraine) raises an additional question of the scope of private insurance and of a possible federal insurance program.

The proliferation of cyber insurance policies, and payouts from such policies, has led to professionalization of another aspect of the ransomware ecosystem, with vendors assisting victim businesses to negotiate and recover from attacks.[25] The Treasury Department's Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN) have issued guidelines on handling ransomware payouts, reiterating to businesses of the dangers of running afoul of U.S. sanctions regimes by paying sanctioned entities, and outlining the penalties associated with such violations.[26] While it does not appear that any enforcement actions have yet been brought by the U.S. government in connection with a victim's payment of a ransom to a sanctioned individual or entity, the coordinated release of guidance by both OFAC and FinCEN has indisputably caught industry's attention and will almost certainly influence behavior going forward.

Targets

Ransomware has become a highly effective means of pursuing interests for cybercriminals, as well as for nation-states acting through cybercriminals. To that end, the scope of targets has broadened to include not just businesses, but also hospitals, schools,

[23] Request for Comment on Potential Federal Insurance Response to Catastrophic Cyber Incidents, 87 Fed. Reg. 59161 (Sept. 29, 2022).

[24] The request for comment lays out these potential issues and dives deeper into the many other issues that Treasury aims to scrutinize in connection with a federally-backed cyber insurance program. *See* DEP'T OF TREASURY, *Potential Federal Insurance Response to Catastrophic Cyber Incidents*, FED. REGISTER (SEPT. 29, 2022).

[25] Jordan Robertson, Ransomware Negotiation Evolves, As Victims Hope for Discounts, BLOOMBERG (Jun. 15, 2022).

[26] Dept. of Treasury, Off. Of Foreign Asset Controls, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (2021);Dept. of Treasury, Fin. Crimes Enf't Network, FIN-2021-A004, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransomware Payments (2021).

cities, and critical infrastructure. 2021 illustrated this trend as cybercriminals targeted numerous high-profile businesses.[27] Attacks on critical infrastructure and supply chains were especially noteworthy, enabling cybercriminals to strike major blows to U.S. industry, often doing so in support of a nation-state, while also increasing the likelihood of receiving larger ransom payments. Often overlooked is ransomware's potential to be used as a form of punishment that might be misinterpreted as a purely cybercriminal act, as illustrated by Russia's deployment of NotPetya against Ukraine in 2017.[28] Deployment of ransomware for this purpose is not limited to nation-states; competitors and disgruntled insiders can do this as well.

While the high-profile ransomware operations of 2021 proved lucrative, they drew plenty of attention from U.S. and international law enforcement. This may be one reason why ransomware attacks appear to have shifted from high-profile private sector and U.S. government targets in 2021 to lower-profile targets with fewer protections and U.S. government connections in 2022. In a summer 2021 interview, an alleged member of the so-called BlackMatter ransomware group specifically said the group would avoid targeting critical infrastructure and attracting "unwanted attention" from the U.S. He indicated that some industries were "off-limits" (including healthcare, critical infrastructure, oil and gas, defense, non-profits, and government organizations) and that BlackMatter would instead target companies with annual revenues of more than $100 million.[29] Notwithstanding these comments, certain critical infrastructure sectors, such as transportation and shipping, have since seen an increase in ransomware attacks in the third quarter of 2022 when compared to previous quarters.[30] This seeming contradiction is indicative of the expansive nature of the cybercriminal environment and reflects the fact that cybercriminals may vary greatly in terms of their operational objectives.

Another reason why ransomware attacks appear to have shifted away from victimizing high-profile targets is that

[27] Victims included Colonial Pipeline, JBS (which operates plants that process about 1/5 of the U.S. meat supply), CNA Financial (one of the largest insurance companies in the U.S.), and Kaseya Limited (a U.S. software provider) as well as numerous entities in the healthcare sector, academia, and government offices.

[28] Ellen Nakashima, Russian Military Was Behind NotPetya Cyberattack in Ukraine, CIA Concludes, WASHINGTON POST (Jan. 12, 2018).

[29] Dmitry Smilyanets, An Interview with BlackMatter: A New Ransomware Group That's Learning From the Mistakes of DarkSide and REvil, THE RECORD BY RECORDED FUTURE (Aug. 2, 2021).

[30] Alfred Alvarado, *et al.*, The Threat Report Fall 2022, TRELLIX ADVANCED RESEARCH CENTER (2022), (ransomware activity in the U.S. shipping and transportation industries doubled from second to third quarter of 2022). The healthcare industry saw an increase in ransomware attacks in the second quarter of 2022 as compared with previous quarters. *See* Laurie Iacono, *et al*., *Q2 2022* Threat Landscape: Ransomware Returns, Healthcare Hit, KROLL (Aug. 10, 2022).

potential targets have likely heeded the call to harden their cyber defenses.[31] The vast majority of ransomware attacks are opportunistic, not targeted. Operators constantly scan the internet for vulnerable targets and strike if the opportunity is right.[32] When a vulnerability is found, operators exploit it to gain access to the victim's network and assess that victim's potential value, and then launch their ransomware. As ransomware has gained greater attention as a threat to national and economic security, many high-profile victims have increased their focus on cyber defenses, potentially forcing cybercriminal groups to shift to smaller, more vulnerable targets.

Payouts

Even as reported attack numbers declined in 2022, ransomware payouts have been increasing in size.[33] One reason for the increase in payouts is the increased professionalization of the ransomware ecosystem, as described above, which has resulted in a surge in detected RaaS attacks. As ransomware has become more common, businesses have sought financial protection through insurance coverage. Insurance coverage is a factor that cybercriminals look for when conducting reconnaissance of a business's operating systems because it provides leverage in negotiation and permits them to adjust their ransom demands according to the insurance policy.[34] Many businesses would rather pay the ransom and have their data returned, systems unlocked, and receive an insurance reimbursement, than lose critical data. This helps explain why ransomware insurance premiums have risen drastically in recent years as have insurance reimbursements to victims.[35]

Cryptocurrency is an important ransomware driver because cryptocurrency transactions are fast, easy, and are perceived (often mistakenly) to be difficult to trace. This helps cybercriminals conceal their identities and avoid detection by government and law enforcement while helping victims pay ransoms more easily. Cryptocurrencies eliminate the need for trusted third parties (e.g., banks) to verify transactions or to serve a financial surveillance function. Notably, a subset of cryptocurrencies known as "privacy coins" are specifically designed to

[31] Statement by President Biden on Our Nation's Cyberdefenses (Mar. 21, 2022) (urging private sector critical infrastructure owners and operators to "harden [their] cyber defenses immediately").

[32] Ransomware: Facts, Threats and Countermeasures, CENTER FOR INTERNET SECURITY.

[33] Ryan Olsen, *Average Ransom Payment Up 71% This Year, Approaches $1 Million*, PALO ALTO NETWORKS (Jun. 7, 2022). This varies, however, according to who is providing data and who has access to data. This is due to a lack in reporting of ransomware events from entities of all sizes, resulting in potentially skewed data which, at times, makes it difficult to ascertain a precise picture of the ransomware landscape.

[34] Josephine Wolff, As Ransomware Demands Boom, Insurance Companies Keep Paying Out, WIRED (Jun. 12, 2021).

[35] *Id.*

frustrate the blockchain's inherent traceability (e.g., by employing cryptography to conceal the sender's and recipient's identities). While privacy coins may have certain legitimate uses, especially considering public blockchains' otherwise transparent nature, they have also become popular among illicit actors, including cybercriminals. Criminals also utilize foreign centralized exchanges and mixing services to "launder" the crypto proceeds of their ransomware attacks and convert it into fiat currency. Despite the convenience of crypto in facilitating ransomware payments, crypto as a ransom payment method is facing intense pressure from markets and scrutiny from government actors, including regulators and law enforcement.[36] In 2021, cryptocurrency was the most popular medium for ransomware payouts as cryptocurrency market values soared, but 2022 has proven to be a much different environment.

A sudden crypto market crash in May 2022 caused over $2 trillion in cryptocurrency value to be lost in a matter of months, with severe devaluations in cryptocurrencies across the board. Cybercriminal groups may now be less willing to collect ransoms in crypto out of fear of large devaluations.

> "... crypto as a ransom payment method is facing intense pressure from markets and scrutiny from government actors, including regulators and law enforcement."

Additionally, U.S. regulators have been scrutinizing cryptocurrency intermediaries for their role in facilitating criminal behavior. OFAC designated virtual currency exchange SUEX in September 2021 for facilitating financial

[36] U.S. lawmakers actively have been pursuing crypto regulation for some time, and calls for regulation have only intensified in the wake of FTX's dramatic collapse. In June 2022, Senators Cynthia Lummis (R-WY) and Kirsten Gillibrand (D-NY) proposed the Responsible Financial Innovation Act, a comprehensive bill to regulate crypto. In August 2022, Senators Debbie Stabenow (D-MI) and John Boozman (R-Ark) introduced the Digital Commodities Consumer Protection Act (DCCPA), a more limited bill designating the CFTC as the lead regulator for crypto. While the viability of DCCPA is uncertain, in no small part due to its association with former FTX CEO Sam Bankman-Fried and his lobbying efforts on its behalf, several lawmakers have publicly indicated that FTX's collapse has reinforced the perceived need for additional federal oversight in the crypto industry. Separately, the SEC has stepped up its scrutiny of crypto by nearly doubling the size of its "Crypto Assets and Cyber Unit." In the EU, the Markets in Crypto Assets (MICA) regulation, set to take effect in 2024, sets forth a regulatory framework intended to protect investors, enhance protections against money laundering, and preserve financial stability.

transactions for ransomware actors.[37] In April 2022, OFAC sanctioned both Hydra Market, the world's "largest and most prominent darknet market," as well as the virtual currency exchange Garantex for allowing their systems to be abused by illicit actors.[38]

Mixing and tumbling services, which are used to obscure the source of cryptocurrency funds,[39] also have come under intense scrutiny from regulators in the U.S. and abroad. While mixing services may offer a degree of financial privacy to legitimate actors, they also pose a significant money laundering risk.[40] In a first-of-its-kind action in 2019, Dutch authorities seized and shut down the Bestmixer.io cryptocurrency mixer for allegedly laundering over $200 million in cryptocurrency.[41] OFAC subsequently sanctioned mixing service Blender.io in May 2022, alleging that North Korea used the service to support malicious cyber activities and launder stolen virtual currency.[42]

Just a few months later, in what has since become a highly controversial move, OFAC sanctioned virtual currency mixer Tornado Cash for allegedly laundering over $7 billion in virtual currency.[43] OFAC alleged, among other things, that Tornado Cash was a key money laundering tool for North Korean state-sponsored hackers that pose a threat to U.S. national security and "repeatedly failed to impose effective controls designed to stop [Tornado Cash] from laundering funds for malicious cyber actors on a regular basis."[44]

Unlike traditional mixers, Tornado Cash is decentralized, meaning that it operates through so-called "smart contracts" that automatically move crypto based on specified rules coded into software. Accordingly, OFAC's

[37] Dep't. of Treasury, Off. Of Foreign Asset Controls, *supra* note 26.

[38] Dep't of Treasury, Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex (2022).

[39] Anonymizing services such as mixers and tumblers essentially make it more difficult to track crypto funds (e.g., by allowing many users to pool cryptocurrency funds, mix them, and then withdraw from the pool the amount deposited).

[40] FinCEN has identified transactions that "make[] use of mixing and tumbling services" as one of several "red flag" indicators that can be used to identify cryptocurrency activity linked to illicit conduct. Dept. of Treasury, Fin. Crimes Enf't Network, FIN-2019-A003, Advisory on Illicit Activity Involving Convertible Virtual Currency (2019. Comprehensive digital asset market structure legislation introduced in the U.S. House of Representatives in July 2021 would require FinCEN to engage in a formal rulemaking process which would address anonymizing services, including mixing and tumbling services. *See*, H.R. 4741, the Digital Asset Market Structure and Investor Protection Act, Section 402.

[41] Charlie Osborne, Bestmixer seized by police for washing $200 million in tainted cryptocurrency clean, ZDNet (May 23, 2019).

[42] Dep't of Treasury, U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats (2022).

[43] According to a subsequent industry report, only $1.5 billion of the $7.6 billion was from illegal activity. Tornado Cash Mixer Sanctioned After Laundering Over $1.5 Billion, Elliptic (Aug 8, 2022).

[44] Dep't of Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug 8, 2022).

sanctions targeted these "smart contracts" as well as the crypto wallets associated with Tornado Cash.

OFAC's sanctions against Tornado Cash have been a source of significant controversy, with leading crypto advocates such as Coinbase and Coin Center suing and/or funding lawsuits against OFAC. These suits allege, among other things, that OFAC's designation of Tornado Cash exceeded its authority because Tornado Cash is a software privacy tool and not a person or entity properly subject to sanctions; that OFAC's sanctions criminalizing use of Tornado Cash mixing services unlawfully infringe on Tornado Cash users' First Amendment rights to associational privacy; and that OFAC violated Fifth Amendment due process rights when it froze assets without notice, leaving some plaintiffs' crypto locked in Tornado Cash.[45] In September, OFAC attempted to address several of these issues in "FAQs" posted to its website.[46] Not long after, in November 2022, OFAC deemed its original sanctions designation of Tornado Cash inoperative and simultaneously "redesignated" Tornado Cash (not on the grounds that the mixing service supported North Korean hackers, but on the grounds that North Korea used the mixing service to support its weapons of mass destruction program).[47] How OFAC's recent actions will affect the pending legal challenges to OFAC's original designation of Tornado Cash remains to be seen. But one thing is clear: taken together, recent regulatory actions against cryptocurrency mixers, including Tornado Cash, serve as a strong reminder that regulators are committed to preventing cryptocurrency from being used to facilitate illicit activity. Western sanctions complicate the ransomware landscape for malign actors, making it more difficult for ransomware operators to "extract funds out of the ecosystem."[48] Meanwhile, as described above, victims–and entities that facilitate ransomware payments–can face severe civil and criminal penalties for running afoul of the sanctions regime by paying a sanctioned entity, even if they did not know, and had no reason to know, that the payee was sanctioned.[49]

Multi-Extortion Ransomware

Ransomware attacks skyrocketed in 2021. During traditional ransomware

[45] Coin Center Is Suing OFAC Over Its Tornado Cash Sanction, COIN CENTER (OCT 12, 2022).
[46] DEP'T OF TREASURY, Frequently Asked Questions (2022).
[47] Dep't of Treasury, Treasury Designates DPRK Weapons Representatives: Tornado Cash Redesignated with Additional DPRK Authorities, New OFAC Guidance (Nov. 8, 2022).
[48] Payton Doyle, How Russian Sanctions May Be Helping US Cybersecurity, TECHTARGET (Jun. 14, 2022).
[49] DEP'T OF TREASURY, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (2021). *See also*, Faegre Drinker Biddle and Reath LLP, Ransomware Payments Become and Even Riskier Choice Amidst the Ever-Growing Sanctions List, JDSUPRA (Jul. 18, 2022).

attacks, cybercriminals would encrypt information on a victim's operating system and demand a ransom in exchange for a decryption key. However, in 2021, cybercriminals adapted their techniques. Cybercriminals more frequently utilized double extortion methods where they would encrypt a company's data, exfiltrate that data, and threaten to not only withhold it from the victim, but to leak the data to the public or sell it on the dark web if the ransom was not paid.[50] Exploitation of dark web sales demonstrates criminals' adaptability to countermeasures and their ability to identify revenue opportunities beyond their initial aims. Double extortion operations proved more popular in 2021 than traditional ransomware, as it is estimated that over 70% of ransomware incidents in the fourth quarter of 2020 involved double extortion (up from 50% during the third quarter of 2020).[51] Double extortion has essentially neutralized the practice of using backup data storage to avoid having to pay a ransom because victims now have to contend with the additional threat of their sensitive information being leaked to the world. Cybercriminals continually are adapting their practices to extort more money. For example, with "triple extortion," cybercriminals not only extort the original victim, but also those who may be impacted by the release of the exfiltrated data (e.g., the company's clients), thus radically expanding the field of potential ransom payments.[52]

"Cybercriminals continually are adapting their practices to extort more money."

In some cases, triple extortionists also have attacked the reputation of the victim company by telling the company's clients that they would not have become victims had the company paid the requested ransom. Cybercriminals also have threatened to level distributed denial-of-service (DDoS) attacks against the original victim if that victim does not cooperate in order to further pressure the victim into payment.[53] As cybercriminals have fine-tuned their tactics to extort more money, the overall cost of ransomware attacks has increased even as the overall number of reported ransomware attacks has declined.

[50] 2021 Trends Show Increased Globalized Threat of Ransomware, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (Feb. 10, 2022).

[51] *Ransom Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands*, COVEWARE (Feb. 1, 2021).

[52] Natalie Paskoski, What are Double and Triple Extortion Ransomware Attacks?, RETAIL AND HOSPITALITY ISAC, (Feb. 16, 2022).

[53] Triple Extortion Ransomware: The DDoS Flavour, PACKETLABS (May 12, 2022),

V. Private Sector and Ransomware

This section will address ransomware's impacts on the private sector and the actions the private is taking, and needs to take, to address these impacts.

> *"Ransomware poses a significant threat to businesses of all types and sizes."*

Impact on the Private Sector

Ransomware poses a significant threat to businesses of all types and sizes. In 2021, cybercriminals targeted companies where they had the greatest leverage and could receive the highest payouts. These targeted businesses often had the money to pay ransoms but lacked the cyber resources to stave off and weather ransomware attacks. Examples include Colonial Pipeline, which paid around $4.4 million in ransom, JBS, which paid around $11 million in ransom, CNA Financial, which paid a ransom of over $40 million, and numerous healthcare providers.[54]

Reporting Requirements

Reporting requirements and the potential for prohibitions on ransom payments complicate matters for private sector ransomware victims. Private sector companies with the resources to pay a ransom may wish simply to do so, recover their data or regain access to their systems, and move on. Businesses may be hesitant to report ransomware attacks (or payments) where they are able to pay the ransom because they seek to continue operations, limit the government's involvement in their businesses, and avoid inadvertently providing the government with evidence that a law or regulation has been violated. For the same reasons, businesses may oppose restrictions/prohibitions on ransom payments. Businesses also may be hesitant to make public disclosures alerting shareholders and customers to ransomware attacks, to avert stock

[54] Maggie Miller, *Oversight Finds Small Lapses In Security Led to Colonial Pipeline, JBS Hacks*, THE HILL (Nov. 16, 2021), https://thehill.com/policy/cybersecurity/581800-house-oversight-panel-finds-that-small-lapses-in-security-led-to-recent/; Scott Ikeda, *Colonial Pipeline May Face $1 Million Penalty for Operational Lapses in 2021 Ransomware Attack*, CPO MAGAZINE (May 12, 2021), https://www.cpomagazine.com/cyber-security/colonial-pipeline-may-face-1-million-penalty-for-operational-lapses-in-2021-ransomware-attack/.

drops, consumer panic, and reputational harm.

Although most companies are not obligated to report cyber incidents to the federal government, some are. For example, defense contractors are required to report cyber incidents within 72 hours of discovery.[55] Cloud service providers operating systems on behalf of federal agencies are required to report cyber incidents to affected customers and the U.S.-CERT within one hour of discovery.[56] Critical pipeline owners and operators are required to report confirmed and potential cybersecurity incidents to CISA.[57] Public companies also have certain disclosure obligations associated with material cybersecurity incidents.[58]

Critical infrastructure owners and operators are required to report certain cyber incidents to CISA within 72 hours and to report ransomware payments to CISA within 24 hours pursuant to the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), which President Biden signed into law in March, 2022. The stated aim of the bill, according to CISA, is to "allow CISA to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims."[59] Indeed, these requirements are intended to give the government greater visibility into the ransomware threat; allow attack parameters to be shared (e.g., through JCDC) to facilitate better overall defense; and potentially enable operational agencies (e.g., FBI and U.S. Cyber Command) to disrupt ongoing attacks.

CIRCIA is the first statutory cyber incident reporting requirement directed at critical infrastructure owners and operators.[60] The law specifies that "covered entities" report "covered cyber incidents" to CISA within 72 hours and ransomware payments to CISA within 24 hours. CISA, which is charged with implementing CIRCIA's reporting requirements, has up to two years to issue a notice of proposed rulemaking, and 18 months after that to issue final rules. Already CISA has requested public input on a number of issues,[61] including: the scope of "covered entities" and "covered cyber incidents;" and what constitutes a "reasonable

[55] Defense Federal Acquisition Regulation Supplement, 252.204-7012 (Oct. 28, 2022).
[56] FEDRAMP INCIDENT COMMUNICATIONS PROCEDURES, FEDRAMP 6 (2021).
[57] DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators, DEP'T OF HOMELAND SECURITY (Jul. 20, 2021).
[58] CF Disclosure Guidance, Topic No. 2 Cybersecurity, SEC DIVISION OF CORPORATION FINANCE (Oct. 13, 2011).
[59] *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*, Cybersecurity Infrastructure Sec. Agency https://www.cisa.gov/circia.
[60] Ankura, CISA to Oversee Enforcement of Cyber Incident Reporting in Critical Infrastructure, JD SUPRA (Sept. 29, 2022).
[61] Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022, 87 Fed. Reg. 55833 (Sept. 12, 2022).

belief" that a cyber incident has occurred so as to trigger a reporting obligation. Properly crafted, the final regulation will provide much-needed clarity, and simplified compliance, for the private sector in what has become an increasingly complex reporting environment characterized by a patchwork quilt of requirements. The private sector should seize the opportunity to help shape CISA's reporting rules to ensure that they function effectively to foster timely and accurate reporting while minimizing the burden on businesses.

> *"The private sector should seize the opportunity to help shape CISA's reporting rules to ensure that they function effectively to foster timely and accurate reporting while minimizing the burden on businesses."*

Finally, public companies may soon be subject to new cyber risk disclosure requirements. For over a decade, the SEC has required public companies to disclose certain "material" cybersecurity risks.[62] Last spring, just one week before CIRCIA was signed into law, the SEC proposed new cybersecurity risk disclosure requirements for public companies.[63] Citing "growing concerns" that material cyber incidents are underreported and that reporting may not be sufficiently timely, the SEC's newly proposed rule requires public companies to report a "material" cyber event on a publicly available 8-k form within four days.[64]

While intended to enhance cybersecurity, such requirements could have unintended consequences. Requiring immediate disclosure of a cyber incident could: interfere with coordinated public-private efforts to remediate, disrupt or otherwise address a cyberthreat; undermine an active law enforcement investigation, hindering efforts to apprehend cybercriminals and prevent further incidents; or result in public reporting of a vulnerability before appropriate remedial measures (e.g., patching) have been taken to prevent exploitation of that vulnerability.[65] Regulators should carefully craft disclosure requirements to avoid such results.

[62] SEC DIVISION OF CORPORATION FINANCE, *supra* note 58.
[63] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 17 C.F.R. 229, 232, 239, 240, & 249 (proposed Mar. 9, 2022).
[64] *Id.*
[65] Sasha Hondagneu-Messner, Steve McInerney, & Alan Charles Raul, Cyclops Blink' Shows Why the SEC's Proposed Cybersecurity Disclosure Rule Could Undermine the Nation's Cybersecurity, LAWFARE (Aug. 30, 2022).

Prevention, Mitigation, and Response

Businesses can and should take a range of measures to protect themselves from ransomware. Two critical preventive measures are vulnerability management and multi-factor authentication (MFA). In the first quarter of 2021, 63% of successful ransomware attacks leveraged vulnerabilities in internet facing devices and another 23% relied on compromised credentials.[66] Identifying and addressing vulnerabilities (e.g., through patching) and effective MFA could have prevented those attacks.

Beyond basic cyber hygiene, the most important measure is to be proactive in achieving cyber security and resilience. Among other things, this requires beginning the more difficult, but essential, work of migrating toward zero trust ("never trust, always verify") architectures. There is no one-stop shop where organizations can "buy" zero trust; rather, zero trust is an approach to cyber security whose success requires sustained commitments of time and resources. (Resilience also requires preparing for the quantum threat. [67] As with zero trust, there is no one-stop shop for future-proofing against quantum capabilities, but many organizations already are, or should be, working to ensure quantum cyber readiness.[68])

One critical aspect of zero trust is phishing-resistant MFA. Businesses should aim to implement phishing-resistant MFA to prevent this source of infiltration. By preventing access to networks via credential abuse, businesses greatly reduce the risk of becoming victims of ransomware as cybercriminals will likely move on to an easier target given that cybercriminals are mainly opportunistic.

To reduce the risk of harm from a ransomware attack, businesses should invest in isolated backups that can assist in data recovery efforts and develop a restoration plan for how to utilize and implement those backups. Businesses must rehearse for a ransomware attack (e.g., tabletop exercises can be used to test a business' incident response plan) so that when one does occur, they are not caught flat footed. In this regard, businesses would be well advised to assess the potential impact of ransomware on key suppliers in their supply chains, and to consider this impact when rehearsing their response to a ransomware attack. Businesses must do everything they can on the front end with the resources they have in order

[66] *Secureworks:* Ransomware Report Summer 2021 Volume 1, EM360, December 15, 2021.

[67] *See generally* Alexandfra Lohr, Quantum Computing's Threat to Cybersecurity – Winter Is Coming, FEDERAL NEWS NETWORK (Aug. 30, 2022).

[68] Beato et al., *Transitioning to a Quantum-Secure Economy 4*, WORLD ECONOMIC FORUM (2022).

to save costs from a likely threat in the long run.

While these preemptive measures may greatly reduce the risk of harm from a ransomware attack, they cannot completely eliminate the risk. In the event of a ransomware attack, businesses must respond immediately by patching vulnerabilities and weak points and implementing a rehearsed plan. A key part of this plan is data and system restoration to ensure essential operations can remain online with as little interruption as possible. The onus is on businesses to take preemptive measures and be prepared to respond when ransomware occurs.

One effective way to enhance prevention and mitigation efforts is to make the cost of taking these preemptive steps less than the cost of not doing so, thereby helping to raise protection levels across industries. Incentives would encourage businesses to take these measures[69] instead of opting to save on cybersecurity and make ransom payments once an attack occurs. The more hardened a target is, the less likely an attack will occur, and incentives should be adjusted accordingly.

> *"There is no one-stop shop where organizations can "buy" zero trust; rather, zero trust is an approach whose success requires sustained commitments of time and resources."*

In addition to internal actions businesses may take to mitigate risk and respond to ransomware, they must work with government and share information to prevent cybercriminals from acting in the first place. Businesses need not reveal all the facts of an incident or its internal operations, but sharing information enlists a body of authorities, colleagues, and the security community to assist in preparation and recovery. Information sharing between the private sector and government specifically can lead to benefits for the private sector such as advanced threat notices, offensive operations to disable malicious actors before they can strike, increased arrests of cybercriminals, and recovery efforts.

Cyber security is a team effort and the greater the flow of information between the private sector and government, the

[69] *See* Franklin D. Kramer, Melanie J. Teplinsky, and Robert D. Butler, We Need a Cybersecurity Paradigm Change, The Hill (Feb. 15, 2022), (proposing transferable cybersecurity investment tax credits to provide the necessary financial impetus for the development and adoption of integrated cybersecurity capabilities built around a core set of security requirements).

better equipped both sides will be to defend against and confront cybercriminals.

> *"The private sector is gaining critical operational experience [working with the Ukrainian government] which may translate to greater operational integration and coordination with U.S. government entities in the future. It is critical that this cooperation extend beyond a moment of crisis and into day-to-day activity."*

Private sector action in Ukraine in response to Russia's invasion may be a harbinger for increased public/private cooperation in cyberspace in the future. In the early days of Russia's invasion, Ukraine's internet and communications networks were attacked. In response, SpaceX CEO Elon Musk activated Starlink in Ukraine to support its defense efforts. This August, after seeing Starlink's effectiveness in supporting civilian infrastructure and military operations, the U.S. Air Force signed a year-long contract with SpaceX to utilize Starlink internet capabilities to support its forces in Europe and Africa.[70]

Microsoft has also been working closely with Ukrainian officials "to identify and remediate threat activity against Ukrainian networks" since Russian forces began amassing near Ukraine's border.[71] Microsoft's active engagement in this space has aided Ukrainian efforts to defend its networks. Cisco is another actor that not only worked with its Ukrainian government clients, but also worked with U.S. actors such as CISA. Cisco teams engaged in aggressive threat hunting in Ukrainian networks, intelligence gathering, and intelligence sharing with Ukrainian government entities.[72] These selected examples are illustrative of the public/private cooperation in the lead up to Russia's invasion and the cooperation that is still ongoing.

This kind of private sector cooperation with Ukrainian government entities bodes well for future cooperation with U.S. government entities. The private sector is gaining critical operational experience which may translate to

[70] Christopher Woody, U.S. Air Force is Signing Up for Starlink After Watching it Help Ulkraine Stay Online Amid Russia's Ongoing Attacks, BUSINESS INSIDER (Aug. 8, 2022).

[71] Microsoft Digital Security Unit, Special Report: Ukraine—An Overview of Russia's Cyberattack Activity in Ukraine 3 MICROSOFT (APR 27, 2022)

[72] Matt Olney, Cisco Stands on Guard With Our Customers in Ukraine, CISCO BLOGS (Mar. 3, 2022),

greater operational integration and coordination with U.S. government entities in the future. It is critical that this cooperation extend beyond a moment of crisis and into day-to-day activity. The public and private sectors have shown their ability to rally around the common cause of defending a nation besieged by an unjust invasion. They should now take that cooperation model and apply it to the common cause of overall network threat detection and security to create a safer cyberspace environment for all, not only at a time of crisis. The Biden Administration appears to be heading down this path as private sector actors were invited to participate in the Second International Counter Ransomware Initiative at the White House in October 2022 for the first time in the Initiative's nascent history.[73]

VI. National Security and Ransomware

Ransomware poses a serious threat to U.S. national security, a point brought home by the Colonial Pipeline attack. Ransomware threatens to disrupt operation of critical infrastructure (e.g., electric power, oil pipelines, and transportation), hospitals, governments, businesses and more. Such disruptions have a direct impact on Americans and harm not only our economic interests, but our national security interests as well. More frequently, nation-states have been the perpetrators of such disruptions in order to pursue their strategic, national security, and espionage priorities. In some instances, nation-states have deployed ransomware with no intent to collect a ransom, but merely to sow chaos and punish their adversaries, as in 2017, when Russia deployed NotPetya to disrupt and destroy Ukrainian targets.[74] Moreover, as the Ransomware Task Force has recognized, "the immediate physical and business risks posed by ransomware are compounded by the broader societal impact of the billions of dollars steered into criminal enterprises, funds that may be used for the proliferation of weapons of mass destruction, human trafficking, and other virulent global criminal activity."[75] This threat calls for an "all tools" approach where the government uses every instrument of power at its disposal–diplomatic, informational, military, economic, financial, intelligence, and law enforcement–to tackle the issue.

[73] Senior Administration Official, *Background Press Call Previewing the Second International Counter Ransomware Initiative Summit* (Oct. 30, 2022).

[74] Andy Greenberg, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED (Aug. 22, 2018.

[75] Institute for Security and Technology, Combating Ransomware 5 RANSOMWARE TASK FORCE (2021).

Nation-States and Ransomware

Ransomware, and cyber operations generally, has become an increasingly common tool that nation-states employ to facilitate their national security and strategic goals. Similarly, nation-states themselves have increasingly become targets of cyber threat groups and other nation-states.

> *"Ransomware, and cyber operations generally, has become an increasingly common tool that nation-states employ to facilitate their national security and strategic goals."*

Historically, China, Russia, North Korea, and Iran have frequently used ransomware and proxy groups to target nation-states, particularly Western countries.[76] China in particular has relied on the cyber threat group WICKED PANDA to facilitate its latest five-year plan and support its state intelligence apparatus while Iran has relied, in part, on the group PIONEER KITTEN to conduct ransomware operations against Israeli targets for revenue generation.[77] There are signs that other states, such as Vietnam and Pakistan, are exploring this realm as well.[78]

While the scope of nation-states operating in this realm is expanding, the targets are expanding beyond traditional Western countries to those with potentially weaker cyber defenses. In August 2022, a ransomware attack against Montenegro, a NATO member, crippled its government services and targeted critical infrastructure including electric power, transportation, banking, and water.[79] To complicate matters, a financially motivated ransomware group known as "Cuba" claimed responsibility for the attack[80] after Montenegrin security officials reportedly blamed Russia for the attack. In September 2022, Albania, another NATO member, cut diplomatic ties with Iran over a ransomware attack that shut down some of its government digital services and websites. Albania characterized Iran's operation as state aggression.[81] Also in

[76] *See generally* Center for Strategic and International Studies, Significant Cyber Incidents Since 2006, CSIS (2022).

[77] 2021 Global Threat Report, CrowdStrike (2021) 35, 41.

[78] *Id.* at 34.

[79] Ines Kagubare, FBI Deploys Cyber Team to Montenegro Following Massive Cyberattack, The Hill (Aug. 31, 2022); Erica Lonergan and Maggie Smith, Who Attacked Montenegro? The Moral and Strategic Hazards of Misassigning Blame, Political Violence at a Glance (Sept. 21, 2022).

[80] Dusan Stojanovic, NATO Member Montenegro Grapples With Massive Cyberattack It Blames on Russia, LA Times (Sept. 12, 2022).

[81] Kevin Poireault, NATO-Member Albania Cut Times with Iran Over Cyber-Attack, Info Security (Sept. 8, 2022).

September 2022, Bosnia and Herzegovina's parliament was effectively crippled by a ransomware attack.[82] This occurred at a particularly sensitive time as the country was, and still is, facing potential political upheaval over demands for secession from Bosnian Serbs. In the summer of 2022, Costa Rica was the victim of unprecedented ransomware attacks targeting numerous government offices, including those controlling taxes, customs, and public health services.[83]

"targets are expanding beyond traditional Western countries to those with potentially weaker cyber defenses."

The Costa Rican government was forced to declare a state of emergency in response to the crippling attacks. The notorious Russian-based Conti ransomware group (described above), which perpetrated the attacks, eventually leaked hundreds of gigabytes of data taken from Costa Rican government servers, including the Ministry of Finance.[84]

Although by some measures the number of ransomware attacks appears to have declined in 2022,[85] the spate of recent ransomware attacks by and against nation-states cautions against complacency given ransomware's potentially significant national security implications.

International Law Dimensions

Counter-ransomware efforts also have an important international law dimension, which requires exploration of, *inter alia,* the concepts of attribution, sovereignty, and due diligence.

First, attribution. International law treats state and non-state actors differently, so properly attributing ransomware operations to a state or non-state actor can be crucial to determining a state's available prevention and response

[82] Jonathan Grieg, Bosnia and Herzegovina Investigating Alleged Ransomware Attack on Parliament, THE RECORD (Sept. 19, 2022),.

[83] Associated Press, Costa Rica, 'Under Assault' Is a Troubling Test Case on Ransomware Attacks, NBC NEWS (Jun. 17, 2022).

[84] Costa Rica May Be Pawn in Conti Ransomware Group's Bid to Rebrand, Evade Sanctions, KREBSONSECURITY (May 31, 2022).

[85] NSA Director of Cybersecurity Rob Joyce observed at a spring 2022 conference that the incidence of ransomware "is actually down." National Cyber Security Centre CyberUK 2022, *Plenary 1: Global response*, *Global impact: Strategic Alignment and Collaboration*, YOUTUBE at 47:40; *but see* Kevin Collier (@kevincollier), TWITTER (Nov 16, 2022) (stating "FBI deputy director Paul Abbate at @AspenCyber puts to rest the idea that ransomware attacks in the US are slowing: "We've only seen the problem get worse [....] We've seen a higher volume of ransomware attacks and the financial losses are increasing as well,") (quoting FBI Deputy Director).

options. Attribution can be challenging, but over the past decade, attribution abilities have improved significantly due to improved technical capabilities and, importantly, more effective public and private sector coordination.

> *"Although by some measures the number of ransomware attacks appears to have declined in 2022,*[85] *the spate of recent ransomware attacks by and against nation-states cautions against complacency."*

The U.S.'s increase in use of speaking indictments (discussed in more detail below in the 'Current Government Action' section), as well as official public statements (often coordinated internationally, as in the case of NotPetya) is a sign of the government's growing confidence in making attributions.

In addition to demonstrating the increasing capability to effectively and rapidly identify ransomware actors, such public attributions can be used to signal to adversaries that the U.S. deems a particular cyber operation unacceptable, either as a matter of international law or national policy. However, the U.S. should continue to ensure rigor in making such pronouncements to avoid premature or poorly supported public accusations that could damage its credibility[86] and to align them with broader policy objectives.[87]

Second, the role of sovereignty in international law has important implications for U.S. counter-ransomware operations. The normative status and parameters of sovereignty in cyberspace are unsettled questions in international law, currently being debated publicly[88] and in fora such as the two major UN-sponsored initiatives: the Governmental Group of Experts (GGE) and the Open-Ended Working Group (OEWG).[89]

[86] Erica Lonergan and Maggie Smith, *Who Attacked Montenegro?* The Moral and Strategic Hazards of Misassigning Blame, POLITICAL VIOLENCE AT A GLANCE (Sept. 21, 2022).

[87] Public attribution also has several other possible objectives, which the U.S. has achieved in varying degrees. For example, public attribution can be used to deter a state actor; specifically, to persuade a malicious state cyber actor to cease its operations. Recognizing that "naming and shaming," by itself, may be insufficient to deter concerted cyber adversaries, the U.S. has coupled public attribution with sanctions, indictments, and even cyber-based counterstrikes. Attribution also can expose individual malicious cyber actors, introducing friction into an adversary state's cyber ecosystem (e.g., by making it more difficult for a state to recruit individual cyber actors). The actual deterrent effect of public attribution remains an open question.

[88] Michael Schmitt, The Sixth United Nations GGE and International Law in Cyberspace, JUST SECURITY (Jun. 10, 2021), (discussing the UN GGE debate over sovereignty).

[89] The UN's Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security

Although the U.S. has not announced an official position on whether sovereignty in cyberspace is a principle or rule of international law, elements of the government have expressed sympathy toward the United Kingdom's stance that sovereignty is not a primary rule of international law. Under this position, a state has a greater degree of leeway in conducting counter-ransomware cyber operations against infrastructure located in second or, more likely, third-party states.

On the other hand, if a state recognizes sovereignty as a primary rule, it is likely to consider cyber operations generating more than *de minimis* effects on its territory as a breach of international law. This presents an important consideration for U.S. counter-ransomware policy and potential operations; recognizing sovereignty as a rule of international law may present legal barriers to the conduct of certain counter-ransomware operations (e.g., taking down ransomware infrastructure on foreign soil to disrupt an ongoing ransomware threat originating in a third country).

One last consideration is the principle of due diligence, according to which states should not allow their territory or cyber infrastructure to be used to adversely affect other states.

> *"Although the U.S. has not announced an official position…, elements of the government have expressed sympathy toward the United Kingdom's stance that sovereignty is not a primary rule of international law. Under this position, a state has a greater degree of leeway in conducting counter-ransomware cyber operations against infrastructure located in second or, more likely, third-party states."*

States have an affirmative duty to mitigate the harm if they know their territory or cyber infrastructure is being used for malign activity. This rule has a low standard of proof: one need only show that the state is failing to stop the harm, not that it is directly facilitating the harm. However, like sovereignty, the normative status of the due diligence

(UNGGE) was established in 2004 to develop norms of responsible state behavior in cyberspace and most recently adopted a consensus final report in May 2021. The UN's Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (UN OEWG), created by a 2018 Russia-sponsored resolution, resulted in a consensus report in March 2021. See United Nations, Off. Disarmament Affairs, Open-ended Working Group (Mar 12, 2021).

principle and its applicability to the cyber context is unsettled among states.

Due diligence often is proffered as an important part of counter-ransomware efforts as it ostensibly provides a legal basis for responses "to hostile cyber operations of non-state actors or in cases where attribution to a state proves difficult to reliably establish."[90] Difficulty with due diligence arises in the form of each state's resources.

While acceptance of due diligence as a principle is growing, numerous states recognize the inherit limits of some states in effectively mitigating the harm emanating from their territory.[91] Some states do not have the capacity to effectively prevent and halt cyber threat groups' operations being launched from their territory. Others may lack the technical sophistication or know-how to recognize that their territories (and the infrastructure housed therein) are being used in this way.

This is notable in the context of discussions in 2021 between President Biden and Russian president Vladimir Putin concerning the proliferation of ransomware in 2021. Russia undoubtedly has the resources to enforce the due diligence rule, and, after talks in the summer of 2021, it appeared that the U.S. and Russia might be on a path toward cooperation in reducing operations emanating from Russia.[92] Those hopes, however, were effectively eliminated with Russia's invasion of Ukraine, and it seems likely that Russia will remain a safe haven for malign cyber activity for the foreseeable future.

Whether due diligence in cyberspace is a rule of international law or a mere "voluntary, non-binding norm of responsible state behavior" remains a matter of spirited debate among states and experts.[93] Accordingly, it remains unclear whether states "bear a *legal obligation* to thwart criminal ransomware activities emanating from their territories."[94] While the applicability of the "rule" of due diligence to cyberspace remains unsettled, there is steadily growing acceptance that the concept of due diligence should be applied to cyberspace, as evidenced by the September 2022 statement of the Quad (Australia, India, Japan, and U.S.)

[90] Gary Corn, International Law's Role in Combating Ransomware?, JUST SECURITY (Aug. 23, 2021).

[91] United Nations General Assembly, "Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266," July 13, 2021.

[92] Joe Tidy, Why Cyber-Gangs Won't Worry About US-Russia Talks, BBC NEWS (Jun. 16, 2021).

[93] *See*, e.g., Michael Schmitt, Three International Law Rules for Responding Effectively to Hostile Cyber Operations, JUST SECURITY (Jul. 13, 2021), (explaining that the Tallinn Manual Group of Experts concluded such a rule existed in the cyber context while the UN GGE was unable to reach consensus that such a rule existed and instead concluded that due diligence was a voluntary, non-binding norm).

[94] Gary Corn, *supra* note 90.

foreign ministers calling on states to "take reasonable steps to address ransomware operations emanating from within their territory."[95]

VII. Current Government Action

The U.S. has embraced an "all tools" approach, taking significant steps to combat ransomware over the past year. These include various efforts to improve critical infrastructure cybersecurity ranging from new regulations (e.g., DHS' revised and reissued security directives for natural gas and oil pipelines) to CISA's "Shields Up" campaign; beefed up law enforcement capabilities; and new sanctions targeting not only ransomware operators but the cryptocurrency exchanges, virtual wallets, and various services (e.g., mixing services) used to move and launder the illicit funds from their operations.

Some of the most notable efforts to combat ransomware emanate from the Executive Branch. On the law enforcement front, the Department of Justice has engaged the Ransomware Task Force,[96] the Civil Cyber Fraud Initiative,[97] the National Cryptocurrency Enforcement Team,[98] and civil lawsuits[99] to dismantle cyber infrastructure that criminals use to conduct operations. CISA has been providing defensive resources to the private sector, most recently through its "Shields Up" campaign in response to Russia's invasion of Ukraine.[100] Various financial regulators, including the SEC, CFTC, and Treasury's OFAC and FINCEN, also are

[95] DEP'T OF STATE, Quad Foreign Ministers' Statement on Ransomware (Sept. 23, 2022),.

[96] Alexander Culafi, DOJ Creates Ransomware Task Force To Combat Digital Extortion, TECHTARGET (APR 22, 2021).

[97] DEP'T OF JUST., Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber Fraud Initiative (Oct. 6, 2021),

[98] DEP'T OF JUST, Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team (Oct. 6, 2021).

[99] For example, the civil injunctive process played a critical role in DoJ's March 2022 disruption of the Cyclops Blink botnet controlled by Sandworm, a Russian state-sponsored hacking group. *See* DEP'T OF JUST., Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU) (Apr. 6, 2022). For a more detailed discussion of the role and limitations of the civil injunctive process in disrupting botnets *see* Statement of Richard W. Downing, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice Before U.S. Senate Judiciary Committee Hearing, America Under Cyber Siege: Preventing and Responding to Ransomware Attacks at 9; Statement of Sujit Raman, Associate Deputy Attorney General Department of Justice Before the Subcommittee on Crime and Terrorism, Committee on the Judiciary, United States Senate, Cyber Threats to Our Nation's Infrastructure, at 9-10 (discussing legal limitations on DoJ's use of the civil inunction process to disrupt botnets); April Falcon Doss, We're From the Government, We're Here to Help: The FBI and the Microsoft Exchange Hack, JUST SECURITY (Apr. 16, 2021); Asaf Lubin and João Marinotti, Why Current Botnet Takedown Jurisprudence Should Not Be Replicated, LAWFARE (Jul. 21, 2021).

[100] Cybersecurity and Infrastructure Security Agency, "Shields Up."

working to combat ransomware. For example, OFAC and FINCEN are working to improve visibility into crypto offramps where criminals convert their ill-gotten cryptocurrency into fiat money.

In addition, as part of DoD's "Defend Forward" strategy,[101] U.S. Cyber Command is reportedly taking active measures to target and disrupt cybercriminals abroad.[102] Some critique the use of the military to pursue cybercriminals on the grounds that such activity is a law enforcement, not military, role. However, as President Biden has made clear, ransomware presents not just a criminal, but a national security threat.

As such, it is within the President's constitutional and statutory authority to pursue ransomware actors using both law enforcement and military resources, subject to certain limitations. Care must be taken not to run afoul of Federal laws, such as the *Posse Comitatus Act,* that prohibit the use of the military to enforce the law. There may be an element of law enforcement when the military conducts such operations, but it conducts its operations abroad for the purpose of disrupting national security threats—much as it does when conducting operations abroad to eliminate terrorist threats–and is not using troops for domestic law enforcement. Further, the military is not gathering evidence or building cases, but is disrupting cybercriminals and preventing them from conducting operations. Ultimately, the military has immense resources with which to tackle the ransomware problem.

> *"... ransomware presents not just a criminal, but a national security threat. As such, it is within the President's constitutional and statutory authority to pursue ransomware actors using both law enforcement and military resources, subject to certain limitations."*

Taking the military entirely out of the equation would run counter to the government's "all tools" approach to combating ransomware and could harm U.S. interests and national security. While adherence to traditional *posse comitatus* restrictions is complicated in the context of cyber, Federal law does not preclude the President from directing DoD to counter these threats. Nevertheless, the government should develop clear policy guidelines

[101] SUMMARY, Department of Defense Cyber Strategy, 2018.

[102] Mark Pomerleau, Here's How Cyber Command is Using Defend Forward, C4ISRNET (Nov. 12, 2019).

governing these DoD operations to ensure consistency with *posse comitatus* principles.

On the diplomatic front, the U.S. has been engaging with allies to prioritize tackling the ransomware issue, as recently demonstrated by the Quad Foreign Ministers' Statement on Ransomware.[103] The State Department also has been using its Rewards for Justice program to seek out ransomware operators and bring them to justice.[104]

An additional tool the U.S. has employed is the "speaking indictment." Speaking indictments allow the government to identify cybercriminals and lay out a legal case as to what could be proved in court if the cybercriminals were apprehended. Even where the charged individual never sees the inside of a U.S. courtroom, these indictments draw attention to cybercriminals' actions and help clarify and solidify international norms, especially when the perpetrator is a state actor or affiliated with a state actor. Notable examples include the 2021 indictment of three North Korean military hackers in connection with the 2017 "WannaCry" ransomware attacks and other significant financial and cyber crimes, including the attempted theft of $1.3 billion;[105] and the 2018 indictment of two Iranian actors alleged to have deployed "SamSam" ransomware causing more than $30 million in losses to over 200 victims.[106] Speaking indictments put the actors on notice and often target a very specific audience to inform that audience that the U.S. knows what is happening, how it happened, and who did it. Those named in such an indictment may face professional embarrassment, difficulty traveling internationally, and the possibility of capture, trial, and punishment. By themselves, these indictments will not stop ransomware, but by making life more difficult for those identified in the indictments and facilitating norms development, they are effective instrumentalities of the "all tools" approach.[107]

Other executive actions that have been discussed include prohibiting ransom

[103] DEP'T OF STATE, *supra* note 95.

[104] DEP'T OF STATE, Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice (May 6, 2022).

[105] DEP'T OF JUST., Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe (FEB. 17, 2021).

[106] DEP'T OF JUST., Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses (NOV. 28, 2018).

[107] For discussions of the merits of a deterrence strategy that includes the filing of criminal charges against foreign-based malign cyber actors, *see generally* Sujit Raman, "The Rule of Law in the Age of Great Power Competition in Cyberspace," Associate Deputy Attorney General Sujit Raman Delivers Remarks at the ABA Rule of Law Initiative Annual Issues Conference | OPA | Department of Justice (defending this approach); Garrett Hinck & Tim Maurer, *Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Activity*, JOURNAL OF NAT'L SEC. LAW & POLICY (2020); *but see* Jack Goldsmith & Robert D. Williams, *The Failure of the United States' Chinese-Hacking Indictment Strategy*, LAWFARE (Dec. 28, 2015), (criticizing the strategy of indicting Chinese hackers for violations of U.S. law).

payments. Both ideas have been met with pushback. Many businesses pay the demanded ransom if they can in order to recover from attack. Banning ransom payments may lead to prosecution of businesses that decide to pay ransom to recover and would likely result in businesses hiding such payments in order to avoid prosecution.

For these reasons, federal officials recently rejected an outright ban on ransomware payments, choosing instead to discourage such payments, encourage better cybersecurity practices, and encourage cyber insurance companies to incentivize better cyber hygiene through lower premiums and stricter underwriting requirements.[108]

VIII. Expert Recommendations

To combat ransomware, the U.S. government should strengthen:

⇒ Defense

- Strengthen efforts to provide resources to the private sector regarding how best to (1) prepare for ransomware attacks; (2) remain resilient in the face of such attacks; and (3) recover from such attacks.
- Encourage use of the National Institute of Standards and Technology ransomware profile[109] (identify, protect, detect, respond, recover) for larger entities and the Ransomware Task Force's Blueprint for Ransomware Defense for small and medium sized entities.[110]
- Facilitate adoption of cybersecurity hygiene measures, including potentially through regulatory requirements (at both the federal and State levels), tax incentives, or adoption of "labels" on key products (and their constituent parts).
- To avoid moral hazard (i.e., the problem of entities using cyber insurance as a substitute for appropriate cybersecurity controls), ensure that eligibility for any government cyber reinsurance program is conditioned on insurance

[108] Matt Kapko, U.S. Government Rejects Ransom Payment Ban to Spur Disclosure, CYBERSECURITY DIVE (SEPT. 19, 2022).

[109] William C. Barker, *et al.*, Ransomware Risk Management: A Cybersecurity Framework Profile, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (FEB. 2022).

[110] *See generally* Aaron McIntosh & Valecia Stocchetti, Blueprint for Ransomware Defense, INSTITUTE FOR SECURITY + TECHNOLOGY (2022).

companies requiring/enforcing minimal cybersecurity standards for their customers.

- Establish transferrable tax incentives for investments in advanced cybersecurity measures[111] to protect key critical infrastructures (e.g., electric grid) from national security threats. Cybersecurity investment tax credits also could be made available to assist small- and medium-sized businesses engaged in advancing emerging or advanced technologies of critical importance to national security (e.g., AI, quantum computing, robotics).[112]
- Encourage additional government cybersecurity information sharing with the private sector with a "need to *share*," rather than "need to *know*," paradigm.
- Encourage additional private sector cybersecurity information sharing with the government through incentives rather than (or in addition to) penalties, such as immunity from prosecution or regulatory action based on information shared.
- Promote mechanisms for pooling information and intelligence about ransomware attacks (and the illicit actors behind them). For example, explore options for the U.S. intelligence community, the Financial Stability Oversight Council, and the financial services industry to work towards establishment of a 21st-century crypto threat information sharing database with regulators and financial institutions.

⇒ Offense

- Update and clarify federal laws (e.g., CFAA) to provide clear guidance to the private sector on the scope of permissible responses to ransomware attacks.
- Prioritize the public sector's efforts to disrupt ransomware infrastructure, including by targeting the ransomware-as-a-service ecosystem.
- Consider more transparency and public justification of offensive cyber operations conducted by the US military.
- Consider options, including legislative and policy amendments, to provide greater flexibility to military cyber operators to assist law enforcement, consistent with privacy and civil liberties protections, in identifying and disrupting cybercriminals' malicious activities on domestic infrastructure.

[111] At a minimum, such measures should include zero trust architectures complemented by an effective threat hunting program, which are equivalent to measures being undertaken for federal civilian executive branch agencies pursuant to President Biden's May 12, 2021 Executive Order.

[112] Franklin D. Kramer, Melanie J. Teplinsky, & Robert D. Butler, We Need a Cybersecurity Paradigm Change, THE HILL (FEB. 15, 2022).

⇒ Law Enforcement

- Despite the continued severity of the ransomware problem, there have been certain notable successes in recent months including: arrests of major illicit actors (most of whom were operating abroad); [113] disruptions and takedowns of key ransomware digital infrastructure (e.g., NetWalker, Emotet[114]); and the seizure of ransomware payments[115] so that illicit actors cannot benefit from them. Law enforcement efforts along each of these dimensions should continue to be strengthened, including through (1) enhanced international cooperation and partnerships on cybercriminal investigations, (2) amendments to U.S. law to better facilitate criminal infrastructure takedowns, and (3) continued investment in blockchain analytics tools and training on cryptocurrency-based investigations.

⇒ Cyber Incident Reporting Regime

- Rationalize the existing patchwork quilt of federal sector-specific reporting requirements and state data breach reporting requirements to reduce the compliance burden on companies while maintaining the benefits of timely and accurate cyber incident reporting.
- In the short term, as CISA works to promulgate regulations to implement CIRCIA, CISA should work to rationalize and simplify the complex reporting environment that businesses face.
- Craft any necessary requirements for public disclosure of cyber incidents so as not to conflict with the needs of active law enforcement investigations, national security, or responsible vulnerability disclosure.
- The private sector should seize the opportunity to help shape CISA's forthcoming cyber incident and ransomware payment reporting regulations to ensure that they function effectively to facilitate accurate and timely reporting of threat information while minimizing the burden on business.
- U.S. companies not covered by CIRCIA or other federal cyber incident reporting requirements should be incentivized to share as much

[113] *Top Zeus Botnet Suspect 'Tank' Arrested in Geneva*, KREBS ON SECURITY (Nov. 15, 2022); DEP'T OF JUSTICE, Canadian National Sentenced in Connection with Ransomware Attacks Resulting in the Payment of Tens of Millions of Dollars in Ransoms (OCT. 4, 2022); *See also* Statement of Richard W. Downing, *supra* note 99 at 6, https://www.judiciary.senate.gov/imo/media/doc/Downing%20-%20Statement.pdf.

[114] DEP'T OF JUST, DEPARTMENT OF JUSTICE LAUNCHES GLOBAL ACTION AGAINST NETWALKER RANSOMWARE (JAN. 27, 2021), DEP'T OF JUST, EMOTET BOTNET DISRUPTED IN INTERNATIONAL CYBER OPERATION (JAN. 28, 2021).

[115] DEP'T OF JUST, Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (JUN. 27, 2021).

information as practicable about identified cyber threats and cyber incidents in a common database.

⇒ Cryptocurrency Efforts

- Establish high-level coordination between departments and agencies on federal regulation and policy regarding all crypto activities. In addition, Congress should conduct hearings to explore the applicability to the crypto market of standards similar to those in place for federally regulated financial markets, and should craft appropriate legislation, as needed.

⇒ International Efforts

- Strengthen and support international cooperation and partnerships: (a) on cybercriminal investigations; (b) to combat illicit use of cryptocurrency (e.g., by encouraging global implementation and enforcement of anti-money laundering and counter financing of terrorism (AML/CFT) controls); and (c) to identify and put in place measures that disincentivize nation-states from harboring cybercriminals.