PEPPERDINE UNIVERSITY

Pepperdine Law Review

Volume 50 | Issue 1 Article 3

1-20-2023

Typing a Terrorist Attack: Using Tools from the War on Terror to Fight the War on Ransomware

Jake C. Porath

Typing a Terrorist Attack: Using Tools from the War on Terror to Fight the War on Ransomware

Abstract

The United States faces a grave challenge in its fight against cyberattacks from abroad. Chief among the foreign cyber threats comes from a finite number of "ransomware-as-a-service" gangs, which are responsible for extorting billions of dollars from American citizens and companies annually. Prosecuting these cybercriminals has proven exceedingly difficult. Law enforcement often struggles to forensically trace ransomware attacks, which makes identifying and prosecuting the perpetrators challenging. Moreover, even when prosecutors can identify the perpetrators of these attacks, the ransomware gangs are headquartered in foreign adversarial nations that do not extradite criminals to the United States. Finally, ransomware gangs are governed by complex structures that push the limits of joint criminal enterprise liability. While these challenges are complex, they are not unprecedented. The United States has crafted successful legal solutions in response to similar challenges in its fight against the War on Terror.

This Comment analyzes one of these legal solutions from the War on Terror, 8 U.S.C. § 1189, which establishes the Foreign Terrorist Organization list and assesses whether the State Department can and should designate foreign ransomware gangs as "Foreign Terrorist Organizations" (FTOs). This Comment argues that ransomware gangs qualify as "foreign organizations," engage in "terrorist activities" as defined under the statute, and threaten the national security of the United States. Thus, ransomware gangs meet

the statutory requirements for designation as FTOs. Given the prosecutorial and investigatory benefits and the useful financial and political implications of the designation, this Comment argues that the State Department should list ransomware gangs as FTOs.

TABLE OF CONTENTS

"There are a lot of parallels [between the 2021 ransomware attacks and the challenges posed following the September 11 Attacks], there's a lot of importance, and a lot of focus by us on disruption and prevention . . . ."
- Federal Bureau of Investigation Director, Christopher A. Wray[1]

"If men were angels, no government would be necessary."
- Federalist No. 51[2]

I. INTRODUCTION—A MAJOR BREACH: THE LANDSCAPE OF AMERICA'S RANSOMWARE CRISIS

On May 7, 2021, the "jugular" of the East Coast's oil supply—the Colonial Pipeline—was forced to shut down in the wake of a catastrophic ransomware attack.[3] The pipeline spans from Texas to New Jersey and supplies approximately forty-five percent of the region's petrol and diesel supply.[4] Despite the company paying $4.4 million in ransom, the pipeline could not resume operations for nearly a week, which wreaked havoc across the region.[5] The Southeast was "particularly vulnerable" due to its fewer number of local refineries and its geographical idiosyncrasies that make importing large quantities of gasoline from abroad notably more difficult.[6] Gas demand spiked over forty percent across Florida, Georgia, South Carolina, North Carolina, and Virginia,[7] and the East Coast's gasoline stockpile decreased by approximately 4.6 million barrels.[8] Despite statements from public officials urging

1. Julian E. Barnes, F.B.I. Director Compares Danger of Ransomware to 9/11 Terror Threat, N.Y. Times (June 4, 2021), https://www.nytimes.com/2021/06/04/us/politics/ransomware-cyberattacks-sept-11-fbi.html.

2. *The Federalist Papers: No. 51*, YALE L. SCH.: THE AVALON PROJECT, https://avalon.law.yale.edu/18th_century/fed51.asp (last visited Sept. 29, 2022).

3. *A Cyber-Attack Exposes Risks to America's Energy Infrastructure*, THE ECONOMIST (May 13, 2021), https://www.economist.com/united-states/2021/05/13/a-cyber-attack-exposes-risks-to-americas-energy-infrastructure.

4. *Id.*

5. Collin Eaton & Dustin Volz, *Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*, WALL ST. J., https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636 (May 19, 2021, 4:51 PM).

6. Collin Eaton et al., *Pipeline Shutdown has East Coast Drivers Making a Run on Gas*, WALL ST. J., https://www.wsj.com/articles/east-coast-drivers-make-run-on-gas-stations-following-colonial-pipeline-shutdown-11620748473?mod=article_inline (May 11, 2021, 4:10 PM).

7. *Id.*

8. Eaton & Volz, *supra* note 5 ("East Coast stockpiles of gasoline dropped by about 4.6 million barrels last week . . . .").

consumers against "panic buying," long queues quickly formed at gas stations, many pumps ran out of fuel altogether, and the effects rippled through the region's economy.[9]

Colonial Pipeline's actions before and following the attack exacerbated its gravity and impact on the region.[10] Officials in President Joe Biden's administration "privately voiced [their] frustration with . . . Colonial Pipeline's weak [cyber]security protocols and [] lack of preparation."[11] For example, Colonial Pipeline did not directly report the attack to the Cybersecurity and Infrastructure Security Agency (CISA).[12] Moreover, in a move contradicting the Federal Bureau of Investigation's official position advising against making ransom payments, Colonial Pipeline's Chief Executive Officer, Joseph Blount, quickly paid the seventy-five Bitcoin ($4.4 million) ransom.[13] Nevertheless, despite the company's hope that the decryption key would enable a more immediate restoration of its operations to the pipeline, the shutdown lasted nearly a week.[14]

Although the government's response was more successful than the vast majority of cybercrime investigations,[15] it was nevertheless slow, cumbersome, and disorganized in many respects.[16] Ultimately, like the vast majority

9. *See* Eaton et al., *supra* note 6. In Georgia, for example, approximately five percent of all gas stations ran out of fuel. *Id.* American Airlines temporarily changed the flight path of two of its long-haul routes. *Id.* Similarly, Southwest Airlines began transporting additional fuel to the Nashville International Airport to supplement its local supply of jet fuel. *Id.*

10. *See generally* Zachary Cohen et al., *Biden Administration Officials Privately Frustrated with Colonial Pipeline's Weak Security Ahead of Crippling Cyberattack*, CNN, https://www.cnn.com/2021/05/11/politics/biden-administration-ransomware-frustration/index.html (May 11, 2021, 9:25 PM) (outlining Colonial Pipeline's unpreparedness and failure to notify the Cybersecurity and Infrastructure Security Agency).

11. *Id.*

12. *See id.* Instead of informing CISA directly, Colonial Pipeline informed the Federal Bureau of Investigation (FBI) about the attack, who then brought in CISA to assist in the investigation. *Id.*

13. *See* Eaton & Volz, *supra* note 5.

14. *Id.*

15. *See Over Half of Ransomware Victims Pay the Ransom, but Only a Quarter See Their Full Data Returned*, KASPERSKY (Mar. 30, 2021), https://www.kaspersky.com/about/press-releases/2021_over-half-of-ransomware-victims-pay-the-ransom-but-only-a-quarter-see-their-full-data-returned. According to a study conducted by cybersecurity firm Kaspersky, of 15,000 ransomware-attack victims, approximately "[fifty-six percent] of ransomware victims paid the ransom to restore access" to their computer systems, yet scarcely a quarter of those who paid saw their access fully restored. *Id.*

16. *See* Cohen et al., *supra* note 10 (reporting the Biden Administration's struggle with "limited access to the private company's systems and technical information about the vulnerabilities exploited by the hackers" and Colonial Pipeline's delayed contact to CISA).

of all cyberattacks, the authors of the malware used in the Colonial Pipeline attack, DarkSide, were never publicly identified as individuals.[17] Moreover, authorities have still not identified the DarkSide affiliates responsible for buying the ransomware and executing the attack.[18] Similarly, the individuals behind DarkSide may have gone on to commit other disruptive, high-profile attacks.[19] Despite the aforementioned shortcomings, the response was actually one of the most successful government operations against a cyberattack in recent memory.[20] While the vast majority of cyberattack victims who pay ransoms never recover the payments, the Justice Department was eventually able to recover approximately sixty-four out of the seventy-five Bitcoins paid by Colonial Pipeline.[21]

Against the backdrop of the Colonial Pipeline attack and global cybercrime losses totaling nearly $1 trillion in 2020,[22] the unfortunate reality is that preventing, investigating, and prosecuting cybercrime is complex and

17. *Id.*

18. *See* Amanda Macias & Christina Wilkie, *U.S. Recovers $2.3 Million in Bitcoin Paid in the Colonial Pipeline Ransom*, CNBC, https://www.cnbc.com/2021/06/07/us-recovers-some-of-the-money-paid-in-the-colonial-pipeline-ransom-officials-say.html (June 8, 2021, 9:09 AM). DarkSide operates as a ransomware-as-a-service (RaaS) model, where they develop malware and market it to other criminal "affiliates." *Id.* The affiliate executes the attack, and the ransomware syndicate retains a percentage fee recovered. Kellen Dwyer, *The Best Way to Stop Ransomware Attacks: Be Proactive, Not Reactive*, WALL ST. J. (Sept. 7, 2021, 4:30 PM), https://www.wsj.com/articles/the-best-way-to-stop-ransomware-attacks-be-proactive-not-reactive-11631046600.

19. *See* David Uberti, *Iowa Grain Cooperative Hit by Cyberattack Linked to Ransomware Group*, WALL ST. J. (Sept. 20, 2021, 5:22 PM), https://www.wsj.com/articles/iowa-grain-cooperative-hit-by-cyberattack-linked-to-ransomware-group-11632172945?tpl=cs. Just months after the Colonial Pipeline attack, an Iowa grain co-op was targeted by a ransomware gang, BlackMatter, which demanded $5.9 million to unlock the organization's data. *Id.* Cybersecurity researchers note that "BlackMatter uses similar types of malware and overlapping cryptocurrency wallets with DarkSide, suggesting the hackers may have rebranded under a new name to avoid law-enforcement scrutiny." *Id.*

20. *See* Carly Page, *The Year the Tide Turned on Ransomware*, TECHCRUNCH (Dec. 30, 2021, 11:00 AM), https://techcrunch.com/2021/12/30/the-year-the-tide-turned-on-ransomware/ (noting Colonial Pipeline was among the rare wins against ransomware attacks).

21. *See* Vanessa Romo, *U.S. Has Recovered Some of the Millions Paid in Ransom to Colonial Pipeline Hackers*, NPR, https://www.npr.org/2021/06/07/1004050873/u-s-retrieves-some-of-the-colonial-pipeline-ransom (June 7, 2021, 4:27 PM); Vanessa Romo, *How a New Team of Feds Hacked the Hackers and Got Colonial Pipeline's Ransom Back*, NPR (June 8, 2021, 2:08 AM), https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac (denoting the factors that led to the government's successful recovery). According to April Falcon Doss, an executive director at Georgetown Law, the government's response was actually "a really big win" because "[r]ansomware is very seldom recovered." *Id.*

22. *See generally* James A. Lewis et al., *The Hidden Costs of Cybercrime*, CTR. FOR STRATEGIC & INT'L STUD. (Dec. 9, 2020), https://www.csis.org/analysis/hidden-costs-cybercrime.

challenging.[23] With respect to prevention, stopping the hackers—whose identities range from foreign governments to cybercriminal gangs—from exploiting a plethora of soft targets with weak cybersecurity is popularly viewed as impossible.[24] Moreover, while proactive approaches like intelligence gathering and preventative prosecution are arguably the most promising strategies, the Department of Justice would need to add more cyber prosecutors and agents to conduct the types of long-term, multi-jurisdictional investigations necessary to make a measurable impact on the issue.[25]

While prevention is difficult, investigating cyberattacks after they take place is likewise challenging.[26] Many companies are reluctant to inform authorities that they were hacked, as it is often reputationally damaging for a company to publicize that their consumers' data has been compromised.[27] Investigations are also often difficult given the technical challenges associated with forensically tracing cyberattacks.[28] Moreover, the ransomware gangs committing the majority of highly disruptive attacks typically do not breach computer systems themselves but instead merely "create the malware needed for such attacks and lease it to low-skilled 'affiliates' in exchange for a percentage of the take."[29] Targeting the affiliates is often ineffective, however, since they are akin to "low-level drug-dealers" in that they are "unskilled, unsophisticated[,] and easily replaceable."[30] Finally, the use of cryptocurrency exacerbates issues surrounding traceability and makes certain types of traditional financial regulatory tools less effective.[31]

---

23. *See* Dwyer, *supra* note 18.

24. *See* Daniel Howley, *Why America Will Never Be Safe from Cyberattacks*, YAHOO! (Mar. 17, 2021), https://www.yahoo.com/now/why-america-will-never-be-safe-from-cyberattacks-195250844.html (noting the difficulties of defending against cyberattacks for governments and private companies).

25. *See* Dwyer, *supra* note 18.

26. *See id.* (noting the difficulties with investigating after the cybercrime has taken place).

27. *See* David Uberti, *U.S. Officials Call for Fines Against Companies That Don't Report Hacks*, WALL ST. J. (Sept. 24, 2021, 5:30 AM), https://www.wsj.com/articles/u-s-officials-call-for-fines-against-companies-that-dont-report-hacks-11632475802?tpl=cs. This incentive for companies to not report hacks will only continue to grow as attacks, where hackers target sensitive consumer or client data and threaten to release it unless a ransom is paid, are increasingly frequent. *See* Catherine Stupp, *The Latest Cybersecurity Threat: Pay Us or We Release the Data*, WALL ST. J. (Sept. 7, 2021, 3:07 PM), https://www.wsj.com/articles/cyber-security-threats-11631041568?tpl=cs.

28. *See* Dwyer, *supra* note 18 (noting that "even the least sophisticated hackers will launch their attacks from rented servers that can be effectively untraceable").

29. *See id.*

30. *Id.*

31. *See* JAMES LEWIS, *Economic Impact of Cybercrime—No Slowing Down*, CTR. FOR STRATEGIC

Likewise, prosecuting the attacks poses its own significant challenges.[32] Ransomware gangs perpetrate attacks from foreign countries.[33] Prosecuting international criminals requires multi-jurisdictional investigations, foreign government cooperation, and formal extradition agreements.[34] However, the majority of cyberattacks are launched from Russia and other former Soviet-bloc countries,[35] where diplomatic ties are frayed and no extradition agreements exist.[36]

Despite these challenges, the United States has faced similar challenges in fighting the war on terror.[37] Specifically, terror attacks, like ransomware attacks, are often perpetrated by transnational foreign adversaries who operate outside of the United States' jurisdiction.[38] Similarly, terror organizations, like ransomware gangs, often operate with unique organizational structures that push the limits of traditional legal theories of joint criminal liability.[39] Finally, in both terror and ransomware attacks, the magnitude of the harm from successful attacks necessitates unique, proactive solutions.[40] In other words, when a terrorist detonates a bomb in a crowd causing a mass-casualty event, law enforcement has failed.[41] Similarly, once DarkSide's malware overwhelmed Colonial Pipeline's cyber-defenses, for example, which precipitated the pipeline's shutdown and a regional energy crisis, law enforcement had already lost.[42] Thus, in combatting both terror and ransomware attacks,

& INT'L STUD. 14 (2018), https://www.csis.org/analysis/economic-impact-cybercrime ("[T]he expansion of cybercrime has been enabled by the easy availability of tools like Bitcoin and Tor, which have allowed cybercriminals to conceal their identities while paying for services through a digital medium that significantly complicates law enforcement tracking efforts.").

32. *See* Dwyer, *supra* note 18.

33. *See* LEWIS, *supra* note 31, at 9–10 ("CSIS believes that Russia leads overall in cybercrime, reflecting the skill of its hacker community and its disdain for western law enforcement. The complex and close relationship between the Russian state and Russian organized crime means that Russia provides a sanctuary for the most advanced cybercriminals . . . .").

34. *See* Dwyer, *supra* note 18.

35. *See* LEWIS, *supra* note 31, at 10 (detailing the reasons why Russia is a leader in cybercrime).

36. *See* Dwyer, *supra* note 18.

37. *See id.* (noting that proactive solutions played a major role in the government's success in preventing another terrorist threat of the magnitude of the September 11 Attacks and arguing for its application in the context of preventing cybercrimes).

38. *See id.*

39. *See* Patrick J. Keenan, *The Changing Face of Terrorism and the Designation of Foreign Terrorist Organizations*, 95 IND. L.J. 789, 810 (2020).

40. *See* Dwyer, *supra* note 18.

41. *See id.* (highlighting the successful law enforcement strategy of investigating and prosecuting terrorist attacks proactively before they take place).

42. *See id.* (suggesting that law enforcement launch proactive investigations to thwart ransomware

law enforcement cannot wait until after an attack happens; instead, law enforcement must craft proactive solutions that focus on preventing and prosecuting the perpetrators before they can carry out attacks.[43]

To mitigate the aforementioned challenges in the terrorism context, prosecutors have heavily relied upon the "Foreign Terrorist Organization" (FTO) designation authorized under 8 U.S.C. § 1189 of the Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA).[44] AEDPA authorizes the Secretary of State to assemble a catalog of foreign organizations that engage in terrorist activities that "threaten[] the security of United States nationals or the national security of the United States."[45]

The FTO designation facilitates prosecutors and investigators by making it easier for them to target those who "materially support" FTOs, which is illegal under 18 U.S.C. §§ 2339A–2339B.[46] The threshold level that qualifies as materially supporting an FTO is notably low, enabling prosecutors to successfully convict a defendant for providing assistance to an FTO even where there are no specific plans for an attack in motion.[47] As a result, this low threshold for what qualifies as providing "material support" enhances prosecutors' ability to secure a defendant's cooperation and "allows law enforcement and counterterrorism personnel to act sooner than might otherwise be possible and leverage early-level cooperation to obtain information about other participants."[48] In addition to the prosecutorial benefits of designating terrorist groups as FTOs, there are various other beneficial social, political, and financial consequences.[49]

This Comment will recommend that the Secretary of State designate the major ransomware gangs who threaten the United States' national security as FTOs.[50] Although state actors and traditional terrorist groups have historically

attacks).

43. *See id.*

44. *See* Aaron L. Schwartz, *National Security and the Protection of Constitutional Liberties: How the Foreign Terrorist Organization List Satisfies Procedural Due Process*, 3 PENN ST. J.L. & INT'L AFF. 292, 293 (2014) ("Section 1189 offers the U.S. government an effective legal tool to impede terrorist organizations that threaten U.S. national security interests."); Keenan, *supra* note 39, at 791 ("For prosecutors putting together cases against suspected terrorists, one of the most important tools of counterterrorism has been the designation of terrorist groups as foreign terrorist organizations.").

45. 8 U.S.C. § 1189.

46. *See* 18 U.S.C. §§ 2339A–2339B.

47. *See* Keenan, *supra* note 39, at 791–92.

48. *Id.* at 792.

49. *See* discussion *infra* Section III.D.

50. *See infra* Part IV.

committed a multitude of high-profile and disruptive cyberattacks against the United States, ransomware attacks are the "fastest growing cybercrime" tool.[51] The ransomware variants that present the greatest national security threat to the United States come from the "Ransomware-as-a-Service (RaaS) model," where the criminal gangs "author" the malware and lease it to third-party "affiliates."[52] The affiliates launch the attacks, while the ransomware gang authors receive a commission fee based on the ransom collected.[53] Despite the massive cost to America's national security and economic interests, fewer than ten strains of ransomware were responsible for most of the attacks committed in the past six years.[54] This Comment will argue that the most prolific ransomware gangs legally fit the definition of FTOs.[55] In addition to the other financial and political benefits, designating ransomware gangs as FTOs would enable prosecutors to leverage cooperation from a multitude of new parties who are responsible for "materially supporting" the ransomware gangs.[56]

Part II of this Comment explains the technology of ransomware, the RaaS business model, the motives behind the ransomware attacks, and the attacks' critical cost to American society.[57] Part III discusses the history of the FTO list, the process by which the government designates a new FTO, the constitutional arguments for and against the statute, and the consequences of the designation for those listed.[58] Part IV applies the FTO statute to ransomware gangs and emphasizes the legal, financial, and political benefits that would result from designating ransomware gangs as FTOs.[59] Lastly, Part V summarizes and concludes.[60]

51. *See* LEWIS, *supra* note 31, at 11.

52. *Id.*; *see* Andrew E. Kramer et al., *Secret Chats Show How Cybergang Became a Ransomware Powerhouse*, N.Y. TIMES, https://www.nytimes.com/2021/05/29/world/europe/ransomware-russia-darkside.html (June 3, 2021).

53. LEWIS, *supra* note 31, at 11.

54. *See* Dwyer, *supra* note 18.

55. *See infra* Part IV.

56. *See* Keenan, *supra* note 39, at 791–92.

57. *See infra* Part II.

58. *See infra* Part III.

59. *See infra* Part IV.

60. *See infra* Part V.

II. LOCKED OUT: CONTEXTUALIZING THE RANSOMWARE REVOLUTION

In 1989, an eccentric Harvard evolutionary biologist sent 20,000 floppy disks through the mail to health researchers, which were said to contain a survey to test one's risk of contracting AIDS.[61] However, when the disk was inserted, the software encrypted the researchers' computers and demanded that the researchers send $189 in cash to a Panamanian P.O. box for the key to unlock their data.[62] Although ransomware attacks remained crude and obscure for years following the 1989 attack, the number of ransomware attacks exploded in the last decade with technology's rapid development.[63] This Section will describe the technology used in ransomware attacks in further depth, the black-market business model of ransomware distribution, the motives fueling the attacks, and the attacks'cost to society.[64]

A. The Technology of Ransomware

Ransomware is a form of malware that hijacks or encrypts a computer system or its files and holds it as ransom in exchange for money (usually cryptocurrency).[65] Ransomware is considered a type of "scareware," which is defined as "[m]alware that 'takes advantage of people's fear of revealing their private information, losing their critical data, or facing irreversible hardware

61. Alina Simone, *The Strange History of Ransomware*, THE WORLD (May 17, 2017, 11:45 AM), https://theworld.org/stories/2017-05-17/strange-history-ransomware.

62. *Id.*

63. *See* LEWIS, *supra* note 31, at 11. "Until 2015, ransomware campaigns were typically run by organized crime groups that wrote their own code. From 2012 to 2015, 33 new ransomware offerings were released, but that number doubled in 2016, with 70 new families of ransomware products made available." *Id.* (footnote omitted).

64. *See infra* Sections II.A–C.

65. Bart Custers et al., *Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies*, 28 EUR. J. CRIME, CRIM. L. & CRIM. JUST. 121, 122 (2020). Bitcoin is overwhelmingly used as the cryptocurrency to facilitate ransomware extortion payments, which is likely "a consequence of familiarity within the customer base." *Id.* at 136. Although Bitcoin typically ensures a high degree of anonymity for the hackers receiving extortion payments, there are still ways for law enforcement to identify where ransomware payments are sent. *See* LEWIS, *supra* note 31, at 14–15. Cybersecurity expert James Lewis explains,

> [T]here are still instances in which [a] cybercriminal using Bitcoins can be identified, either through IP address mapping or accidental leaks by web trackers. As a result, a number of attempts have been made at developing a truly anonymous cryptocurrency that could provide greater security to cybercriminals. The three most popular today are Dash, Monero, and Zcash.

Id. at 15 (footnotes omitted).

damage.'"[66] Ransomware technology has become increasingly sophisticated in recent years.[67]

In the early years, "locker ransomware" was the predominant variant of ransomware attacks.[68] Locker ransomware—such as WinLocker and Master Boot, which were predominant in the early days of the proliferation of ransomware—blocks a victim's access to using the computer, its interface, and its files.[69] Locker ransomware does not alter or access the files within the computer.[70] Instead, locker ransomware merely adds a new lock to a computer, which can be imagined as a metaphorical vault.[71] Since the contents of the vault are unaltered, users can first recover the computer's contents by paying to unlock the ransomware.[72] However, law enforcement experts also have other options, such as "bypass[ing] the door by (metaphorically) drilling out the lock, taking the door off its hinges, or just removing the walls from around the unit's contents."[73] As a result, although this type of ransomware is still employed,[74] cybercriminals have since created more sophisticated and problematic iterations of ransomware.[75]

The predominant technology employed in ransomware attacks today is

66. James A. Sherer et al., *Ransomware—Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web*, 23 RICH. J.L. & TECH. ANN. SURVEY 1, 6 (2017) http://jolt.richmond.edu/2017/04/30/volume23_annualsurvey_sherer/.

67. *See id.* at 10 (emphasizing that while "many earlier forms" of ransomware technology are still in use, "[r]ansomware's efficacy has improved over the decades since its introduction").

68. *See id.* at 6.

69. *Id.* at 7.

70. *See id.*; *see also* Amy Deen Westbrook, *A Safe Harbor for Ransomware Payments: Protecting Stakeholders, Hardening Targets and Defending National Security*, 18 N.Y.U. J.L. & BUS. 391, 400 (2022) ("'Locker' ransomware holds the user's data behind a locked interface, demanding that the victim pay the ransom to unlock the data. Under such an attack, a computer may be unusable, but data files may be untouched.").

71. *See* Sherer et al., *supra* note 66, at 7.

72. *See id.*

73. *See id.*

74. *See id.* at 10 (third alteration in original) (footnotes omitted) ("[M]any earlier forms [of ransomware] are still in use. This may be due in part to its inherent longevity, as one key element of older Ransomware's functionality is the malicious way in which its self-propagating features make it incredibly difficult to eliminate. Some legacy Ransomware variations are no longer in circulation, but certain '[m]alware that was released years—in some cases, decades—ago is still alive and well today,' making awareness of modern Ransomware's progenitors required knowledge for practitioners active in this space.").

75. *See, e.g.*, Custers et. al., *supra* note 65, at 124 ("The threat of ransomware developed rapidly in recent years. . . . By 2017, the number of ransomware families exploded, their impact significantly overshadowing other malware threats such as banking Trojans.").

called "Cryptoware"[76] or "Crypto Ransomware."[77] To a victim locked out of their system, Cryptoware attacks appear the same as locker ransomware.[78] In both instances, victims are required to pay a ransom in exchange for access to their files.[79] However, Cryptoware typically enables users to keep using the computer but encrypts files on the target computer.[80] From law enforcement's perspective, recovering access by cracking the code is functionally impossible.[81] Cryptoware attaches itself to "unstructured data" within the computer, such as PDFs, photos, and Word and Excel files, and encrypts the individual files and data.[82] Therefore, continuing with the vault metaphor, if law enforcement could find a way to penetrate the metaphorical vault, they would nevertheless find the vault's contents locked up in separate locked vaults with similarly, impossibly complicated codes to crack.[83]

While these two techniques typically target individual computer networks, cybercriminals have increasingly begun to use ransomware "worms" to inflict more catastrophic damage.[84] Ransomware worms work by infiltrating other computers that are tied into the same network.[85] Among the most

76. *See id.* at 121.

77. *See* Sherer et al., *supra* note 66, at 8.

78. *See id.*

79. *See id.*

80. *See id.*; Westbrook, *supra* note 70, at 400 ("'Crypto' ransomware leaves the data accessible to the system but makes it indecipherable and therefore unusable without the decryption key. During a crypto attack, the computer may still be usable, though continuing to use it may spread the ransomware.").

81. *See* Sherer et al., *supra* note 66, at 8.; *Trading in Fear: The Anatomy of Ransomware*, IDX (July 12, 2021), https://www.idx.us/knowledge-center/trading-in-fear-the-anatomy-of-ransomware. Cryptoware uses RSA 2048 encryption to encrypt the files on computer systems. Sherer et al., *supra* note 66, at 8. This encryption technology would take an average computer around 6.4 quadrillion years to crack the code. *Id.*

82. *See* Sherer et al., *supra* note 66, at 8.

83. *See id.* at 9 ("When it comes to Crypto Ransomware, there is no option to drill out the lock, take the door off the hinges, or tear down the wall; each file is locked up separately and indefinitely. Accordingly, this type of Ransomware poses a very different kind of threat and, as such, is handled quite differently by experienced security professionals tasked with solving the problem.").

84. *See* LEWIS, *supra* note 31, at 11. Worms are described as "similar to viruses in that they both have the ability to self-replicate, but viruses require human action to be activated whereas worms begin to self-replicate automatically. Worms can self-propagate through emails, the internet, file-sharing, computer networks or instant messages. Worms' ability to self-propagate renders them particularly difficult to neutralize." Macon Biannucci et al., *Computer Crimes*, 59 AM. CRIM. L. REV. 511, 519 (2022) (footnotes omitted).

85. *See* LEWIS, *supra* note 31, at 11 ("[Worms] work their way through networks to lock out many more computers than just the initial target.").

notorious worm attacks were the WannaCry[86] and the NotPetya incidents.[87] In the NotPetya attack, for example, the target was designed to be used as a cyberweapon against Ukraine.[88] However, the worm was designed to have an uncontrollable trajectory that would quickly and indiscriminately target all of the systems on the same network.[89] One commentator explained, "If the initial attack on Ukraine was the nuclear detonation, the spreading of the worm beyond Ukraine represented the nuclear fallout."[90] In addition to Ukraine experiencing catastrophic damage, the worm also caused major disruptions to several major American multinational companies.[91]

Ransomware viruses with exfiltration capabilities are another problematic emerging trend.[92] These viruses are capable of "stealing target files and locking the user out" of the computer system simultaneously.[93] Also known as "Doxware," this type of ransomware makes it especially difficult for companies and individuals to avoid paying ransoms.[94] This is because, even where victims have uninfected backup drives that would allow them to otherwise ignore a demand for ransom, the cost of having sensitive personal or proprietary information released might be too much to withstand.[95] Doxware attacks frequently target businesses' customer data, which similarly increases the

86. *See id.* (citing the WannaCry ransomware worm).

87. Niall Brennan & Marc Voses, *The Coming Cyber Pandemic: Part II*, NAT'L L. REV. (Aug. 10, 2020), https://www.natlawreview.com/article/coming-cyber-pandemic-part-ii#google_vignette ("[T]he world faced what has been referred to as the most devastating cyberattack in history. In June 2017, the NotPetya cyberattack occurred, causing staggering collateral damage. . . . NotPetya was engineered to spread on its own accord, both quickly and without a concrete direction. . . . [NotPetya] left an estimated $10 billion of destruction in its wake.").

88. *See id.*

89. *See id.*

90. *Id.*

91. Patrick Reevell et al., *Massive Cyberattack Spreads Ransomware Across Europe, US*, ABC NEWS (June 27, 2017, 6:16 PM), https://abcnews.go.com/International/massive-cyberattack-strikes-europe/story?id=48303592. Companies such as Maersk (the largest multinational shipping firm), Mondelez (a New Jersey-headquartered food and beverage company), Merck (an American multinational pharmaceutical company), and DLA Piper (one of the largest global firms) all experienced major disruptions to their operations. *Id.* The damage in Ukraine, the target of the attack, was even more catastrophic. *Id.* The Ukrainian government confirmed major banks, telecom providers, and "[e]ven radiation monitoring at the Chernobyl nuclear power station was impacted, with technicians forced to take measurements around the ruined station manually after their Windows computers were knocked out . . . ." *Id.*

92. *See* LEWIS, *supra* note 31, at 11.

93. *See id.*

94. *See* Sherer et al., *supra* note 66, at 9.

95. *See* Stupp, *supra* note 27.

pressure on companies to comply and pay the ransoms.[96] Doxware was featured in a staggering "81% of ransomware attacks during the second quarter of 2021."[97]

Although ransomware is highly automated in its spread, planting the ransomware still typically requires at least some human error.[98] To enact a ransomware attack against a company, for example, hackers will typically utilize common tactics such as spear phishing emails.[99] Malware can also infect computers where an individual visits a compromised website on a computer that lacks up-to-date "browsers, browser plugins, and other software."[100] While some hackers send mass phishing emails "in hopes of hitting 'as many individual targets . . . as quickly as possible' by virtue of sheer volume," other hackers send out highly particularized and tailored emails to evade victims' suspicions.[101] Steven J. Murdoch, professor of security engineering at University College London, cynically noted, "A sufficiently well-designed phishing email will get clicked on 100 percent of the time," because the emails are seemingly sent from a reliable source on a matter that would likely come from that source.[102] This makes sense, as sophisticated phishing emails will appear to come from an individual whom the victim knows, from an email address nearly identical to the real person who was thought to have sent the email, and refer to subjects that the real person would likely discuss.[103] Very few

96. *See id.*

97. *See id.*

98. *See* Sherer et al., *supra* note 66, at 10. *But cf.* Dana Priest et al., *Private Israeli Spyware Used to Hack Cellphones of Journalists, Activists Worldwide*, WASH. POST, https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/ (July 18, 2021, 8:15 PM) (noting the increasing prevalence of "zero-click" malware attacks where the cybercriminals can plant malware into a device without a user touching an infected link).

99. *See* Sherer et al., *supra* note 66, at 10–11. Ransomware attacks are also perpetrated via the use of "'exploit kits,' '[w]eb exploits and drive-by downloads,' 'infected removable drives, infected software installers,' and 'mass phishing campaigns.'" *See id.* at 11 (footnotes omitted).

100. *See id.* at 11.

101. *See id.* at 12 (alteration in original).

102. Isabella Kwai, *Train Workers' Covid Bonus Offer Turns Out to Be a Phishing Test*, N.Y. TIMES (May 13, 2021), https://www.nytimes.com/2021/05/13/world/europe/phishing-test-covid-bonus.html. A British railroad company's controversial phishing test exemplifies the effectiveness of phishing. *Id.* The company conducted a phishing test by sending an email that seemingly came from the company's payroll department that promised a "one-off" thank you bonus for the company's employees who worked tirelessly through the most dangerous days of the COVID-19 pandemic. *Id.* The employees who clicked the link and entered their login details "discovered that there was no bonus after all, only a notice that the email was a security test, measuring recipients' susceptibility to messages faked by outside hackers." *Id.*

103. *See id.*

individuals stop to verify every email address for every email they receive if no other signs arouse suspicion.[104]

B. The Business Model of Ransomware

In 2015, ransomware attacks exploded as the ransomware gangs who wrote the malware code began to sell their technology to third-party criminals.[105] Prior to this proliferation, "ransomware campaigns were typically run by organized crime groups that wrote their own code."[106] However, ransomware gangs realized that they could make more money by leasing or selling their malware technology to less technologically-savvy criminals, who then could use the technology to extort targets themselves.[107] After lowering the barrier of entry for executing ransomware attacks to those who lacked the technological sophistication to write the code themselves, the number of reported ransomware attacks grew exponentially.[108] Indeed, during this time period, the FBI reported that $24 million in ransom payments made in 2015 jumped to $209 million in ransom paid in just the first quarter of 2016.[109] Since 2019, the number of ransomware attacks has only continued to increase in frequency and disruptiveness against targets primarily situated in the United States.[110] This section will examine the two primary business models of ransomware attacks today: the ransomware toolkit model and the RaaS model.[111]

104. *See id.*
105. *See* LEWIS, *supra* note 31, at 11.
106. *See id.*
107. *See id.*
108. *See id.*
109. *See id.*
110. *See* Westbrook, *supra* note 70, at 402–03 (footnotes omitted) ("The pace of ransomware attacks has continued to accelerate, breaking records in 2020 and 2021 with the United States bearing the brunt. One factor contributing to the number of attacks in 2020 was the COVID-19 pandemic, which shifted a substantial part of the U.S. workforce to working from home. One survey found that, during the pandemic, over a third of companies did not practice common cybersecurity protocols such as phishing training and multi-factor authentication. Remote work required people to do business from out-of-network, relatively unsecured, computers. A computer network is only as strong as its least vigilant user, and during the pandemic many users were overstretched and distracted.").
111. *See* Sherer et al., *supra* note 66, at 16–18.

1. Early Origins: Ransomware Toolkit Model

First, cheap and effective ransomware toolkits have played a major role in the explosion of ransomware attacks.[112] These toolkits allow hackers to lock victims out of their systems and are widely available across the dark web.[113] The proliferation of such toolkits is due in large part to their cheap price and ease of use, which allows technical novices to conduct disruptive attacks.[114] Although the cybercriminals launching these attacks are not particularly technologically savvy, the "Tor" network, which encrypts users' traffic and then "rout[es] it through multiple random relays on its way to its destination," allows purchasers of ransomware kits to evade law enforcement by remaining nearly completely anonymous while accessing the dark web.[115]

Ransomware toolkits are currently highly affordable.[116] Depending on the complexity of the ransomware being sold, kits can vary from under a dollar

112. *See* LEWIS, *supra* note 31, at 11.

113. *See* LEWIS, *supra* note 31, at 11. For those who seek out the technology, it can be quickly found across the dark web. *Id.* at 12. An early kit marketed,

> You always wanted a Ransomware but never wanted two pay Hundreds of dollars for it? This list is for you!?? Stampado is a cheap and easy-to-manage ransomware, developed by me and my team. It's meant two be really easy-to-use. You'll not need a host. All you will need is an email account.

See Sherer et al., *supra* note 66, at 16*; see also* Rob Thubron, *Vicious New Ransomware Available on Dark Web for Just $39*, TECHSPOT (July 15, 2016, 12:45 PM), https://www.techspot.com/news/65603-vicious-new-ransomware-available-dark-web-39.html.

114. *See* Rick McElroy et al., *Dark Web Ransomware Economy Growing at an Annual Rate of 2,500%*, ENTERPRISE IT NEWS (Nov. 3, 2017, 12:41 AM), https://www.enterpriseit-news.com.my/dark-web-ransomware-economy-growing-at-an-annual-rate-of-2500/.

115. *See* LEWIS, *supra* note 31, at 12. Tor is an acronym that stands for "The Onion Router." *Id.* Tor, in simple terms, is an internet browser that individuals can use to "anonymously browse ordinary sites like Wikipedia or YouTube." *Id.* However, Tor is frequently used by cybercriminals "to access special 'dot.onion' addresses on the dark web, which serves as the home for most internet black markets." *Id.* In addition to other illegal products that are freely and anonymously sold on "dot.onion" websites, users can anonymously purchase ransomware largely without fear of legal consequences, as Tor is "considered to be highly resilient to law enforcement." *See id.* at 12 ("This process makes it nearly impossible for law enforcement agencies to track users or determine the identities of visitors to certain sites.").

116. *See* McElroy et al., *supra* note 114 ("Unlike many other forms of cyberattacks, ransomware can be quickly and brainlessly deployed with a high probability of profit. As our research found, these dark web economies are empowering even the most novice criminals to launch ransomware attacks via do-it-yourself (DIY) kits and providing successful ransomware authors with annual incomes into six figures. . . . There are currently 6,300+ estimated dark web marketplaces selling ransomware, with 45,000 product listings. The prices for do-it-yourself (DIY) kits range from $0.50 to $3K. The median price is $10.50.").

to several thousand dollars for specialized offerings.[117] The median cost is on the lower end of this spectrum, costing criminals just $10.50 for a ransomware kit.[118] In 2018, over 6,000 online marketplaces sold over 45,000 different products.[119] The number of criminals buying these kits is alarmingly large.[120] The FBI estimated that one dark web marketplace that has since been shut down by authorities, AlphaBay, "serviced over 200,000 users and had 40,000 vendors."[121]

Despite the massive number of criminal buyers using these ransomware toolkits, some experts have estimated that the number of those creating the kits is fairly small.[122] In 2015, one estimate by the deputy director of the United Kingdom's National Cybercrime Unit noted that the economy of sellers was "built on the work" of less than two hundred people.[123] Selling such kits can often produce handsome profits for criminals who might be wary of defrauding people directly themselves.[124] The ransomware kit model has become less prevalent with the rise of the RaaS model.[125] Nevertheless, it remains a major nuisance to American consumers and has led to significant economic losses in the aggregate.[126]

117. *See id.*; Alex Scroxton, *Buy 'Plug-n-Play' Malware for the Price of a Pint of Beer*, COMP. WEEKLY (July 21, 2022, 5:30 PM), https://www.computerweekly.com/news/252523004/Buy-plug-n-play-malware-for-the-price-of-a-pint-of-beer ("A wide variety of malwares and vulnerability exploits can be bought with ease on underground marketplaces for about $10 (£8.40) on average, according to new statistics[—]only a few pennies more than the cost of London's most expensive pint of beer.").

118. *See* McElroy et al., *supra* note 114.

119. *See* LEWIS, *supra* note 31, at 11.

120. *See id.* at 13 ("[T]he number of participants in these communities is massive . . . .").

121. *Id.*

122. *Id.*

123. *Id.*

124. *See id.* ("There are numerous ways for a cybercriminal to profit without ever having to engage in the 'traditional' cybercrime acts like financial fraud or identity theft."). Individual developers of ransomware kits are estimated to be able to net over "twice the annual salary of a software developer in Eastern Europe, where most of the criminals operate." *Id.* Even without ever conducting an actual attack themselves, ransomware developers can make over $100,000. *Id.*

125. *Id.* at 11.

126. *See* Sherer et al., *supra* note 66, at 10 (noting the prevalence and longevity of earlier strains of ransomware).

2. Big Business: The Ransomware-as-a-Service Model

The RaaS model is the source of the most sophisticated ransomware attacks, which can often evade and cripple even the best cyber defenses.[127] For successful ransomware attacks, the hacker needs "(1) access to [the] compromised computer[], (2) malware to remotely encrypt the victim's data and (3) [the know-how to] launder ransom payments."[128] In the RaaS model, there are cybercriminals who are specialists in each of these areas who work together with varying levels of involvement to execute attacks.[129]

In their purest form, ransomware gangs are separate entities from affiliates who execute the attacks.[130] The ransomware gangs typically only write the malware but do not breach computer systems themselves.[131] Instead, the ransomware gangs sell or lease their malware to affiliates.[132] Meanwhile, the affiliates are responsible for targeting and executing the attacks.[133] Ransomware gangs typically receive a commission for the successfully extracted ransoms.[134] On occasion, however, experts have observed some models where ransomware gangs charge affiliates up-front fees or lease time blocks to run the campaigns.[135]

Affiliates are primarily responsible for the targeting and execution of attacks.[136] In the RaaS model, email phishing is "by far the most popular means of compromising target computers, meaning that with access to darknet RaaS offerings, anyone with the ability to successfully phish a target can begin to profit from ransomware."[137]

In the RaaS model, even where the ransomware gang authors disagree

127. *See* LEWIS, *supra* note 31, at 12 ("[E]xperienced criminals are able to focus on developing more specialized skill sets, confident in their ability to find others within the thriving darknet ecosystem who can complement their services, and with whom they could collaborate to develop new tools of unprecedented sophistication.").

128. Dwyer, *supra* note 18.

129. *See id*.; *see also* McElroy et al., *supra* note 114 ("Ransomware sellers are increasingly specializing in one specific area of the supply chain, further contributing to ransomware's boom and econom[ic] development.").

130. *See* Kramer et al., *supra* note 52.

131. *Id.*

132. *Id.*

133. *Id.*

134. *See* LEWIS, *supra* note 31, at 11.

135. *Id.*

136. *Id.*

137. *Id.*

with the affiliate's target and have no input in choosing it, the ransomware gang still profits from the attack.[138] For example, in the Colonial Pipeline attack previously discussed in the Introduction section, the ransomware gang responsible, DarkSide, released a statement criticizing their affiliate for targeting the pipeline.[139] In a public statement, DarkSide explained that their affiliate "partners" had "decided to target Colonial Pipeline without the hacking group's knowledge."[140] This situation encapsulates the dangers of the RaaS model: ransomware gangs are leasing out easily accessible weapons of mass destruction with no oversight, no code of ethics, and no repercussions.[141]

Ultimately, while ransomware gangs' criminal business model relies on the gang affiliates to provide victims with the encryption keys to unlock their servers when victims pay, every transaction is unpredictable.[142] Law enforcement authorities typically advise that companies invest heavily in cybersecurity, as if strong cybersecurity alone is a perfect defense against ransomware attacks.[143] However, the reality for American companies is that even with the best cybersecurity, breaches still frequently occur, and paying the ransom is often the only option to avoid debilitating disruption costs.[144] Ultimately, while some commentators note that hackers typically stick to their word and provide the encryption keys when victims pay the requested ransom, there are many examples of companies paying the ransom and never receiving the key.[145] Moreover, experts emphasize that the only guaranteed way to restore

138. *See, e.g.*, Cohen et al., *supra* note 10 (reporting that DarkSide still pocketed their commission despite apparently disagreeing with its affiliate's actions).

139. *Id.*

140. *Id.* The ransomware gang stated, "We are apolitical, we do not participate in geopolitics, do not need to tie us with a defined government and look for our motives . . . . Our goal is to make money, and not creating problems for society. From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future." *Id.* Binary Defense, an independent cyber intelligence firm, confirmed DarkSide's statement was authentic. *Id.*

141. *See, e.g.*, *id.*

142. *See* Sherer et al., *supra* note 66, at 18 ("Some commentators note that there is 'some honour among thieves,' where 'hackers almost always honour their word and provide the encryption key to those who make timely online payments.' Others disagree, noting that a decision to pay does not consistently restore functionality . . . .").

143. *See* Eaton & Volz, *supra* note 5 ("For years, the Federal Bureau of Investigation has advised companies not to pay when hit with ransomware, a type of code that takes computer systems hostage and demands payment to have files unlocked. Doing so, officials have said, would support a booming criminal marketplace.").

144. *See id.* ("[M]any companies, municipalities and others debilitated by attacks do pay, concluding it is the only way to avoid costly disruptions to their operations.").

145. *See* Sherer et al., *supra* note 66, at 18–19.

the affected system to its normal operation is to shut down the system and remove the malware.[146] However, when high-pressure businesses are attacked, shutting down operations to reboot a network for even a few hours can have life or death implications.[147]

C. Factors Motivating Attacks and the Cost to Society

The targets of ransomware attacks can be separated into two categories: small-level attacks launched at lower-level targets and attacks aimed at major, high-value targets.[148] Although the latter type of attacks will be the focus of this section, the former category nevertheless deserves attention.[149]

The first category of targets, typically aimed at individuals and small businesses, are often launched in high volumes, demand lower ransoms, and are less tailored to the specific victim.[150] These attacks are hard to address and are problematic when aggregated; however, the attacks are more of a nuisance to Americans' online safety than they are a threat to national security.[151]

The second category of attacks—which will be the focus of this section—are more sophisticated, use RaaS malware, and pose a greater national security risk.[152] These attacks typically target specific companies that are capable of paying hundreds of thousands to millions of dollars in ransom.[153] While hackers have launched ransomware attacks for non-monetary purposes,[154] the

146. *Id.* at 19.

147. *See, e.g.*, Stacy Weiner*, The Growing Threat of Ransomware Attacks on Hospitals*, AAMC (July 20, 2021), https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals (reporting on the staggering number of ransomware attacks on hospitals and the real threat that hospital system computer failure poses of killing patients in need of critical care).

148. *See* Custers et al., *supra* note 65, at 133. *See generally*, Sherer et al., *supra* note 66, at 10–12 (detailing ransomware attacks differing delivery mechanisms).

149. *Compare infra* text accompanying notes 150–51, *with infra* text accompanying notes 152–68.

150. *See* Custers et al., *supra* note 65, at 132.

151. See *id.* at 123, 132 (noting that these attacks tend to encrypt individual's "family pictures, personal letters and financial documents" while demanding approximately $250 for the encryption key).

152. *See* Sherer et al., *supra* note 66, at 17–18.

153. *See* Carly Page, *Ransomware Recovery Can be Costly, and Not Just Because of the Ransom*, TECHCRUNCH (Aug. 18, 2021, 8:30 AM), https://techcrunch.com/2021/08/18/ransomware-recovery-can-be-costly-and-not-just-because-of-the-ransom/ (noting the average cost to companies hit by ransomware attacks is approximately $5.6 million with nearly $800,000 of the cost accounting for ransoms paid).

154. *See* Ellen Ioanes, *Kim Jong Un Has Quietly Built a 7,000-Man Cyber Army That Gives North Korea an Edge Nuclear Weapons Don't*, BUS. INSIDER (June 17, 2020, 6:05 AM), https://www.businessinsider.com/north-korea-kim-jong-un-cyber-army-cyberattacks-nuclear-weapons-2020-6.

overriding motivation for these attacks is money.[155] Nevertheless, unlike a typical bank robbery where the risk to society is somewhat contained to the bank and its immediate surroundings, ransomware attacks present significant national security risks.[156]

Ransomware attacks threaten national security because they habitually target companies and government entities that are critical to the United States' vital infrastructure.[157] The RaaS business model incentivizes hackers to target enterprises where the value of encrypted files and the cost of the ransomware's prolonged disruption is greater than the ransom payment that is demanded.[158] The Colonial Pipeline attack—where the social and financial cost of shutting down its operations for an indefinite amount of time to restart its systems was magnitudes higher than the cost of the $4.4 million ransom amount demanded—is a prime example of the strategy's success in practice.[159] The chief executive officer of Colonial Pipeline defended his decision to pay as a simple cost-benefit analysis: the societal and opportunity costs of a prolonged pipeline shutdown were much greater than the $4.4 million ransom.[160]

Adversarial countries, in particular, have launched ransomware attacks against the United States for various political purposes. *Id.* For example, North Korea has effectively employed ransomware to advance its agenda abroad. *Id.* Former United States Assistant Secretary of State for East Asian and Pacific Affairs, Daniel Russel, noted that North Korea's "[c]yber theft effectively neutralizes UN and US sanctions against North Korea," because if the pariah state "is denied a billion dollars in the sale of coal and iron and mushrooms, but it can go out and steal a billion dollars, then sanctions are not going to have the intended effect." *Id.* Russel argues,

> The WannaCry virus, on the one hand, was ransomware; you could argue that it's aimed at getting money, but it caused a huge disruption of hospitals in the UK and, potentially, in something like 100-plus other countries where they had disseminated the ransomware. This was software that brought the operation of critical facilities to a standstill. This is not hacking; this is cyber warfare.

Id.

155. *See* Samara Lynn & Catherine Thorbecke, *Why Ransomware Cyberattacks Are on the Rise*, ABC NEWS (June 4, 2021, 2:00 AM), https://abcnews.go.com/Technology/ransomware-cyberattacks-rise/story?id=77832650 (noting that a primary motive behind such attacks is financial, while Russia's failure to prosecute and extradite cybercriminals has a political dimension).

156. *See* David Gura, *U.S. Suffers Over 7 Ransomware Attacks an Hour. It's Now a National Security Risk*, NPR (June 9, 2021, 5:24 PM), https://www.npr.org/2021/06/09/1004684788/u-s-suffers-over-7-ransomware-attacks-an-hour-its-now-a-national-security-risk (emphasizing the national security implications of ransomware attacks on American national security); *see also infra* Section IV.C.

157. Gura, *supra* note 156.

158. *See generally* Eaton & Volz, *supra* note 5.

159. *Id.*

160. *See id.* ("Mr. Blount acknowledged publicly for the first time that the company had paid the ransom, saying it was an option he felt he had to exercise, given the stakes involved in a shutdown of such critical energy infrastructure.").

This reality makes the companies and government entities that are responsible for America's critical infrastructure particularly enticing targets for hackers.[161] Hackers have targeted hundreds of hospitals with ransomware attacks in recent years.[162] As the COVID-19 pandemic has pushed America's hospitals to the brink of collapse, hackers took advantage of the hospitals' vulnerability by increasing their number of attacks.[163] Josh Corman, the head of CISA's COVID-19 task force, noted, "Hospitals' systems were already fragile before the pandemic. Then the ransomware attacks became more varied, more aggressive, and with higher payment demands."[164] In the first half of 2020, there was a forty-five percent uptick in attacks against the healthcare sector.[165] The risk of ransomware attacks to the healthcare industry is manifest, with "more than 1 in 3 health care organizations globally" being hit by ransomware in 2020.[166] The reality of these attacks is that "it can take just one employee falling for a fake email" for the ransomware to compromise the entire hospital's ability to provide patients with even the most basic types of care.[167] In summary, even when money is supposedly the sole motivation for an attack, the hackers employing the ransomware have demonstrated their inherent intent to endanger the physical safety of Americans.[168]

161. *Deputy Attorney General Rosenstein Delivers Remarks at the 2017 North American International Cyber Summit*, U.S. DEP'T OF JUST., https://www.justice.gov/opa/speech/deputy-attorney-general-rosenstein-delivers-remarks-2017-north-american-international (Oct. 30, 2017). In a speech delivered at the 2017 North American International Cyber Summit, Deputy Attorney General Rod Rosenstein warned,

> Whether you work for local law enforcement, a utility provider, a hospital, or a small or large company, you need to protect your critical infrastructure against cyber infiltration. The threat that cybercriminals pose to public entities and private businesses is substantial. A single intrusion could mean economic loss, bankruptcy, and in some cases, loss of human life.

Id.

162. *See* Weiner, *supra* note 147.

163. *Id.*

164. *See id.* (quoting Josh Corman, Head of the CISA COVID-19 task force).

165. *Id.*

166. *Id.* Hospital executives are acutely aware of the issue, with one UTHealth officer stating that "[c]ybercriminals try every hospital, every day; every computer, multiple times a day." *Id.*

167. *Id.*

168. *See supra* notes 161–67 and accompanying text.

III. THE FTO LIST TODAY: THE CURRENT STATE OF 8 U.S.C. § 1189

A. The History of the FTO List

Although the FTO list took center stage in the years following the September 11 Attacks, the FTO list was created by the 1996 Antiterrorism and Effective Death Penalty Act (AEDPA), which amended § 219 of the Immigration and Nationality Act.[169] In 1997, the State Department released its first FTO list, which initially contained thirty entities.[170] The groups that the State Department has subsequently added have ranged from jihadist terrorist movements (like Al Qaeda) to Colombian paramilitary drug traffickers (like the United Self-Defense Forces of Colombia).[171] The FTOs listed have operated throughout the world in regions like the Middle East, Southeast Asia, Europe, South America, and Africa.[172] Since the list's inception, the State Department has removed twenty organizations.[173] There are currently sixty-eight active FTOs listed as of September 2022.[174]

B. The Process of Designating an FTO

Although Congress and the judiciary serve critical functions in the process, the FTO designation procedure is primarily a function of the Executive Branch.[175] Despite taking place primarily within the Executive Branch, the process for designating an FTO is stringent, comprehensive, and provides ample opportunities for oversight.[176] According to the United States Government Accountability Office (GAO), the State Department—which is statutorily tasked with producing and editing the FTO list under 8 U.S.C. § 1189—has developed a six-step process for designating an FTO.[177] Although the process

169. *See* AUDREY KURTH CRONIN, CONG. RSCH. SERV., RL32120, THE "FTO LIST" AND CONGRESS: SANCTIONING DESIGNATED FOREIGN TERRORIST ORGANIZATIONS 1–2 (2003).

170. *Id.* at 6.

171. *See Foreign Terrorist Organizations*, U.S. DEP'T OF STATE, https://www.state.gov/foreign-terrorist-organizations/ (last visited Sept. 30, 2022).

172. *See id.*

173. *See id.*

174. *See id.*

175. *See id.*

176. *See infra* text accompanying notes 177–99 (detailing the process of designating a criminal organization as an FTO).

177. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-15-629, COMBATING TERRORISM: FOREIGN TERRORIST ORGANIZATION DESIGNATION PROCESS AND U.S. AGENCY ENFORCEMENT ACTIONS 5

takes place primarily within the Executive Branch, the State Department does not construct the list alone but consults with several other bureaus and agency partners at various steps throughout the process.[178]

The Bureau of Counterterrorism (CT), a subsection of the State Department, carries out the first several steps.[179] First, CT is tasked with identifying potential targets for designation.[180] CT advertises that its criteria for identifying potential new organizations for designation includes (1) whether an organization has carried out an actual terrorist attack, (2) whether the group is actively "engaged in planning and preparations for possible future acts of terrorism," or (3) whether the group retains the capability and intent to carry out future attacks.[181] CT then conducts what is referred to as an "equity check," where CT "consults with its stakeholders to determine if any concerns should prevent the designation of the target organization."[182]

After CT identifies a potential FTO, the second step is CT's preparation of a "detailed 'administrative record.'"[183] The administrative record "is a compilation of information, typically including both classified and open source[d] information, demonstrating that the statutory criteria for designation have been satisfied."[184] Put simply, to qualify statutorily as an FTO under 8 U.S.C. § 1189, the potential designee (1) is a foreign organization, (2) that is engaging in terrorist activity, and (3) the organization's terrorist activity or terrorism must threaten the security of American nationals or the national

(2015) ("State has developed a six-step process for designating foreign terrorist organizations."); CRONIN, *supra* note 169, at 1–3, 10 (describing the designation process as primarily a function of the Executive Branch with a limited number of opportunities for judicial review and congressional oversight).

178. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 177, at 5.

179. *Id.* at 6.

180. *See Foreign Terrorist Organizations*, *supra* note 171.

181. *Id.*

182. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 177, at 6. According to GAO, CT consults "with other State bureaus, federal agencies, and the intelligence community, among others, to determine whether any law enforcement, diplomatic, or intelligence concerns should prevent the designation of the target organization." *Id.* at 7. GAO explained,

> If any of these agencies or other bureaus has a concern regarding the designation of the target organization, it can elect to place a "hold" on the proposed designation, which prevents the designation from being made until the hold is lifted by the entity that requested it. The equity check is the first step where an objection to a designation can be raised; however, in practice, a hold can be placed at any step in the FTO designation process prior to the Secretary's decision to designate.

Id.

183. *See Foreign Terrorist Organizations*, *supra* note 171.

184. *Id.*

security (national defense, foreign relations, or the economic interests) of the United States.[185]

Third, CT submits this compilation to the Secretary of State's Office of the Legal Adviser, the Justice Department, and the Treasury Department.[186] This stage is referred to as the "Clearance Process."[187] This is where the Secretary of State and its partnering agencies complete a final review of the administrative record to confirm that it fits the FTO statute.[188] The Justice and Treasury Departments may suggest edits to the administrative record if necessary.[189] The process is completed when the Justice and Treasury Departments provide the State Department with signed letters of concurrence indicating that the record is legally sufficient.[190]

Fourth, the materials supporting the designation are sent to the Secretary of State for a final review and decision.[191] The Secretary may authorize the designation if the legal elements are satisfied.[192] Designating a group as an FTO has severe political implications.[193] As a result, America's domestic and foreign policy interests might be better served in certain contexts by using different methods to sanction an organization that otherwise meets the statutory definition of an FTO.[194] Indeed, the State Department has used other

185. *See* 8 U.S.C. § 1189; *Foreign Terrorist Organizations*, *supra* note 171. More precisely, 8 U.S.C. § 1189 states:

> The Secretary is authorized to designate an organization as a foreign terrorist organization in accordance with this subsection if the Secretary finds that—
>
> (A) the organization is a foreign organization;
>
> (B) the organization engages in terrorist activity (as defined in section 1182(a)(3)(B) of this title or terrorism (as defined in section 2656f(d)(2) of title 22), or retains the capability and intent to engage in terrorist activity or terrorism); and
>
> (C) the terrorist activity or terrorism of the organization threatens the security of United States nationals or the national security of the United States.

Id. (footnote omitted).

186. *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 177, at 6–7.

187. *See id.*

188. *See id.*

189. *See id.*

190. *See id.* at 7.

191. *See id.*

192. *See id.* ("The Secretary of State is authorized, but not required, to designate an organization as an FTO if he or she finds that the legal elements for designation are met.").

193. *See* CRONIN, *supra* note 169, at 5 ("The FTO list has unique importance not only because of the specific measures undertaken to thwart the activities of designated groups but also because of the symbolic, public role it plays as a tool of U.S. counterterrorism policy.").

194. *See id.* at 9–10 ("Competing foreign policy concerns often result in decisions to keep groups off the list. This is not necessarily a problem, as U.S. foreign policy considers numerous competing

Executive Branch terrorist lists,[195] targeted sanctions, and various diplomatic strategies in situations where listing an otherwise qualified entity as an FTO would be counterproductive to United States' policy goals.[196]

Fifth, if the Secretary of State authorizes designation, Congress is notified and given a seven-day period to review the designation.[197] Congress has the option to block the designation or to allow the designation by either affirmatively approving it or letting the seven-day waiting period expire.[198]

Finally, if Congress chooses to allow the designation, the State Department "is required to publish the designation announcement in the Federal

---

priorities in any given situation. The law 'authorizes' but does not require the Secretary of State to make any given designation. If there are countervailing foreign policy priorities, then his or her judgment prevails. Nonetheless, inconsistencies of standards from the perspective strictly of terrorism can make the U.S. government appear hypocritical, especially in the eyes of those who see the FTO list only in black and white terms and may not appreciate the existence of other terrorist lists. Statements about organizations that are not designated regularly appear in the press, journals[,] and academic writing, for example. Having such a high-profile list can politicize and oversimplify what is actually a complex web of legal sanctions that may be in addition to, or instead of, those pursuant to the AEDPA."); *cf.* Madison Standon, *Applying the "War on Terror" to the "War on Drugs:" The Legal Implications and Benefits of Recategorizing Latin American Drug Cartels as Foreign Terrorist Organizations*, 22 SAN DIEGO INT'L L.J. 365, 407 (2021) (arguing against designating Latin American drug cartels as FTOs because it "would exacerbate the problems seen in the War on Terror and the War on Drugs, by diverting funding from other necessary areas of government" and "strain[] foreign relations").

195. *See* CRONIN, *supra* note 169, at 3–4. There are four other prominent terrorism lists. *Id.* at 3–5. One of the other prominent lists includes the "state-sponsors of terrorism" list, which includes nations that have "repeatedly provided support for acts of international terrorism." *Id.* at 3. Recently, the Trump Administration blurred the lines between this list and the FTO list by adding the Islamic Revolutionary Guard Corps, a particularly nefarious wing of the Iranian military, to the FTO list. *See* Edward Wong & Eric Schmitt, *Trump Designates Iran's Revolutionary Guards a Foreign Terrorist Group*, N.Y. TIMES (Apr. 8, 2019), https://www.nytimes.com/2019/04/08/world/middleeast/trump-iran-revolutionary-guard-corps.html. Second, the "specially designated terrorists" list was enacted pursuant to an executive order in 1995 and oriented towards "persons (individuals and entities) who threaten to disrupt the Middle East Peace Process." *See* CRONIN, *supra* note 169, at 4. Third, following the September 11 attacks, "the President invoked the same emergency authorities in Presidential Executive Order 13224, to block 'all property and interests in property' of certain designated terrorists and individuals and entities materially supporting them." *Id.* Both of these lists are "especially targeted toward blocking terrorist financing," "do not have an immigration element" like the FTO list, and are led by the Secretary of the Treasury. *Id.* Fourth, there is a Terrorist Exclusion List that is primarily related to restricting immigration of terrorist organizations and their members. *Id.* at 5.

196. *See* CRONIN, *supra* note 169, at 8–9. One terrorism specialist, Audrey Kurth Cronin, notes, "There may be competing priorities in dealing with a group, such as a desire to engage a group in negotiations or to use the FTO naming as leverage for another foreign policy aim." *Id.* at 9 (discussing the ways in which an FTO designation may be counterproductive to United States foreign policy goals). Countervailing policy priorities often weigh heavily on the Secretary of State's decision. *Id.*

197. *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 177, at 6, 8.

198. *Foreign Terrorist Organizations*, *supra* note 171.

Register and, upon publication, the designation is effective for purposes of penalties that would apply to persons who provide material support or resources to designated FTOs."[199]

C. Constitutional Challenges to 8 U.S.C. § 1189

Although the aforementioned process has drawn the ire of several scholars and commentators, the designation process is both fair and constitutional.[200] Specifically, critics argue that it violates the Fifth Amendment's procedural due process requirement by failing to give listed organizations adequate notice or a pre-designation hearing.[201] Although the statute allows for judicial review of the designation, critics stress that the statute does not permit designated FTOs to present evidence on their own behalf.[202] Moreover, during the judicial review of a designation, the government is free to rely on and present classified information ex parte and in camera without disclosing that information to the FTO contesting its designation.[203]

With respect to FTOs receiving judicial notice, while FTOs do not receive

199. *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 177, at 8.

200. *See* Randolph N. Jonakait, *A Double Due Process Denial: The Crime of Providing Material Support or Resources to Designated Foreign Terrorist Organizations*, 48 N.Y.L. SCH. L. REV. 125, 167 (2004); Eric Broxmeyer, *The Problems of Security and Freedom: Procedural Due Process and the Designation of Foreign Terrorist Organizations under the Antiterrorism and Effective Death Penalty Act*, 22 BERKELEY J. INT'L L. 439, 487 (2004).

201. *See generally* Justin S. Daniel, *Blacklisting Foreign Terrorist Organizations: Classified Information, National Security, and Due Process*, 166 U. PA. L. REV. 213, 219 (2017) (citing various scholarly criticisms of the FTO statute).

202. *See, e.g.*, Andrew V. Moshirnia, *Valuing Speech and Open Source Intelligence in the Face of Judicial Deference*, 4 HARV. NAT'L SEC. J. 385, 405–06 (2013) (footnotes omitted) ("The current scheme for review of FTO designation cannot seriously be called robust judicial review. The People's Mujahedin of Iran (MEK), for example, shows that political favor, rather than actual fact-finding, may determine a group's designation. The group, made up of Marxist Iranian dissidents, focused its attacks again[st] the Islamic Republic of Iran. The group was designated as an FTO in 1997, a move which one Clinton official characterized as 'intended as a goodwill gesture to Tehran and its newly elected moderate president, Mohammad Khatami.' The group appealed this designation for the next 15 years. It presented very strong evidence when seeking de-listing . . . . The Government noted MEK's possible consideration of suicide attacks in Iraq and the MEK's possibly fraudulent fundraising efforts as justification for refusing to de-list the group. The Government's argument was hard to understand, as the MEK was confined to an American-controlled camp at this time and therefore had little to no operational capacity. In a climate where the Government may rely largely on classified (and therefore uncontested) hearsay, there are few, if any, effective avenues of correcting or overturning FTO designations through the courts.").

203. *See* 8 U.S.C. § 1189(c)(2).

"pre-deprivation notice" before the entity is listed in the Federal Register,[204] there is a vital public policy justifying the statute's procedure.[205] First, requiring pre-designation notice would severely undercut the purpose of the FTO statute.[206] This is because giving potential FTOs pre-designation notice "would inform putative organizations that the U.S. is investigating its clandestine activities."[207] In response, the organization "would then (1) tighten up its network—which negatively impacts the ability of the U.S. to gather information on the organization—and (2) withdraw all funds from U.S. controlled banks" to avoid the subsequent freezing of its assets by the Treasury Department.[208]

Second, the requirement for a fair hearing under the Fifth Amendment is also likely satisfied.[209] To determine whether the defendant FTO's procedural due process rights were violated, courts have applied the standard developed by the Court in *Mathews v. Eldrige*.[210] The *Mathews* test weighs (1) "the private interests that will be affected by the official action," (2) "the risk of an erroneous deprivation of such interest of the procedure used, and the probable value, if any, of additional or substitute procedural safeguards," and (3) "the government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirements would entail."[211] Ultimately, courts have determined that the risk of an erroneous deprivation is small, the burden of pre-deprivation hearings would be immense, the level of private interests may vary, and the government's interest in fighting terrorism is substantial.[212] Therefore, the risk of "an organization [withdrawing] its funds and supporters" from the United States is simply too high to justify pre-designation hearings in this context.[213]

204. *See* Schwartz, *supra* note 44, at 314 (noting that while procedural due process typically requires that "affected parties be given . . . 'reasonably calculated'" pre-deprivation notice, "[p]ost-deprivation notice is . . . permissible where pre-deprivation notice is impractical or impossible, and post-deprivation remedies exist").

205. *See id.* at 314–15 (citing public policy undergirding the FTO designation's lack of pre-designation notice).

206. *Id.*

207. *Id.* at 314.

208. *Id.* at 314–15.

209. *See id.* at 315–19.

210. *See* Nat'l Council of Resistance of Iran v. Dep't of State, 251 F.3d 192, 205 (D.C. Cir. 2001) (citing Mathews v. Eldrige, 424 U.S. 319, 335 (1976)).

211. *Id.* at 206.

212. *Id.* at 208.

213. *See* Schwartz, *supra* note 44, at 319.

Finally, the fact that the government is allowed to use classified information upon an FTO appeal for judicial review is similarly justified.[214] The State Department, Department of Justice, Treasury Department, and several other intelligence agencies and executive bureaus all provide input and must agree that an organization's inclusion on the FTO list is justified.[215] As a result, a proponent of the statute explained, "Requiring the disclosure of classified information is akin to asking the U.S. to hand over its secrets to the 'enemy.' Not only would such a requirement frustrate the purposes of the law, but it would also jeopardize national security."[216]

Ultimately, when defending against any existential threat to the United States, the government must balance the often competing interests of protecting citizens' rights and protecting the public's safety.[217] While the threat of terrorism presents a grave threat to Americans' safety and security, the statute's incorporation of post-deprivation judicial notice, and post-deprivation hearing ex parte and in camera is adequate to protect FTOs due process rights.[218] Moreover, unlike other terrorist[219] and cyber-crime[220] sanction lists that were established via executive orders and unanimously upheld as legal, 8 U.S.C. § 1189 was dually approved by both chambers of Congress and requires continued congressional and judicial oversight to approve new FTOs.[221]

214. *See id.* (noting that "national security overrides any limited benefits of disclosure").

215. *See id.* at 320 (". . . [E]very organization listed as an FTO has raised a legitimate flag in the eyes of the U.S. government. A wrongfully designated organization should be able to demonstrate its innocence without access to classified information . . . ."); U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 177, at 5.

216. *See* Schwartz, *supra* note 44, at 320.

217. *See id.* at 321 (emphasizing that "[t]he government must walk a fine line between protecting the rights of its citizens and protecting their safety").

218. *See supra* notes 204–16 and accompanying text.

219. *See, e.g.*, Exec. Order No. 12947, 60 Fed. Reg. 5079 (Jan. 23, 1995); *see also* CRONIN, *supra* note 169, at 4 (noting that the Executive Order 12947 established the "specially designated terrorists" list, which was followed by Executive Order 13224, which created the "Specially Designated Global Terrorists list").

220. *See, e.g.*, Exec. Order No. 13694, 80 Fed. Reg. 18077 (Apr. 1, 2015) (establishing Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities").

221. *See* 8 U.S.C. § 1189.

D. The Consequences of the FTO Designation

The FTO list yielded several bureaucratic and legal advantages in fighting the War on Terror.[222] Chief among the bureaucratic advantages is that the list "provides lucidity in the often complicated interagency process of coordinating the actions of Executive agencies, by giving them a central focal point."[223] The list provides the Treasury Department, State Department, and Justice Department with one singular entity to target with financial sanctions, intelligence operations, immigration sanctions, and prosecution if captured.[224] Similarly, the list is helpful to facilitate the United States' partnership with other governments and allies who are engaged in uniform counterterrorism efforts.[225] Likewise, labeling an entity as an FTO signals to adversarial governments the seriousness with which the United States regards the organization and clarifies the increased cost that adversarial nations will face by continuing to harbor or allow such activity to continue within the adversary's borders.[226]

Socially, another important benefit of the list is to stigmatize and draw attention to the listed groups.[227] The United States carries a significant level of soft power, and the designation of an entity as an FTO brings unwanted attention to the group that can cause social isolation.[228] Moreover, since "[m]any modern terrorist organizations have a varied portfolio of activities, some of which may be ostensibly legitimate," the FTO designation can serve to harm these more legitimate branches of the FTO as well.[229]

If the State Department designates an organization as an FTO, there are three principal legal ramifications.[230] First, the FTO designation bans alien representatives and members of the group from entering the United States and

222. *See* CRONIN, *supra* note 169, at 7.
223. *Id.*
224. *Id.*
225. *Id.*
226. *See Foreign Terrorist Organizations*, *supra* note 171 (explaining that the FTO designation "signals to other governments [the United States'] concern about named organizations"); CRONIN, *supra* note 169, at 8 ("Moreover, states that are, actually or potentially, supporting organizations on the list can be left in no doubt about U.S. policy on the issue. Clearly labeling what the United States government considers a foreign terrorist organization can have significant domestic and international foreign policy advantages. It can be a powerful diplomatic tool, residing in the State Department's Office of the Coordinator for Counterterrorism.").
227. *See Foreign Terrorist Organizations*, *supra* note 171.
228. *See* CRONIN, *supra* note 169, at 7–8.
229. *See id.* at 8.
230. *See Foreign Terrorist Organizations*, *supra* note 171.

makes them removable in certain circumstances.[231] A second more significant consequence is that "any U.S. financial institution that becomes aware that it has possession of or control over funds in which a designated FTO or its agent has an interest must retain possession of or control over the funds and report the funds to the Office of Foreign Assets Control of the U.S. Department of the Treasury."[232] Third, and most significantly for prosecutors, it is unlawful for any person to knowingly provide "material support or resources" to a designated FTO.[233]

The legal ramifications of this third benefit have proven to be vital in turning the tide in the fight against terrorism.[234] The Justice Department confronted the threat of terrorism using "proactive rather than reactive investigations and reorganized itself accordingly."[235] Prosecutors have used the material support statute to identify and threaten individuals "who may be subject to prosecution" for materially supporting terrorism to "convince them to work as informants to help the prosecution build cases against other individuals."[236] The material support statute is unique in that the defendant need not be aware of any specific attack that the FTO is planning.[237] This has aided prosecutors

231. *Id.*; *see* 8 U.S.C. §§ 1182(a)(3)(B)(i)(IV)–(V), 1227(a)(1)(A).

232. *Foreign Terrorist Organizations*, *supra* note 171. Moreover, financial institutions that do not comply are liable for a minimum $50,000 civil penalty. *See* 18 U.S.C. § 2339B(b)(A).

233. *See* 18 U.S.C. §§ 2339A–2339B. Under § 2339A, "the term 'material support or resources' means any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who maybe or include oneself), and transportation, except medicine or religious materials." Moreover, 18 U.S.C. § 2339A(b)(2) states that "'training' means instruction or teaching designed to impart a specific skill, as opposed to general knowledge."

234. *See generally*, Robert Chesney, *Anticipatory Prosecution in Terrorism-Related Cases*, *in* THE CHANGING ROLE OF THE AMERICAN PROSECUTOR 157 (John L. Worrall & M. Elaine Nugent-Borakove eds., 2008) (explaining the importance of the FTO statute and 18 U.S.C. § 2399, its "material support" counterpart, in reducing the flow of resources to FTOs and preventatively prosecuting affiliated individuals).

235. *See* Dwyer, *supra* note 18; *see also* Chesney *supra* note 234, at 163–64 ("The paradigmatic material support defendant in that context is someone who does not pose a personal threat of violence, but whose conduct in providing support might facilitate the ability of others to cause harm. But § 2339B's utility turns out not to be limited to the paradigm case. Because of the breadth of the definition of 'material support or resources,' prosecutors also have been able to employ the statute as a vehicle for anticipatory prosecution of persons who are potentially dangerous in and of themselves.").

236. *See* Keenan, *supra* note 39, at 801.

237. *See* Chesney *supra* note 234, at 160 ("Because this strategy seeks to achieve a degree of prevention without knowledge of which individuals might actually carry out a terrorist attack, enforcement of § 2339B in most instances counts as a method of untargeted prevention; in the typical material support case, the defendant is not viewed as a potentially-dangerous person in their own right, but

because it "allows law enforcement and counterterrorism personnel to act sooner than might otherwise be possible and leverage early-level cooperation to obtain information about other participants."[238]

IV. CONFRONTING THREATS ON THE CYBER FRONTIER USING TRADITIONAL TOOLS: THE APPLICABILITY OF 8 U.S.C. § 1189 TO FOREIGN RANSOMWARE GANGS

The Secretary of State can only list foreign ransomware gangs as FTOs if they fit the statutory requirements outlined in 8 U.S.C. § 1189(a)(1)(A)–(C).[239] To designate an FTO, the statute provides:

> The Secretary is authorized to designate an organization as a foreign terrorist organization in accordance with this subsection if the Secretary finds that—
>
> (A) the organization is a foreign organization;
>
> (B) the organization engages in terrorist activity (as defined in section 1182(a)(3)(B) of this title or terrorism (as defined in section 2656f(d)(2) of title 22), or retains the capability and intent to engage in terrorist activity or terrorism); and
>
> (C) the terrorist activity or terrorism of the organization threatens the security of United States nationals or the national security of the United States.[240]

This Section will examine each element of § 1189 and apply the law to the factual realities of ransomware crime.[241] Although Congress may have intended the statute to apply to foreign organizations committing terrorism with only physical weapons when written in 1996, this Section will explain why the statute allows for the Secretary of State to legally extend the FTO designations to the major ransomware gangs.[242]

---

rather as someone whose conduct facilitates the danger posed by others.").

238. *See* Keenan, *supra* note 39, at 792.

239. *See* 8 U.S.C. § 1189(a)(1).

240. *See* 8 U.S.C. § 1189(a)(1)(A-C).

241. *See infra* Sections IV.A–D.

242. *See infra* Sections IV.A–D.

A. Ransomware Gangs Qualify as Foreign Organizations

To satisfy the first element of § 1189, the Secretary must find that the group is a foreign organization.[243] Although FTOs have litigated their designation on other grounds, "[p]rosecutors have asserted without proof, and defendants have accepted without contesting, that the targeted entity fulfilled the organization requirement under the statute."[244] However, given the unique nature and structure of the ransomware-as-a-service model,[245] whether or not ransomware gangs qualify as "organizations" deserves attention.[246] Ultimately, basic principles of American joint criminal enterprise liability under the federal Racketeer Influenced and Corrupt Organizations Act (RICO) suggests that ransomware gangs qualify as organizations under the FTO statute.[247]

Before defining the meaning of the term "organization" under the FTO statute, it is important to note that the "foreign" requirement is satisfied for every particular major ransomware gang that poses a national security risk to the United States.[248] The most prolific ransomware gangs are from Russia and other former Soviet-bloc countries.[249] According to cybersecurity firm BlackFog, the same eleven foreign ransomware-gang variants—including REvil,[250]

243. *See* 8 U.S.C. § 1189(a)(1)(A).

244. *See* Keenan, *supra* note 39, at 810.

245. *See supra* Section II.B.

246. *See supra* notes 243–44 and accompanying text; *see also infra* notes 248–77 and accompanying text.

247. *See* Keenan, *supra* note 39, at 810; *cf.* Press Release, U.S. Dep't of Just., Four Individuals Plead Guilty to RICO Conspiracy Involving "Bulletproof Hosting" for Cybercriminals," (May 7, 2021), https://www.justice.gov/opa/pr/four-individuals-plead-guilty-rico-conspiracy-involving-bulletproof-hosting-cybercriminals (reporting the DOJ's recent use of the RICO statute to target a cybercriminal organization responsible for renting "Internet Protocol (IP) addresses, servers, and domains to cybercriminal clients, who used this technical infrastructure to disseminate malware used to gain access to victims' computers, form botnets, and steal banking credentials," causing and attempting to cause millions of dollars in losses to U.S. victims).

248. *See infra* notes 248–56 and accompanying text.

249. *See* Uberti, *supra* note 19 (reporting that the Biden administration has focused on "urg[ing] Russian President Vladimir Putin to prosecute ransomware gangs, many of which work out of formerly Soviet states" and pressuring "them to avoid targeting critical infrastructure").

250. Volodymyr Verbyany & Aliaksandr Kudrytski, *U.S. Ransomware Attack Suspect Hails from a Small Ukrainian Town*, BLOOMBERG (Dec. 22, 2021, 4:00 AM), https://www.bloomberg.com/news/articles/2021-12-22/hacking-suspect-s-path-led-teen-genius-to-a-mercedes-maldives (noting REvil's links to Russia).

Conti,[251] DarkSide,[252] CLOP,[253] Egregor,[254] and DoppelPaymer,[255]—were responsible for at least sixty-four percent of the global ransomware threats in the first five months of 2021.[256]

Although 8 U.S.C. § 1189 does not define an "organization," RICO principles of American joint-criminal-enterprise liability can fill this analytical gap if challenged.[257] Put simply, RICO's elements are as follows:

(1) any person,
(2) who
  (a) uses or invests in, or
  (b) acquires or maintains an interest in, or
  (c) conducts or participates in the affairs of, or
  (d) conspires to invest in, acquire, or conduct the affairs of
(3) an enterprise
(4) which
  (a) engages in, or
  (b) whose activities affect, interstate or foreign commerce
(5) through
  (a) the collection of an unlawful debt, or
  (b) the patterned commission of various state and federal crimes.[258]

---

251. Joseph Menn*, Ransomware Attack on Australian Utility Claimed by Russian-Speaking Criminals*, REUTERS, https://www.reuters.com/technology/ransomware-attack-australian-utility-claimed-by-russian-speaking-criminals-2021-12-08/ (Dec. 8, 2021, 5:13 PM) (describing Conti as a Russian-speaking gang).

252. *See* Kramer et. al, *supra* note 52 (reporting that DarkSide is a Russian-speaking ransomware gang).

253. *See* Carly Page, *Clop Ransomware Gang Doxes Two New Victims Days After Police Raids*, TECHCRUNCH (June 23, 2021, 9:38 AM), https://techcrunch.com/2021/06/23/clop-ransomware-gang-doxes-two-new-victims-days-after-police-raids/ (citing CLOP's Ukrainian-linked ties).

254. *See* Jamie Tarabay, *One Cybercrime Gang Extorted $75 Million From Targets: Study*, BLOOMBERG (Apr. 7, 2021, 3:00 AM), https://www.bloomberg.com/news/articles/2021-04-07/one-cybercrime-gang-extorted-75-million-from-targets-study (noting Egregor's Eastern European origin).

255. *See* Jason Murdock, *Russian Cyber Gang Linked to Hospital Hack That Resulted in Woman's Death*, NEWSWEEK (Sept. 23, 2020, 6:20 AM), https://www.newsweek.com/german-hospital-ransomware-cyberattack-russia-hackers-1533752 (confirming DoppelPaymer's ties to Russia).

256. *See* Claudia Glover, *Meet the Ransomware Gangs Fuelling [sic] a Global Cybercrime Spree*, TECH MONITOR, https://techmonitor.ai/technology/cybersecurity/top-ten-ransomware-gangs-fuelling-the-global-cybercrime-spree (July 27, 2022, 4:19 PM) (reporting the percentage of ransomware threats detected from January to May 2021).

257. *See generally* 18 U.S.C. § 1962.

258. *See* CHARLES DOYLE, CONG. RSCH. SERV., 96-950, RICO: A BRIEF SKETCH 1 (2021).

RICO case law regarding (1) the definition of an enterprise and (2) what it means for an individual to conspire with the enterprise are both instructive to discern whether the ransomware gang or affiliate structure is an organization for the purposes of qualifying as an FTO.[259]

Under the RICO statute, an "'enterprise' includes any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity."[260] An enterprise may be in furtherance of either entirely legal purposes or entirely illegal purposes and can include aspects of governmental and nongovernmental entities.[261] In *Boyle v. United States*, the Supreme Court rejected the notion that enterprises must have certain "business-like" attributes to be considered an "association-in-fact enterprise[,]" and instead, it reiterated its finding in *United States v. Turkette* that an "association-in-fact enterprise is simply a continuing unit that functions with a common purpose."[262] To be an enterprise does not require "discernible hierarch[ies], unique modus operandi, chains of command, internal rules and regulations, regular meetings regarding enterprise activities, or even a separate enterprise name or title."[263] Instead, all that is required are "three structural features: a purpose, relationships among those associated with the enterprise, and longevity sufficient to permit these associates to pursue the enterprise's purpose."[264]

Assuming that courts would borrow this accepted interpretation of an enterprise to define an "organization" in the FTO context,[265] the majority of ransomware gangs would likely qualify.[266] According to experts, RaaS gangs are "tightly organized, highly compartmentalized business[es]," with different individuals responsible for (1) authoring the ransomware malware, (2) breaking into and taking control of computer systems, (3) providing "technical support" to affiliates, (4) laundering the gang's ill-gotten gains, and (5) acting as

259. *Id.*; *see also* Keenan, *supra* note 39, at 810.

260. 18 U.S.C. § 1961(4).

261. *See* DOYLE, *supra* note 258, at 16 (citing United States v. Turkette, 452 U.S. 575, 580–93 (1981); United States v. Palacios, 677 F.3d 234, 248 (4th Cir. 2012); United States v. Cianci, 378 F.3d 71, 83 (1st Cir. 2004); United States v. Warner, 498 F.3d 666, 694 (7th Cir. 2007); DeFalco v. Bernas, 244 F.3d 286, 307–08 (2d Cir. 2001); United States v. Massey, 89 F.3d 1433, 1440 (11th Cir. 1995); Pelfresne v. Village of Rosemont, 22 F. Supp. 2d 756, 761–62 (N.D. Ill. 1998)).

262. *See id.* (citing Boyle v. United States, 556 U.S. 938, 948 (2009)).

263. *See id.* (citing *Boyle*, 556 U.S. at 948).

264. *See id.* (citing *Boyle*, 556 U.S. at 946).

265. *See* Keenan, *supra* note 39, at 810.

266. *See infra* notes 266–69 and accompanying text.

official spokespeople responsible for media relations and outreach.[267] Moreover, structurally, the RaaS groups "mimic[ ] franchises, like McDonald's or Hertz," in that they lower the barrier of entry for less skilled affiliates to conduct their own ransomware attacks.[268] Similar to franchisors, ransomware gangs like DarkSide offer their franchisee-like affiliates services such as "providing technical support for hackers, negotiating with targets, . . . processing payments, and devising tailored pressure campaigns through blackmail and other means, such as secondary hacks to crash websites."[269]

While this stratified structure—with ransomware gangs authoring the malware and separate affiliates choosing targets and conducting the attacks—creates questions as to whether the ransomware gang is responsible for the affiliates' actions (and vice versa), the RICO statute is similarly helpful.[270] Specifically, a Congressional Research Service report notes,

> The heart of the crime lies in the agreement rather than any completed, concerted violation of the other three RICO subsections. . . . [T]here is no requirement that a defendant commit or agree to commit two or more predicate offenses himself. It is enough that the defendant, in agreement with another, intended to further an endeavor which, if completed, would satisfy all of the elements of a RICO violation.[271]

These elements of a RICO conspiracy under 18 U.S.C. § 1962(d) include: "(1) the agreement of (2) two or more (3) to invest in, acquire, or conduct the affairs of (4) a commercial enterprise, (5) in a manner that violates" a RICO offense.[272]

Under RICO principles of joint criminal liability, ransomware gangs and their affiliates could be held criminally responsible for each other's actions.[273] Although on the one hand, the ransomware gangs may be unaware of where an affiliate is planning an attack,[274] there is evidence that many ransomware

267. *See* Kramer et al., *supra* note 52.
268. *See id.*
269. *Id.*
270. *See* 18 U.S.C. § 1962.
271. *See* DOYLE, *supra* note 258, at 8.
272. *See id.*
273. *See* 18 U.S.C. § 1962.
274. *See, e.g.*, Cohen et al., *supra* note 10 (explaining that following the Colonial Pipeline attack, DarkSide distanced itself from the attack and stated that they are an apolitical organization in apparent

gangs continue to provide personalized support to help affiliates successfully carry out attacks.[275] More importantly, in the RaaS model, the affiliate conducts the affairs of the ransomware gang by picking and executing the attacks, while the ransomware gang directly benefits by taking a commission after each attack.[276] For example, DarkSide collects commissions from successful affiliate attacks through "a sliding scale: 25 percent for any ransoms less than $500,000 down to 10 percent for ransoms over $5 million . . . ."[277] Thus, both the ransomware gangs and the affiliates are directly invested, and each group is criminally culpable in the actions taken by the other.[278]

B. Ransomware Attacks Qualify as Terrorism Under 8 U.S.C. § 1182(a)(3)(B)

In the context of ransomware attacks, the law has struggled to keep abreast as technological innovations in the cybercrime industry have advanced at a startling pace.[279] When 8 U.S.C. § 1189 was passed in 1996, Congress likely did not foresee the ubiquity and gravity of foreign cyberthreats from non-state actors.[280] As a result, the statute mainly focuses on physical actions (hijacking, sabotaging, killing, bombing, etc.) perpetrated with physical instruments (guns, chemical weapons, nuclear devices, and explosives) that threaten national security in its definition of "[t]errorist activities."[281] Nevertheless, the statute does not preclude defining physical attacks perpetrated with virtual ransomware weapons as "[t]errorist activities."[282] This Section does not suggest contorting the law in radical ways, but merely argues that

recognition that their affiliate had "gone too far").

275. *See, e.g.*, *id.* According to a New York Times investigation, affiliates conducting DarkSide attacks maintain login credentials and access to a dashboard with "DarkSide's list of targets as well as a running ticker of profits and a connection to the group's customer support staff, with whom affiliates could craft strategies for squeezing their victims." *See* Kramer et al., *supra* note 52.

276. *See id.*

277. *See id.*

278. *See supra* notes 270–76 and accompanying text.

279. *Cf.* Julia Griffith, *A Losing Game: The Law Is Struggling to Keep Up with Technology*, J. OF HIGH TECH. L. BLOG (Apr. 12, 2019), https://sites.suffolk.edu/jhtl/2019/04/12/a-losing-game-the-law-is-struggling-to-keep-up-with-technology/ ("Technology seems to be advancing at a rate that the law simply cannot keep up with.").

280. *See* 8 U.S.C. § 1182 (failing to explicitly include computers among its list of potentially dangerous instruments).

281. *See id.*

282. *See id.*

courts should interpret the statute in light of the reasonable technological realities of the modern age.

Under 8 U.S.C. § 1189(a)(1)(B), to be considered as an FTO, the organization must "engage[] in terrorist activity (as defined in section 1182(a)(3)(B) of this title or terrorism (as defined in section 2656f(d)(2) of title 22), or retains the capability and intent to engage in terrorist activity or terrorism)."[283] Although 22 U.S.C. § 2656f(d)(2) proves to be unhelpful in the ransomware context,[284] ransomware attacks perpetrated by ransomware gangs and their affiliates almost unanimously qualify as "terrorist activities" under 8 U.S.C. § 1182(a)(3)(B).[285]

Terrorist activity—under 8 U.S.C. § 1182(a)(3)(B)(iii)—is centered around the commission or threat of significant violence.[286] Under the statute, "terrorist activity" means activity that is "unlawful under the laws of the place where it is committed (or which, if it had been committed in the United States, would be unlawful under the laws of the United States or any State)," and which involves any of the following: (1) "[t]he highjacking [sic] or sabotage of any conveyance (including an aircraft, vessel, or vehicle)"[287] or (2) what 8 U.S.C. § 1182(a)(3)(B)(iii)(V) reads as

> The use of any [ ] (a) biological agent, chemical agent, or nuclear weapon or device, or (b) explosive, firearm, or other weapon or dangerous device (other than for mere personal monetary gain), with the intent to endanger, directly or indirectly, the safety of one or more individuals or to cause substantial damage to property.[288]

Although courts should consider ransomware malware dangerous devices to the same extent as explosives, firearms, and the other devices listed, ransomware attacks are typically motivated by mere monetary gain.[289] Thus,

283. *See* 8 U.S.C. § 1189.

284. *See* 22 U.S.C. § 2656f(d)(2). Under this definition, terrorism means "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents." *Id.* While some ransomware attacks are politically motivated, many ransomware attacks more readily qualify as terrorism under the broader terrorism definition outlined in 8 U.S.C. 1182(a)(3)(B). *See* 8 U.S.C. § 1182(a)(3)(B).

285. *See* 8 U.S.C. § 1182(a)(3)(B).

286. *See* 8 U.S.C. § 1182(a)(3)(B)(iii).

287. *See* 8 U.S.C. § 1182(a)(3)(B)(iii)(I).

288. *See* 8 U.S.C. § 1182(a)(3)(B)(iii)(V).

289. *See, e.g.*, Cohen et al., *supra* note 10 (reporting that DarkSide released a statement emphasizing "We are apolitical . . . . Our goal is to make money, and not creating problems for society").

although ransomware gangs typically cause substantial property damage and endanger Americans by attacking high risk targets like hospitals, infrastructure, and corporate citizens providing vital services, these attacks are often solely for monetary gain and therefore do not qualify as terrorism under this subsection.[290]

Nevertheless, ransomware attacks fit squarely within the second definition.[291] The actions of ransomware gangs qualify as "[t]errorist activities" because ransomware attacks hijack and sabotage conveyances—namely, computer systems.[292] First, this argument requires proving that computers are in fact conveyances.[293] The statute provides a nonexclusive list of three examples of conveyances, which includes (1) aircrafts, (2) vessels, and (3) vehicles.[294] While the statute focuses on physical conveyances, a conveyance is simply defined as "a means or way of conveying: such as" a "transport[ation]" device.[295] Thus, computer systems are both conveyances themselves and are capable of controlling other conveyances.[296] Computer systems are conveyances themselves because they allow users to transfer a plethora of virtual and physical items like money,[297] stocks,[298] and property interests.[299] Moreover,

290. *See* 8 U.S.C. § 1182(a)(3)(B)(iii)(V)(b).

291. *See* 8 U.S.C. § 1182(a)(3)(B)(iii)(I).

292. *See* 8 U.S.C. § 1182(a)(3)(B)(iii)(I); *see also supra* note 65 and accompanying text (explaining the technology of ransomware attacks).

293. *See* 8 U.S.C. § 1182(a)(3)(B)(iii)(I).

294. *See id.*

295. *See Conveyance*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/conveyance (last visited Oct. 1, 2022).

296. *See infra* notes 299–306.

297. *See* E. Napoletano & Mitch Strohm, *What Is a Wire Transfer?*, FORBES, https://www.forbes.com/advisor/banking/all-about-wire-transfers/ (Mar. 30, 2022, 2:06 PM) (noting that wire transfers, Automated Clearing House transactions, and peer-to-peer payment tools are among the several ways that computers act as conveyances to move money electronically).

298. *See generally* Matt Lee, *Stock Certificates Have Gone with the Winds of Change*, INVESTOPEDIA, https://www.investopedia.com/ask/answers/06/stockcertificate.asp (Dec. 10, 2021). For at least 400 years, transferring stock of a company required physically exchanging a piece of paper—a stock certificate. *Id.* However, "the World Wide Web and electronic trading" has led to the demise of the physical stock certificate. *Id.* Today, physical certificates are a rarity, and "most of the world's exchanges have either done away with or are phasing out paper certificates" as electronic records provide verification for stock ownership. *Id.* Computer systems—typically electronic communication networks—provide the conveyance for transferring ownership. *Id.*

299. *See Retail E-Commerce Revenue in the United States from 2017 to 2022, with Forecasts from 2023 to 2025*, STATISTA (Aug. 26, 2022), https://www.statista.com/statistics/272391/us-retail-e-commerce-sales-forecast/ ("Revenue from retail e-commerce in the United States was estimated at roughly 768 billion U.S. dollars in 2021. The Statista Digital Market Outlook forecasts that by 2025, online shopping revenue in the U.S. will exceed 1.3 trillion dollars.").

computer systems are capable of controlling other conveyances like aircrafts, vessels, and vehicles.[300] For example, trucking fleets, the life-blood of the modern economy, are highly vulnerable to attacks and are frequently the target of "serious hackers . . . from well-funded groups working for long periods of time."[301] Additionally, the recent Colonial Pipeline demonstrated how an attack on a virtual conveyance (Colonial Pipeline's computer system) was capable of shutting down a physical conveyance (the primary oil pipeline for the entire southeastern United States).[302] As physical conveyances like cars, aircraft, and trains become increasingly automated,[303] experts warn that ransomware technology could target entire fleets of cars with shared software modules and effectively lock out every vehicle that uses the same system.[304]

Furthermore, ransomware attacks hijack and sabotage the computer systems they successfully encrypt.[305] Technologically, when ransomware is deployed, it overrides the computer's operating system, hijacks the use of the device from the victim, and prevents the victim from accessing their files.[306] In all ransomware attacks, the affected device is necessarily sabotaged

300. *See* Eric A. Taub, *Carmakers Strive to Stay Ahead of Hackers*, N.Y. TIMES (Mar. 18, 2021), https://www.nytimes.com/2021/03/18/business/hacking-cars-cybersecurity.html. The most headline-making computer-controlled vehicle takeover "occurred in 2015 when security researchers on a laptop 10 miles away caused a Jeep Cherokee to lose power, change its radio station, turn on the windshield wipers and blast cold air," which forced Jeep to recall 1.4 million vehicles to patch the vulnerability. *Id.* Cars, trucks, airplanes, and all modern conveyances have electronic control units, which makes vehicles vulnerable to hackers doing everything from eavesdropping on phone calls to causing a car to speed up, change direction, or lose braking power. *Id.* The number of electronic control units (ECUs) in physical conveyances like a passenger vehicle are staggering. *Id.* While modern passenger planes have just fifteen million lines of code, "modern vehicles employ around 150 electronic control units and about one hundred million lines of code." *Id.*

301. *See id.* (noting that entire trucking fleets can "be shut down or otherwise compromised for a ransom").

302. *See supra* notes 3–21 and accompanying text.

303. *See* Taub, *supra* note 299. The amount of electronic control units and lines of code is projected triple in vehicles with "the advent of autonomous driving features and so-called vehicle-to-vehicle communication." *Id.* As a result, vehicle manufacturers face a difficult task in defending against cyberthreats. *Id.*

304. *See* André Weimerskirch & Derrick Dominic, *Assessing Risk: Identifying and Analyzing Cybersecurity Threats to Automated Vehicles*, MCITY: UNIVERSITY OF MICHIGAN 7 (Jan. 2018), https://mcity.umich.edu/wp-content/uploads/2017/12/Mcity-white-paper_cybersecurity.pdf ("[O]ne successful hack could spread across every vehicle that uses the same system, as with the global hacks of the kind seen with Windows computers, such as the WannaCry ransomware attack that shut down more than 300,000 computers in 150 countries during May, at an estimated cost of as much as $4 billion.").

305. *See supra* notes 65–67 and accompanying text.

306. *See supra* notes 65–67 and accompanying text.

because hackers deliberately damage the device so that it does not work correctly.[307] Then in many attacks, even after victims pay the demanded ransom, the victims never receive the encryption key, leaving the victim's device permanently disabled.[308] Similarly, in circumstances where victims do get the encryption key, the affected computer system typically remains out of commission for significant periods of time as IT experts must rebuild the computer's network.[309] As a result, ransomware attacks qualify as "terrorist activit[ies]" under the statute.[310]

C. Ransomware Gangs Threaten the National Security of the United States.

Under the third requirement of 8 U.S.C. § 1189, "the terrorist activity or terrorism of the organization" must "threaten[] the security of United States nationals or the national security of the United States."[311] The State Department defines national security to include the nation's "national defense, foreign relations, or [] economic interests."[312] To assess the degree in which ransomware gangs threaten these interests, this section will compare the threat posed by ransomware gangs to several designated FTOs. Ultimately, this section will conclude that the most prolific ransomware gangs undoubtedly threaten the national security of the United States by diminishing its national defenses, vital infrastructure, and economic interests.

Although every listed FTO fits the statutory definition of 8 U.S.C. § 1189, certain FTOs present less of an immediate threat to the United States than foreign ransomware gangs.[313] Apart from al Qaeda,[314] Islamic State of Iraq

307. *See supra* notes 65–67 and accompanying text.

308. *See supra* note 142 and accompanying text.

309. *See, e.g.*, Eaton & Volz, *supra* note 5 (reporting that despite Colonial Pipelines paying the ransom, their computer systems and operations remained offline for nearly a week).

310. *See* 8 U.S.C. § 1182(a)(3)(B)(iii)(I).

311. *See* 8 U.S.C. § 1189(a)(1)(C).

312. *See Foreign Terrorist Organizations*, *supra* note 171.

313. *See infra* notes 318–39 and accompanying text.

314. Christopher Wray, *Threats to the Homeland Evaluating the Landscape 20 Years After 9/*11, FBI (Sept. 21, 2021), https://www.fbi.gov/news/testimony/threats-to-the-homeland-evaluating-the-landscape-20-years-after-911-wray-092121. In a recent threat assessment delivered to Congress, FBI Director Christopher Wray stated,

> Al Qaeda maintains its desire to both conduct and inspire large-scale, spectacular attacks. Because continued pressure has degraded some of the group's senior leadership, in the near term, we assess that al Qaeda is more likely to continue to focus on cultivating its international affiliates and supporting small-scale, readily achievable attacks, including attacks against the interests of the United States and other Western nations, in regions such as East

and Syria (ISIS),[315] and Iran's Islamic Revolutionary Guard Corps-Qods Force and its primary strategic partners,[316] some FTOs have disbanded and not carried out a successful attack against the United States in decades.[317] Meanwhile, ransomware attacks present a continuous and active threat to American national security by undermining the country's (1) national defenses, (2) vital infrastructure, and (3) economic interests.[318]

Ransomware gangs threaten America's national defense in several ways. First, ransomware gangs attempt and launch successful attacks against local, state, and federal governments in staggering numbers.[319] According to

---

> and West Africa. Over the past year, propaganda from al Qaeda leaders continued to seek to inspire individuals to conduct attacks in the United States and other Western nations. We expect those attempts to continue.

Id.

315. *See id.* ("ISIS remains relentless in its campaign of violence against the United States and our partners—both here at home and overseas. To this day, ISIS continues to aggressively promote its hate-fueled rhetoric and attract like-minded violent extremists with a willingness to conduct attacks against the United States and our interests abroad. ISIS's successful use of social media and messaging applications to attract individuals seeking a sense of belonging is of continued concern to us. Like other foreign terrorist groups, ISIS advocates for lone offender attacks in the United States and Western countries via videos and other English language propaganda that have at times specifically advocated for attacks against civilians, the military, law enforcement, and other government personnel.").

316. *See id.* ("Iran and its global proxies and partners, including Iraqi Shia militant groups, continue to attack and plot against the United States and our allies throughout the Middle East in response to U.S. pressure. Iran's Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) continues to provide support to militant resistance groups and terrorist organizations. Lebanese Hizballah, Iran's primary strategic partner, has sent operatives to build terrorist infrastructures worldwide. Hizballah also continues to conduct intelligence collection, financial activities, and procurement efforts worldwide to support its terrorist capabilities. FBI arrests in recent years of alleged Iranian and Hizballah operatives in the United States suggest the Government of Iran and Hizballah each seek to establish infrastructure here, potentially for the purpose of conducting operational or contingency planning. IRGC-QF Commander Esmail Ghani and Hizballah Secretary General Hasan Nasrallah have each threatened retaliation for the death of IRGC-QF Commander Qassem Soleimani.").

317. *See, e.g.*, Mapping Militant Organizations, *Liberation Tigers of Tamil Elam*, STANFORD UNIV., https://cisac.fsi.stanford.edu/mappingmilitants/profiles/liberation-tigers-tamil-elam (last modified June 2018). The Liberation Tigers of Tamil Eelam (LTTE) were a separatist militant organization that fought for "an independent homeland for Hindu Tamils in Northeaster Sri Lanka." *Id.* While active, the group carried a number of high-profile assassinations of the Sri Lankan president and a former Indian Prime Minister and had a highly developed military wing. *Id.* However, the group disbanded in 2009 after being defeated. *Id.* While thirteen LTTE members were arrested in a plot to attack American and Israeli embassies in India in 2014, the group's strength is certainly diminished. *See Country Reports on Terrorism 2017—Foreign Terrorist Organizations: Liberation Tigers of Tamil Eelam*, REFWORLD (Sept. 19, 2018), https://www.refworld.org/docid/5bcf1f33a.html.

318. *See infra* notes 323–34 and accompanying text.

319. *See, e.g.*, Frank Cilluffo, *Should Cities Ever Pay Ransom to Hackers?*, WALL ST. J. (Sept. 17, 2019, 10:02 PM), https://www.wsj.com/articles/should-cities-ever-pay-ransom-to-hackers-1156877

cybersecurity firm BlackFog, the government experienced the highest volume of attacks by industry in 2021.[320] Moreover, ransomware gangs' frequent attacks on various American government and defense contractors further highlights their danger to America's national defense.[321]

Additionally, ransomware affiliates frequently target and compromise America's vital infrastructure.[322] In 2021, attacks on the United States energy industry and food supply chain garnered the most national attention.[323] However, America's vital infrastructure is broadly vulnerable.[324] For example, the government has reported recent ransomware attacks on local water supplies, which is an especially alarming trend given the ease at which an attack on a water facility could precipitate the mass poisoning of Americans in an entire region.[325] Similarly, America's healthcare system—and more specifically hospitals—has faced a relentless onslaught of ransomware attacks, which can have life or death implications for patients seeking critical care.[326]

Meanwhile, ransomware's cost to America's economic interests is staggering. The global losses from cyberattacks are estimated at nearly $1 trillion

2120 ("estimating '71 ransomware attacks against state and local governments' in 2019 and '54 in 2018'").

320. *The State of Ransomware in 2021*, BLACKFOG (Jan. 4, 2022), https://www.blackfog.com/the-state-of-ransomware-in-2021/ [hereinafter BlackFog].

321. Joseph Marks, *The Cybersecurity 202: Defense Contractors Are Yet Another Sector Highly Vulnerable to Hacking, Study Finds*, WASH. POST (June 22, 2021, 7:09 AM), https://www.washingtonpost.com/politics/2021/06/22/cybersecurity-202-defense-contractors-are-yet-another-sector-highly-vulnerable-hacking-study-finds/.

322. *Cf.* Uberti, *supra* note 19 (reporting that vital infrastructure was one of the areas President Joe Biden stated should be off-limits for foreign ransomware hackers during a 2021 phone call with Russian President Vladimir Putin).

323. *See* Julian Dossett, *A Timeline of the Biggest Ransomware Attacks*, CNET (Nov. 15, 2021, 12:45 PM), https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/.

324. *See* Tom Kelly, *Ransomware is a Growing Threat: US Companies and Infrastructure Providers Need to Be Ready*, THE HILL (Aug. 4, 2021, 6:30 PM), https://thehill.com/opinion/cybersecurity/566409-ransomware-is-a-growing-threat-us-companies-and-infrastructure (warning of the vulnerability in the United States' water supply, electrical grid, health system, and flood dams).

325. Kevin Collier, *50,000 Security Disasters Waiting to Happen: The Problem of America's Water Supplies*, NBC NEWS, https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206 (June 17, 2021, 9:20 AM).

326. *See* Weiner, *supra* note 147; *see also* Melissa Eddy & Nicole Perlroth, *Cyberattack Suspected in German Woman's Death*, N.Y. TIMES (Sept. 18, 2020), https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html (reporting that a hospital patient in Berlin died after the hospital was unable to provide care for emergency patients after cybercriminals targeted the hospital with a ransomware attack).

in 2020.[327] The United States is consistently the target of over half of the global ransomware attacks.[328] In 2021, large American companies lost an average of $5.66 million to ransomware attacks.[329] Only twenty percent of this $5.66 million total actually accounted for ransom payments.[330] Meanwhile, eighty percent of the cost of ransomware attacks comes from "lost productivity and the time-consuming task of containing and cleaning up after a ransomware attack."[331] Additionally, following attacks, companies experience increased cyber-insurance premiums and IT expenditures.[332] Moreover, additional public relations and legal services are frequently required.[333] Similarly, public companies often experience share price volatility in the wake of ransomware attacks, as consumers have historically avoided businesses that prove to be incapable of protecting their customers' data.[334]

327. *See* LEWIS, *supra* note 31, at 6.

328. *See* BlackFog, *supra* note 325.

329. *See* Carly Page, *Ransomware Recovery Can be Costly, and Not Just Because of the Ransom*, TECHCRUNCH (Aug. 18, 2021, 8:30 AM), https://techcrunch.com/2021/08/18/ransomware-recovery-can-be-costly-and-not-just-because-of-the-ransom/.

330. *See id.*

331. *See id.* ("[T]he remediation process for an average-sized organization takes on average 32,258 hours, which when multiplied by the average $63.50 IT hourly wage totals more than $2 million. Downtime and lost productivity is another costly consequence of ransomware attacks; the research shows that phishing attacks, for example, which were determined as the root cause of almost one-fifth of ransomware attacks last year, have led to employee productivity losses of $3.2 million in 2021, up from $1.8 million in 2015.").

332. *Id.*

333. *Id.*

334. *See id.*; *see, e.g.*, Keman Huang & Stuart Madnick, *A Cyberattack Doesn't Have to Sink Your Stock Price*, HARV. BUS. REV. (Aug. 14, 2020), https://hbr.org/2020/08/a-cyberattack-doesnt-have-to-sink-your-stock-price ("A hack can sink a company's stock price and leave investors fuming. In the wake of the Capital One hack, which was publicly reported in July 2019, the company's stock price dropped nearly 6% immediately in after-hours trading, losing a total of 13.89% over two weeks. Likewise, following the announcement of the Equifax breach back in early September of 2017, the company saw a similar negative reaction from the stock market with its stock price plunging from $142.72 to $92.98 in just one week. What is worse, its market share dropped significantly in 2017 and has struggled to recover ever since.").

D. A New Weapon in the DOJ's Expanding Arsenal: The Benefits of Ransomware Gangs' Addition to the FTO list

Although the United States has scored several high-profile victories against ransomware gangs since the DOJ formed the Ransomware and Digital Extortion Task Force in April of 2021,[335] designating the most prolific ransomware gangs to the FTO list would facilitate this fight by adding a new weapon to the Justice Department's prosecutorial arsenal.[336] Including select ransomware gangs on the FTO list will have several financial, legal, and political benefits.[337]

Financially, designating ransomware gangs as FTOs would add pressure on the handful of cryptocurrency exchanges that facilitate cybercriminals' conversion of cryptocurrency ransom into a usable fiat currency.[338] Five cryptocurrency exchanges received eighty-two percent of the illicit funds extorted from ransomware victims.[339] Just as the FTO statute forced banks to implement "Know Your Customer" regulations and customer due diligence policies to avoid becoming criminally liable for materially supporting FTOs,[340] adding ransomware gangs to the FTO list would impose the same cost on cryptocurrency exchanges.[341] Recently, pursuant to Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activity," the Treasury Department's Office of Foreign Asset Control (OFAC) announced sanctions against two cryptocurrency exchanges, Chatex and Suex.[342] The executive order enables the Treasury Department to provide similar sanctions that would result from adding ransomware gangs to the FTO

335. *See* Page, *supra* note 20.

336. *See infra* notes 345–60 and accompanying text.

337. *See infra* notes 345–60 and accompanying text.

338. *See infra* notes 345–51 and accompanying text.

339. *See* Dwyer, *supra* note 18.

340. *See* 18 U.S.C. §§ 2339A–2339B; *see also* PETER BERRIS & JOHNATHAN GAFFNEY, CONG. RSCH. SERV., R46932, RANSOMWARE AND FEDERAL LAW: CYBERCRIME AND CYBERSECURITY 7 (2021).

341. *See* 18 U.S.C. §§ 2339A–2339B.

342. *See* Exec. Order No. 13694, *supra* note 220; *see also* Press Release, U.S. Dep't of Treasury, Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange, (Nov. 8, 2021) https://home.treasury.gov/news/press-releases/jy0471 (explaining the United States designated Chatex after it provided material support to Suex, which the United States sanctioned on September 21, 2021, pursuant to Executive Order 13694); *OFAC Releases Updated Ransomware Advisory and Announces First Designation of Cryptocurrency Exchange*, JD SUPRA (Sept. 29, 2021), https://www.jdsupra.com/legalnews/ofac-releases-updated-ransomware-4695494/ [hereinafter JD SUPRA].

list.[343] Even though the FTO statute and executive order would function in similar ways, adding ransomware gangs to the FTO list would add more political legitimacy to the financial sanctions.[344] This is because, unlike the FTO designation process, the executive order used to sanction the Chatex and Suex exchanges does not provide opportunities for judicial or congressional oversight.[345]

Legally, adding ransomware gangs to the FTO list would facilitate the DOJ's prosecution and investigations of the groups.[346] During the war on terror, prosecutors used the FTO statute to flip low level FTO affiliates by threatening to charge them with the material support of terrorism.[347] Although pursuing this approach will require the DOJ to add "cyber prosecutors and agents," and give the department additional resources to conduct long-term investigations, adding ransomware gangs to the FTO list would facilitate the prosecution in similar ways.[348] Among the parties that would become increasingly amenable to prosecution by designating ransomware gangs as FTOs include: (1) individuals employed within ransomware gangs in various roles, (2) the cryptocurrency exchanges facilitating ransomware gangs' conversion of currency into usable fiat, (3) the ransomware gang affiliates conducting the attacks, and (4) the various parties involved with laundering the ransomware gangs' criminal bounties.[349]

Of course, the problem remains that many ransomware gangs operate from Russia, who many commentators have accused of tacitly supporting and harboring the cybercriminal gangs.[350] Nevertheless, there are several reasons

343. *See* JD SUPRA, *supra* note 341 and accompanying text.

344. *See supra* notes 219–21 and accompanying text.

345. *See supra* notes 219–21 and accompanying text. Moreover, it is permissible for executive orders and the FTO statute to overlap in several key areas. *See* CRONIN, *supra* note 169, at 5. The FTO list and several other key terrorism lists created via executive orders such as the "Specially Designated Terrorist list," the "Specially Designated Global Terrorist" list, and the "Terrorist Exclusion List" share similar functions. *Id.* "These lists do overlap; however, the Executive Branch implements sanctions against state sponsors of terrorism, terrorist organizations, and individual terrorists somewhat differently depending upon which legislation applies, what the purpose is, and which list is being considered." *Id.*

346. *See* Dwyer, *supra* note 18.

347. *See* Chesney, *supra* note 234, at 163–64.

348. *See* Dwyer, *supra* note 18.

349. *See supra* Section II.B.

350. *See* Dwyer, *supra* note 18. In addition to harboring these ransomware gangs, Russia has directly launched their own devastating cyberattacks against the United States. *Id.*

why the FTO statute would benefit the DOJ.[351] First, members of ransomware gangs and their affiliates travel "to U.S.-allied countries despite the known risk of arrest."[352] As a result, America's foreign law enforcement partners have successfully arrested and extradited several prominent ransomware gang members and affiliates in 2021.[353] Second, fully dismantling the ransomware gang network will require a maximum pressure campaign against the countries that harbor these criminals.[354] Since the designation of FTOs has inherently political implications, categorizing ransomware gangs as such will increase the pressure on Russia and many of the former Soviet-bloc countries that allow cybercriminals to commit acts of terror against the United States without repercussions.[355] Third, even where prosecutors are unable to arrest and extradite ransomware gang members and their affiliates, the FTO statute will facilitate the types of proactive investigations that would enable authorities to find and dismantle the cyberinfrastructure of ransomware gangs.[356]

V. CONCLUSION – PATCHING THE NETWORK: FORTIFYING AMERICAN CYBER-DEFENSES BY PROACTIVELY PROSECUTING RANSOMWARE GANGS

In the wake of several headline-making ransomware attacks, in June of 2021, FBI Director Christopher Wray commented on the "current spate of cyberattacks," which he believes poses similar challenges to those that arose

351. *See infra* notes 351–54.

352. *See* Dwyer, *supra* note 18 ("For instance, Aleksei Burkov, the leader of a prominent Russian cybercrime forum, was arrested while vacationing in Israel in December 2015 and subsequently extradited to the U.S. Mr. Burkov's co- conspirator, Ruslan Yeliseyev, planned his own trip to Israel the following year and was likewise arrested and extradited.").

353. *See* Carly Page, *US Charges Kaseya Hacker and Seizes $6M from REvil Ransomware Gang*, TECHCRUNCH (Nov. 8, 2021, 10:55 AM), https://techcrunch.com/2021/11/08/us-charges-kaseya-hacker-and-seizes-6m-from-revil-ransomware-gang/. In 2021, the DOJ had several major wins in terms of successfully arresting ransomware gang members. *Id.* According to Europol, seven affiliates of the notorious REvil ransomware gang who were responsible for launching 2,500 attacks and extorted millions in ransom were arrested in various countries such as Kuwait, South Korea, Romania, and Poland. *Id.*

354. *See* Dwyer, *supra* note 18 (noting that, because Russia denies supporting cybercriminals, exposing such criminals may aid diplomatic efforts).

355. *See supra* note 193 and accompanying text.

356. *See* Dwyer, *supra* note 18 ("When the department can't arrest suspected cybercriminals, it can often dismantle infrastructure it knows has been used in attacks, as it did to the botnet known as Emotet. Law enforcement was able to gain access to Emotet's command-and-control servers and sever its control over 1.6 million compromised computers, which had been used by ransomware gangs and other cybercriminals.").

when investigating the perpetrators of the September 11 Attacks.[357] Wray observed, "There are a lot of parallels, there's a lot of importance, and a lot of focus by us on disruption and prevention."[358] Disrupting and preventing ransomware attacks before they take place is vital to minimizing the damage they inflict on the United States.[359] This comment sought to provide a proven, legal, and relevant tool for the Department of Justice to use in its task of curbing the scale of the damage that ransomware is currently causing.[360] Ultimately, designating ransomware gangs as FTOs is legal and will facilitate the Justice Department—in concert with its investigative partners—in launching the types of long-term investigations that will be necessary to combat this malign threat to the United States' national security.[361]

Ransomware gangs fit within the statutory definition for FTOs.[362] Drawing upon other pertinent areas of criminal law where principles of joint criminal enterprise liability are settled, the established precedent demonstrates that despite ransomware gangs' unique operating structures, the groups qualify as foreign organizations.[363] Moreover, the criminal activities of the most high-profile ransomware gangs fall squarely within the statute's definition of terrorist activities, which defines it to mean the hijacking or sabotaging of a conveyance.[364] Ransomware attacks functionally operate by hijacking and sabotaging computer systems in exchange for ransom.[365] Computer systems—which control the American economy's flow of goods and resources—are conveyances because they are the essential component responsible for controlling physical means of transportations, like fleets of cars, trucks, trains, and airplanes.[366] Finally, by frequently and indiscriminately targeting America's critical infrastructure, ransomware attacks present a grave risk to the country's national security and economic interests.[367] Designating

357. *See* Aruna Viswanatha & Dustin Volz, *FBI Director Compares Ransomware Challenge to 9/11*, WALL ST. J. (Jun. 4, 2021, 12:56 PM), https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003.
358. *Id.*
359. *See id.*; Dwyer, *supra* note 18.
360. *See supra* Section IV.D.
361. *See supra* Section IV.D.
362. *See supra* Sections IV.A–C.
363. *See supra* Section IV.A.
364. 8 U.S.C. § 1182(a)(3)(B)(iii)(I); *see supra* Section IV.B.
365. *See supra* Section IV.B.
366. *See supra* notes 292–312 and accompanying text.
367. *See supra* Section IV.C.

ransomware gangs as FTOs will enable the Justice Department to flip critical informants who make up the fabric of the ransomware-as-a-service business, and bring the major gangs who author the malware to justice.[368]

Although the FTO statute can provide a key resource for law enforcement and prosecutors, there are several key factors that can impede the success of these long-term, proactive investigations.[369] First, vital funding is needed to staff the teams of specialized prosecutors and agents necessary to maintain such investigations.[370] Additionally, while designating ransomware gangs as FTOs will have some benefits even without the full cooperation of Russia, the level of success of the strategy put forward in this comment will depend on an improved relationship between the countries.[371]

Ultimately, while the challenges posed by ransomware are significant, they are neither unprecedented nor insurmountable.[372] No strategy will ever be able to stop all cybercrime, but the United States can apply certain tactics to mitigate ransomware's widespread economic disruption and threat to America's national security.[373] The ransomware gangs attempts at draining the United States of its financial resources via the targeting of America's critical infrastructure are acts of terror and gravely threaten American citizens' safety and security.[374] Proactively prosecuting ransomware gangs, with the

368. *See supra* Section IV.D.

369. *See infra* notes 369–70 and accompanying text.

370. *See* Kellen Dwyer, *It's Time to Surge Resources into Prosecuting Ransomware Gangs*, LAWFARE (May 20, 2021, 8:01 AM), https://www.lawfareblog.com/its-time-surge-resources-prosecuting-ransomware-gangs ("To fight ransomware, the Justice Department should follow the playbook that it used against organized crime in the 1960s and terrorists after 9/11. The department needs a 'troop surge' of cyber prosecutors and agents to conduct long-term, proactive investigations into ransomware gangs and the organizations that enable them. . . . [T]he department could create a strike force that does nothing but long-term, proactive investigations into cybercrime-as-a-service organizations (with a particular focus on those that support ransomware). The department already employs this concept in its Organized Crime and Drug Enforcement Task Force (OCDETF) strike forces, which are permanent, prosecutor-led teams that conduct intelligence-driven, multi-jurisdiction investigations into priority targets and their affiliate financial networks. A cyber strike force modeled on this concept could be extremely effective with a yearly budget of $5 million, which would easily pay the salaries of 10 dedicated prosecutors and 20 agents. This would represent a tiny fraction of the money the government spends on cybersecurity. For perspective, the American Rescue Plan Act of 2021 allocated an additional $650 million to the Cybersecurity and Infrastructure Security Agency (CISA) in order to beef up the nation's cyber defense. The administration has asked for a total of $2.1 billion for CISA in its 2022 discretionary budget request.").

371. *See id.*

372. *See supra* Part III.

373. *See supra* Part IV.

374. *See supra* Section IV.B.

assistance provided from designating the ransomware gangs as FTOs, is a meaningful step towards aggressively addressing the crisis.[375]

Jake C. Porath*

375. *See supra* Section IV.D.

* J.D. Candidate, Pepperdine University Caruso School of Law; B.A. in Political Science and History, Williams College. I would like to thank my parents, Mark and Lynn Porath, my sister, Alex Menna, and my girlfriend, Emily Olsen, for their love and support throughout the process of writing this article. I greatly appreciate the general support of the Pepperdine University Caruso School of Law faculty, who have been critical to my academic development. Finally, I would like to thank the members and editors of Volume XLIX and Volume L of the *Pepperdine Law Review* for their hard work and invaluable feedback throughout the editing process.

The *Pepperdine Law Review* awarded Jake C. Porath the 2022 Ronald M. Sorenson Memorial Writing Award, presented to the member of the Law Review who submits the most well-written, thoroughly researched, and intellectually engaging comment or note.

***