RANSOMWARE CYBERATTACKS, TERRORISM, AND THE AMERICAN PEOPLE: A CALL FOR A UNIFIED RESPONSE TO RANSOMWARE

*Kimberly R. Seiler**

* J.D. 2023, University of Houston Law Center. This Comment received the Mark Vela Endowed Scholarship for Best Paper in Criminal Law. I am grateful to Professor Emily Berman for the conversations that sparked this Comment to life and for sharing her expertise in national security laws. I would also like to thank the Honorable Alamdar

INTRODUCTION

"We're barely able to keep up" reported the Chief Technology Officer of Mandiant, a large cybersecurity firm.[1] The frequency of cyberattacks in America is overwhelming the cybersecurity industry and government agencies like the Department of Homeland Security (DHS).[2] Such cyberattacks can and often do have costly consequences for Americans; most notably, the Colonial Pipeline attack that occurred in May of 2021.[3]

Colonial Pipeline (Colonial), the United States of America's (U.S.) largest refined oil products pipeline, transports nearly 45% of fuel used throughout the East Coast.[4] Early on the morning of May 7, 2021, Colonial personnel discovered a ransomware attack in progress that was being carried out by a cyber gang.[5] Known as DarkSide, the Russian gang successfully targeted the major pipeline to hold critical data captive until the company agreed to

---

S. Hamdani, Professor David Y. Kwok, and Professor Meredith J. Duncan for helpful comments and feedback. This Comment is dedicated to my Parents, who gave me my love of learning and of the law. None of this would be possible without them.

1. Kevin Collier, *'Barely Able to Keep up': America's Cyberwarriors Are Spread Thin by Attacks*, NBC NEWS (July 8, 2021, 3:03 PM), https://www.nbcnews.com/tech/security/ransomware-attacks-leave-cybersecurity-experts-barely-able-keep-rcna1337.

2. *Id.* (explaining how the Department of Homeland Security is urgently trying to fill 2,000 cybersecurity personnel positions); Emsisoft Malware Lab, *The State of Ransomware in the US: Report and Statistics 2020*, EMSISOFT (Jan. 18, 2021), https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/ (noting the U.S. experienced 113 ransomware attacks on federal, state, and municipal agencies, 560 attacks on healthcare centers, and 1,681 attacks on schools, colleges, and universities in 2020).

3. *See* Sean M. Kerner, *Colonial Pipeline Hack Explained: Everything You Need to Know*, TECH TARGET (Apr. 26, 2022), https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

4. Maggie Miller, *Biden Leading 'Whole of Government' Response to Colonial Pipeline Attack*, THE HILL (May 10, 2021, 3:03 PM), https://thehill.com/policy/cybersecurity/552694-biden-leading-whole-of-government-response-to-colonial-pipeline-attack; *Held to Ransom*, THE LEGAL 500, https://www.legal500.com/gc-magazine/feature/held-to-ransom/ (last visited Feb. 23, 2022).

5. Alan Kovski, *Senators Query Colonial Pipeline CEO about Cyberattack Shutdown*, OIL & GAS J. (June 9, 2021), https://www.ogj.com/general-interest/government/article/14204915/senators-query-colonial-pipeline-ceo-about-cyberattack-shutdown.

pay a ransom of $4.4 million.[6] This event became known as one of the largest cyberattacks on a utility in the U.S. to date.[7]

To remedy the situation, Colonial took their computer systems offline;[8] a practice recommended when dealing with different types of intrusions.[9] As a result of the attack, gasoline shortages became rampant across the East Coast.[10] Colonial executives worked with Mandiant, a cybersecurity firm, to revert some segments of the pipeline to manual operations while the computer systems were down.[11] The Federal Bureau of Investigations (FBI) and other agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA) within the DHS, worked with Colonial to respond to the attack.[12]

On the same day of the attack, the Colonial executives decided that the best response was to pay the $4.4 million to the cyber gang in the hope of restarting the system rather than running it manually.[13] The CEO recognized his decision was very controversial.[14] After receiving the ransom payment in the form of Bitcoin cryptocurrency, DarkSide gave Colonial an encryption

---

6. *Id.*; *see also* Russon, *infra* note 52.

7. *See* Miller, *supra* note 4 (reporting the FBI announced the Colonial cyberattack is likely the largest successful attack on a utility in the U.S.); *See also* BOBBY CHESNEY, CHESNEY ON CYBERSECURITY LAW, POLICY, AND INSTITUTIONS, 272 (3.1 ed. 2021) (ebook) (emphasizing the Colonial cyberattack among the increased amount of high-impact ransomware attacks in 2021) [hereinafter CHESNEY].

8. *See* Kristin L. Bryan & Dan Lonergan, *Second Colonial Pipeline Data Incident Litigation Filed on Behalf of. . . over Ten Thousand Gas Stations?* THE NAT'L L. REV. (July 14, 2021), https://www.natlawreview.com/article/second-colonial-pipeline-data-incident-litigation-filed-behalf-over-ten-thousand-gas (noting Colonial was taken offline as a remedial measure).

9. *See* Gregory Falco et al., *Cyber Negotiation: A Cyber Risk Management Approach to Defend Urban Critical Infrastructure from Cyberattacks*, 4 J. CYBER POL'Y 90, 92 (2019) (explaining how systems affected by ransomware may need to be taken offline).

10. Bryan & Lonergan, *supra* note 8.

11. Kovski, *supra* note 5.

12. *Id.*

13. *Id.*

14. Dominick Reuter, *US Authorities Have Recovered a 'Majority' of the Ransom Colonial Pipeline Paid to Reopen its Critical Fuel Route*, INSIDER (June 7, 2021, 2:23 PM), https://www.businessinsider.com/colonial-pipeline-attack-hack-ransom-recovery-us-doj-2021-6?op=1 ("'I know that's a highly controversial decision,' he said. 'I didn't make it lightly. I will admit that I wasn't comfortable seeing money go out the door to people like this.'").

key to regain access to the systems.[15] However, the process of restarting the systems was not easy.[16] With a grim prediction that full restoration could take months, Colonial focused on restarting critical systems for the first week.[17]

The cyber gang likely gained access to Colonial's computer systems through an outdated virtual private network that was no longer intended for use.[18] Although the password was considered complex, the company failed to use standard security features such as multifactor authentication.[19] The consequences of Colonial's lackadaisical approach to cybersecurity were devastating to the general public.[20]

Currently, the federal government allows organizations to pay ransoms to cyber gangs.[21] While some government agencies have issued statements discouraging organizations from paying ransomware, the Internal Revenue Service (IRS) encourages the practice by allowing such payments to be written off as business expenses.[22] The lack of a unified stance against ransomware payments has encouraged organizations to take a wait-and-see approach to cybersecurity and to pay off ransomware demands instead of investing in adequate security measures.[23] As a result, America is experiencing an intensive surge in ransomware

15. Kovski, *supra* note 5.

16. *Id.*

17. *Id.*

18. *Id.*

19. *See id.*

20. *See* Trushinski, *infra* note 53 (reporting gas prices rose to their highest since 2018 and eighteen states declared a state of emergency because of the Colonial attack).

21. *See* Marañon & Wittes, *infra* note 51 (arguing ransomware payments should generally be deemed illegal); *see also* Alan Suderman & Marcy Gordon, *FBI Says Don't Pay Ransom While Tax Advisors Say Payment May Be Tax Deductible*, INS. J. (June 21, 2021),https://www.insurancejournal.com/news /national/2021/06/21/619439.htm (noting some tax experts advise that certain ransomware payments can legally be deducted as necessary and ordinary business expenses).

22. Suderman & Gordon, *supra* note 21 ("'The cheaper we make it to pay that ransom, then the more incentives we're creating for companies to pay, and the more incentives we're creating for companies to pay, the more incentive we're creating for criminals to continue,' said Josephine Wolff, a cybersecurity policy professor at the Fletcher School of Tufts University.").

23. *See id.*

attacks.[24] The conflict between Russia and Ukraine has aggravated cyber tensions, leading to concern over more cyberattacks on the U.S.[25] American citizens are increasingly restless about the status quo and frustrated with the effects of ransomware payments.[26] This Comment will advocate on behalf of the American people to bring change to the current ecosystem that allows ransomware cyber gangs to thrive. Specifically, the federal government should disrupt the ransomware ecosystem by recognizing ransomware attacks as terrorism.

Section II of this Comment will discuss what ransomware is and the effects that it has had on the American public as a whole and minority communities in particular. Section III will examine how ransomware attacks fit the definition of terrorism and will explore the benefits of this interpretation. This Comment will then respond to a major concern raised about criminalizing ransomware payments: will criminalizing payments encourage cyber gangs to target critical organizations that provide life-sustaining services? Finally, this Comment will conclude by explaining why "hackbacks" are a viable solution to deter cyber gangs from targeting such critical organizations.

---

24. Suderman & Gordon, *supra* note 21

25. Brad Dress, *US Cyber Defense Warns of Possible Cyberattacks Amid Tensions*, THE HILL (Feb. 12, 2022, 7:55 PM), https://thehill.com/policy/cybersecurity/594013-us-cyber-defense-agency-warns-of-possible-russian-cyberattacks-amid ("[CISA] has issued a 'Shields Up' alert for American organizations saying that U.S. systems could face Russian cyberattacks amid warnings from Biden administration officials that a Russian invasion of Ukraine could be imminent . . .").

26. *See* Jenni Bergal, *States Weigh Bans on Ransomware Payoffs*, THE PEW CHARITABLE TRUSTS (July 23, 2021), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/07/23/states-weigh-bans-on-ransomware-payoffs (discussing how several state legislatures are considering legislation that would forbid state and local government agencies from paying ransomware).

II. BACKGROUND

A. *The Ransomware Ecosystem: A Vicious Cycle*

Ransomware is malicious software that encrypts the victim's files to render them unusable.[27] In other words, the victim can be left unable to access its own files or computer systems.[28] Ransomware causes major disruptions to operations because organizations suffering from an attack are no longer able to access data that is necessary to function.[29] As the Colonial attack demonstrated, disruptions to critical infrastructure and business operations are costly.[30] The malicious actors traditionally leverage operation disruptions to extort the payment of a ransom in exchange for unlocking the files or system.[31] However, cyber gangs have employed additional coercive tactics, such as threatening to release sensitive information to embarrass the victims or to permanently delete crucial data.[32]

Ransomware cyber gangs are frequently found in countries that provide them a safe harbor.[33] Many countries that are hostile to the U.S. benefit from cyber gangs because the gangs harm the U.S.'s critical infrastructure.[34] Countries such as China, Russia,

---

27. CYBERSECURITY & INFRASTRUCTURE & SEC. AGENCY & MULTI-STATE INFO. SHARING & ANALYSIS CTR., RANSOMWARE GUIDE 2 (2020) [hereinafter MULTI-STATE INFO. SHARING & ANALYSIS CTR.].

28. *Ransomware*, FBI, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware (last visited Feb. 23, 2022) [hereinafter *Ransomware*, FBI].

29. *Id.*; MULTI-STATE INFO. SHARING & ANALYSIS CTR., *supra* note 27.

30. *See* discussion *infra* Section II.B; Collier, *supra* note 1 ("Ransomware cost American victims an estimated $1.4 billion last year.").

31. *See Ransomware*, FBI, *supra* note 28; MULTI-STATE INFO. SHARING & ANALYSIS CTR., *supra* note 27, at 2.

32. MULTI-STATE INFO. SHARING & ANALYSIS CTR., *supra* note 27, at 2; Deborah R. Farringer, *Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals*, 40 SEATTLE UNIV. L. REV. 937, 938 (2017) (noting in 2016 a cyber gang took control of a nonprofit hospital network's computer system and threatened to permanently delete the hospital network's files if the victim did not pay the ransom within ten days).

33. Melissa Hathaway, *Hijacked and Paying the Price-Why Ransomware Gangs Should Be Designated as Terrorists*, INST. FOR NEW ECON. THINKING (May 13, 2021), https://www.ineteconomics.org/perspectives/blog/hijacked-and-paying-the-price-why-ransomware-gangs-should-be-designated-as-terrorists.

34. *See* Hathaway, *supra* note 33.

Iran, and North Korea provide protection to some of the most notorious ransomware gangs, including Charming Kitten, Lazarus group, and REvil Corp., among others.[35] The relationship between the country and the cyber gang is symbiotic.[36] The country provides the gang safe harbor in exchange for a kick-back of the ransom payments or for the gang to act periodically on behalf of the government.[37] Ultimately, governments that are hostile to the U.S. can utilize cyber gangs to surreptitiously commit crimes using ransomware while avoiding responsibility among the international community.[38]

As noted above, the federal government's stance on ransomware payments is inconsistent.[39] Currently, some agencies discourage paying ransoms while others incentivize it.[40] The FBI warns against paying a ransom for several reasons, including that payment does not guarantee the victim organization will regain access to its system.[41] However, the more important reason is that when an organization pays a ransom, it feeds into a vicious cycle by incentivizing cyber gangs to continue launching attacks.[42] Organizations that pay the ransom also encourage other actors to start extorting victims through ransomware because they make it a lucrative business.[43] Consistent with the FBI, the Department of Justice (DOJ) announced after the Colonial attack that it would investigate

---

35. *Id.*

36. *Id.*

37. *Id.*; *see also* Frank Bajak, *How The Kremlin Provides a Safe Harbor for Ransomware*, AP NEWS (Apr. 16, 2021), https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7eb3841be45dff2d93ed3102999 (noting security researchers, U.S. law enforcement, and the Biden Administration agree that Russian cyber criminals dominate ransomware gangs and are sometimes employed by Russian intelligence agencies); Danielle Gilbert, *Ransomware Lessons for a Nation Held Hostage*, LAWFARE (Sept. 12, 2021, 10:01 AM), https://www.lawfareblog.com/ransomware-lessons-nation-held-hostage (arguing that Russian and other state protections for cyber gangs fuel the ransomware attacks abroad).

38. *See* Hathaway, *supra* note 33.

39. *See* Suderman & Gordon, *supra* note 21.

40. *Id.*; *see Ransomware*, FBI, *supra* note 28 (stating that the FBI does not support paying a ransom in response to a ransomware attack).

41. *See Ransomware*, FBI, *supra* note 28.

42. *Id.*

43. *Id.*

ransomware attacks at a level it reserved only for terrorism.[44] In addition, the organizations that pay a ransom run the risk of violating the Office of Foreign Assets Control's regulations.[45]

However, the IRS complicates the matter by incentivizing organizations to pay ransoms by allowing them to write off payments from annual taxable income as a part of the cost of doing business.[46] As a result, organizations may choose to pay the ransom instead of beefing up their security to prevent an attack from succeeding.[47] By providing organizations a financial incentive to pay the ransom, the federal government also encourages cyber gangs to continue attacks.[48]

Insurance policies also play a role in the ransomware ecosystem. Organizations that hold ransomware insurance are more likely to be targeted by cyber gangs.[49] Notably, how the

---

44. Anthony Spadafora, *IT Workers Believe Ransomware is as Serious as Terrorism*, TECHRADAR (Jan. 3, 2022), https://www.techradar.com/news/it-workers-believe-ransomware-is-as-serious-than-terrorism; *see Ransomware and Terrorism: For Security Pros the Threat is Equal*, HELP NET SEC. (Dec. 30, 2021), https://www.helpnetsecurity.com/2021/12/30/ransomware-threats-prioritized [hereinafter HELP NET SEC.]; *see also* Hathaway, *supra* note 33 (reporting the DOJ launched a new task force to target ransomware because it harms Americans' safety and health) [hereinafter HELP NET SEC.].

45. *See* OFF. OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY, ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS 3 (2020); *see also* Hathaway, *supra* note 33 (noting that the U.S. Treasury Office of Foreign Assets Control List includes a cyber gang known as Evil Corp for its role in producing and distributing malware used to further crimes against banks and financial organizations).

46. *See Extorted By Ransomware Gangs? The Payments May Be Tax-Deductible*, CBS NEWS (June 21, 2021, 1:21 PM), https://www.cbsnews.com/news/ransomware-payments-may-be-tax-deductible/ ("[M]ultiple tax experts interviewed by the Associated Press said deductions of ransomware payments as a cost of doing business are usually allowed under law and established guidance.").

47. *See* HELP NET SEC., *supra* note 44 (noting a recent survey of organizations found that less than one-third of the respondents implement basic security mechanisms that would disrupt ransomware attacks); *45% Companies Don't Have Cybersecurity Leader: Study*, CISOMAG (Dec. 11, 2017), https://cisomag.eccouncil.org/45-companies-dont-cybersecurity-leader-study/ (reporting a survey revealed 45% of respondents state their organization lacks reliable cybersecurity leadership).

48. *Extorted By Ransomware Gangs? The Payments May Be Tax-Deductible*, *supra* note 46 (reporting cybersecurity policy professor, Josephine Wolff, argues that the tax write off encourages payments which in turn encourage more ransomware attacks).

49. Hathaway, *supra* note 33 ("Regulators, like the New York State's Department of Financial Services . . . have argued that the insurance market may 'fuel the vicious cycle

federal government allows insurance companies to provide support for ransomware attacks is inconsistent with the law because ransomware payment facilitation may violate regulations issued by the Department of Treasury's Office of Foreign Assets Control.[50]

In short, the inconsistent laws and policies within the U.S. have fostered an ecosystem in which ransomware thrives. Foreign countries that oppose the U.S. benefit from cyber gangs that launch harmful attacks on the American people. Indeed, the impacts of ransomware are detrimental to Americans, which is what we will examine next.

B. Ransomware Impacts on the American Public

The impacts of ransomware and the cost of paying the ransom are not limited to the organization from which the cyber gang is demanding payment. Rather, the effects are wide-reaching and often borne by the public.[51] For example, gas prices increased as a result of the Colonial attack.[52] Indeed, prices rose to their highest levels since 2018.[53] Notably, eighteen states declared a state of emergency because of the effects of the Colonial attack.[54]

But ransomware attacks have additional consequences that are not as apparent. National security experts argue that such

---

of ransomware' because some victims are specifically being targeted because they have [cyber] insurance.").

50. Alvaro Marañon & Stephanie Pell, *Countering the Ransomware Threat: A Whole-of-Government Effort*, LAWFARE (Nov. 22, 2021, 10:56 AM), https://www.lawfareblog.com/countering-ransomware-threat-whole-government-effort [hereinafter Marañon & Pell, *Countering the Ransomware Threat*] (explaining that the Office of Foreign Assets Control took action against organizations involved in facilitating financial transactions to ransomware cyber gangs).

51. *See* Alvaro Marañon & Benjamin Wittes, *Ransomware Payments and the Law*, LAWFARE (Aug. 11, 2021, 3:52 PM), https://www.lawfareblog.com/ransomware-payments-and-law (currently, victim companies can hedge risk by "sloughing" cost of ransoms onto larger market and tax deductibility of ransoms means U.S. Treasury is essentially subsidizing ransomware payments).

52. Mary-Ann Russon, *US Fuel Pipeline Hackers 'Didn't Mean to Create Problems'*, BBC (May 10, 2021), https://www.bbc.com/news/business-57050690 (reporting gas prices rose by six cents per gallon because of the Colonial attack).

53. Matthew Trushinski, *Colonial Pipeline Threat Overview*, ARCTIC WOLF (May 11, 2021), https://arcticwolf.com/resources/blog/colonial-pipeline-threat-overview.

54. *Id.*

ransomware payments have increased the tax burden on Americans.[55] The Colonial attack has also cost taxpayers by draining judicial resources through class-action litigation,[56] which can be costly and time-consuming. For example, several class action lawsuits were filed against Colonial because they failed to use adequate cybersecurity measures.[57] In addition, the DOJ and other agencies expended time and money in their efforts to assist Colonial with addressing the attack and retrieving part of the payment.[58]

Ransomware attacks have detrimental consequences for the American population in general.[59] However, ransomware has a disproportionate impact on minority groups and females in particular.[60] A recent study shows that cybercriminals target minority groups and females at a higher rate than others.[61] This study notes that 59% of the general population respondents reported they were able to avoid financial impact caused by cybercrime, but only 47% of respondents who identified as belonging to a minority group reported being able to successfully avoid financial impacts caused by such crimes.[62]

Additionally, a former senior policy adviser at the Department of Homeland Security argues that minority groups are disproportionately impacted by cyberattacks on critical infrastructure.[63] One reason they are particularly vulnerable is

---

55. *See* Marañon & Wittes, *supra* note 51 (arguing taxes are rising due to criminal ransomware payments).

56. *See* Bryan & Lonergan, *supra* note 8 (discussing two class action lawsuits arising from the attack—one of which is on behalf of more than 11,000 gas stations).

57. *Id.* (reporting a second putative class action lawsuit was filed against Colonial for failing to implement adequate cybersecurity measures).

58. *See* Kovski, *supra* note 5 (explaining that the FBI, CISA, and other agencies worked with Colonial to respond to the attack).

59. *See* Marañon & Wittes, *supra* note 51 (describing ransomware attacks on both the fuel and meat industries that caused regional fuel shortages and increased the prices of beef and pork for Americans).

60. Tara Seals, *Women, Minorities Are Hacked More Than Others*, THREAT POST (Sept. 27, 2021, 2:27 PM), https://threatpost.com/women-minorities-hacked/175038/.

61. *Id.*

62. *Id.*

63. Camille Stewart, *Systemic Racism is a Cybersecurity Threat*, COUNCIL ON FOREIGN RELS. (June 16, 2020, 6:08 PM), https://www.cfr.org/blog/systemic-racism-cybersecurity-threat.

because emergency response capabilities and public health security are lower in minority and low-income communities.[64] Therefore, while all communities are ultimately impacted, minority groups may experience the brunt of it.[65]

Ransomware also impacts education.[66] With the onset of COVID-19 in 2020, ransomware attacks on schools increased by 20% compared to the prior year.[67] Students have experienced identity theft because their data was released,[68] and many days of learning have been lost.[69] In 2020, eighty-three ransomware attacks affected 1,753 schools and colleges that caused 578 days of downtime, and impacted 1.3 million students; the cost of which is estimated to be $7.2 billion.[70] In December 2020, the FBI, CISA, and the Multi-State Information Sharing and Analysis Center warned that the onslaught of cyberattacks on schools will likely continue.[71] The impact will be especially challenging for schools with limited resources.[72] Notably, schools that primarily serve minority groups tend to have limited resources.[73]

In 2018, the Department of Defense issued a new cyber strategy in which the government committed to "defend forward

---

64. *Id.*

65. *Id.*

66. *See* Maggie Miller, *School Districts Struggle to Defend Against Rising Ransomware Attacks*, THE HILL (May 19, 2021, 6:00 AM), https://thehill.com/policy/cybersecurity/553506-school-districts-struggle-to-defend-against-rising-ransomware-attacks?rl=1.

67. *Id.*

68. *Id.*

69. *Id.*

70. Paul Bischoff, *Ransomware Attacks on US Schools and Colleges Cost $3.56bn in 2021*, COMPARITECH (June 23, 2022), https://www.comparitech.com/blog/information-security/school-ransomware-attacks/#How_does_2020_compare_to_previous_years.

71. FBI et al., *Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (2020), https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-345a.

72. FBI et al., *Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (2020), https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-345a.

73. *See* Clare Lombardo, *Why White School Districts Have So Much More Money*, NPR (Feb. 26, 2019, 2:00 PM), https://www.npr.org/2019/02/26/696794821/why-white-school-districts-have-so-much-more-money.

to disrupt or halt malicious cyber activity at its source."[74] However, the government itself lacks the personnel required to deal with the onslaught of attacks.[75] A fundamental change to the current legal framework is needed. In the spirit of defending forward, the federal government should recognize ransomware attacks as terrorism and ensure organizations are lawfully allowed to engage in self-defense to deter future attacks. These topics will be the focus of the remainder of this Comment.

III. ANALYSIS

A. *How Ransomware Fits the Legal Definition of Terrorism*

Under American law, terrorism has different definitions, many of which are drafted to serve a particular purpose.[76] Under both 18 U.S.C. § 2331 and the State Department's definition of terrorism, the Colonial ransomware cyberattack can be categorized as terrorism under the law.[77]

1. 18 U.S.C. § 2331

Under 18 U.S.C. § 2331, terrorism requires actions that are violent, dangerous to human life, or are a crime under American law.[78] DarkSide's ransomware attack created an environment that was dangerous to human life by holding hostage the system

74. STEPHEN DYCUS ET AL., NAT'L SEC. LAW 428 (7th ed. 2020, Wolters Kluwer Legal & Regul. U.S.).

75. David Strom, *What Are the Legalities and Implications of 'Hacking Back'?*, SEC. INTEL. (May 29, 2018), https://securityintelligence.com/what-are-the-legalities-and-implications-of-hacking-back ("Most of these agencies lack the skills or staffing to pursue cyber counter-measures. In many government agencies, there are numerous job vacancies for security analysts—so they are often not centers of excellence when it comes to hacking back efforts.").

76. Sudha Setty, *What's in a Name? How Nations Define Terrorism Ten Years After 9/11*, 33:1 UNIV. PA. J. INT'L L. 1, 18–19 (2011).

77. *See generally* Jonathan Turley, *Why the White House Won't Define Pipeline Attack as Terrorism*, THE HILL (May 15, 2021, 10:00 AM), https://thehill.com/opinion/white-house/553690-why-the-white-house-wont-define-darksides-pipeline-attack-as-terrorism?rl=1.

78. 18 U.S.C. § 2331(1)(A) ("[Terrorism means] violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States . . . or that would be a criminal violation if committed within the jurisdiction of the United States . . .").

that supplied the fuel on which hospitals, medical facilities, fire departments, and law enforcement agencies depended on for operations.[79] DarkSide acted violently in the cyberworld by breaking past a security system, entering onto Colonial's property without authorization, and holding the system hostage.[80] This violence caused significant harm in the physical world.[81] Further, if the attack had not been carried out via the internet, DarkSide would have had to actually break and enter Colonial's physical facilities to take control of the computer systems.

The Computer Fraud and Abuse Act (CFAA) is widely considered to impose criminal liability on hacking because it imposes liability on anyone who "intentionally access[es] a protected computer without authorization[,] . . . which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States" and causes damage or loss.[82] By hacking into Colonial's computer system, DarkSide violated the CFAA.[83]

Additionally, under 18 U.S.C. § 2331's definition of terrorism, the acts must appear to be intended to "intimidate or coerce a civilian population."[84] DarkSide succeeded in its attempt to coerce the ransomware payment from Colonial by causing a disruption in the fuel supply to a large segment of the American population.[85] In particular, DarkSide satisfied the elements of terrorism in 18 U.S.C. § 2331 by criminally trespassing into Colonial's systems, intending to coerce a ransom payment that is ultimately borne by the general population.[86]

---

79. *See* Alexander Mallin & Luke Barr, *DOJ Seizes Millions in Ransomware Paid by Colonial Pipeline*, ABC NEWS (June 7, 2021, 2:25 PM), https://www.yahoo.com/gma/doj-seizes-millions-ransom-paid-190900933.html; Turley, *supra* note 77 ("The Colonial Pipeline attack was the cyber equivalent of Pearl Harbor"); Trushinski, *supra* note 53 (reporting that eighteen states declared a state of emergency due to the attack).

80. *Id.*

81. *Id.*

82. 18 U.S.C. §§ 1030(a)(5)(C), (e)(2)(B).

83. *See id.*

84. 18 U.S.C. § 2331(1)(B)(i).

85. *See* Turley, *supra* note 77 (arguing that DarkSide committed an act of terrorism by disrupting Colonial's system to coerce the population for profits).

86. *See id.*; 18 U.S.C. § 2331(1)(A)–(C).

2. The State Department's Legal Standard for Foreign Terrorist Organizations

The State Department's definition of terrorism, which is used to classify certain groups as foreign terrorist organizations (FTOs), is also important. This standard focuses more on the motivation of the malicious actors than 18 U.S.C. § 2331. First, to be an FTO, the malicious actors must be a foreign organization, and the terrorism activity must threaten the U.S.'s national security, which can include interfering with foreign relations and economic interests.[87] DarkSide is a foreign organization located in Russia. Its actions threatened national security by damaging foreign relations with Russia and causing President Biden to speak with Vladimir Putin about the attack.[88] Additionally, the attack impacted economic interests by causing significant financial damage to Colonial and to the tens of millions of Americans who relied on Colonial for fuel, including hospitals, emergency medical services, law enforcement agencies, fire departments, airports, truck drivers, and the public in general.[89] Indeed, these actions threatened national security.[90]

However, the State Department also requires, per 22 U.S.C. § 2656f(d)(2), premeditated, politically motivated violence for an organization to be deemed an FTO.[91] While DarkSide has denied

87. Bureau of Counterterrorism, *Foreign Terrorist Organizations*, U.S. DEP'T OF STATE, https://www.state.gov/foreign-terrorist-organizations (listing the legal criteria for designation of a Foreign Terrorist Organization) (last visited Feb. 21, 2022).

88. *See* President Joseph Biden, Remarks by President Biden on the Colonial Pipeline Incident (May 13, 2021) (transcript available on https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident) ("We have been in direct communication with Moscow about the imperative for responsible countries to take decisive action against these ransomware networks.").

89. *See* Mallin & Barr, *supra* note 79.

90. *See generally* Hathaway, *supra* note 33 (arguing that hijacking institutions, intimidation, coercing ransomware payments, and disrupting civil order are threats to economic prosperity and security of the U.S.); Marañon & Pell, *supra* note 50 (noting ransomware attacks that are directed at the U.S.'s critical infrastructure threaten national security).

91. 22 U.S.C. § 2656f(d)(2); *see generally* Turley, *supra* note 77.

political affiliations,[92] the organization's behavior demonstrates political motivation.

Interestingly, DarkSide has not targeted any Russian organizations.[93] DarkSide engineered its platform to work only in certain geographical regions, which is a common practice of cyber gangs.[94] The program that DarkSide used to break into other systems was coded with a "do-not-install list" of countries that included former Soviet Satellites that have favorable relations with the Russian government.[95] Specifically, DarkSide's hacking software would check for the presence of a particular language and would fail to install if the language belonged to one of the countries affiliated with Russia.[96] This revelation has prompted a cybersecurity expert to recommend that organizations install one of the languages that Russian cyber gangs avoid.[97] DarkSide's selectiveness lends support to the argument that the cyber gang has some political motivation when choosing its victims.[98]

While inconclusive, there is some evidence that DarkSide is working, or has worked, under the authority of the Russian government.[99] However, even if DarkSide is not taking direction from Russia, its careful avoidance of targeting Russian

92. Eamon James, *Here's the Hacking Group Responsible for the Colonial Pipeline Shutdown*, CNBC (May 10, 2021, 9:25 AM), https://www.cnbc.com/2021/05/10/hacking-group-darkside-reportedly-responsible-for-colonial-pipeline-shutdown.html.

93. *See* Brian Krebs, *Try This One Weird Trick Russian Hackers Hate*, KREBS ON SEC. (May 17, 2021), https://krebsonsecurity.com/2021/05/try-this-one-weird-trick-russian-hackers-hate.

94. *Id.*

95. *Id.*

96. *Id.*

97. *See id.*

98. *See* Jurgita Lapienyte, *Colonial Pipeline Hack: DarkSide's Claim to Be Apolitical Doesn't Carry Much Weight*, CYBERNEWS, https://cybernews.com/news/colonial-pipeline-hack-darksides-claim-to-be-apolitical-doesn't-carry-much-weight (last visted Sept. 28, 2021).

99. *See* Dustin Carmack, *What We Know About DarkSide, The Russian Hacker Group That Just Wreaked Havoc on the East Coast*, THE DAILY SIGNAL (May 20, 2021), https://www.dailysignal.com/2021/05/20/what-we-know-about-darkside-the-russian-hacker-group-that-just-wrecked-havoc-on-the-east-coast (suggesting it is likely that cyber gangs have military or intelligence backgrounds with cyber training).

organizations is a pro-Russia policy.[100] Ultimately, DarkSide's behavior results in harm to Russia's adversaries while Russia remains untouched.[101]

If this evidence is insufficient to satisfy the political motivation requirement of terrorism, Congress should consider redefining the definition to include groups that are motivated to commit acts of terrorism for financial gain, especially in the cyber context.[102] In keeping with modern advancements, the United Kingdom includes in its definition of terrorism actions that are designed to "interfere with or seriously disrupt an electronic system."[103] Congress would do well to craft laws against terrorism in a similar manner, addressing the modern methods terrorists use to accomplish their goals.

The Biden Administration carefully avoids referring to the Colonial cyberattack as terrorism and resists discussing the ransomware payment.[104] When the administration addressed the payment, it placed responsibility for the payment on the private sector and downplayed the government's responsibility to prevent such attacks.[105] The likely reason for the Biden Administration's hesitancy is that, if the propagators of such ransomware attacks are designated terrorists within the U.S., the ransomware payment becomes more problematic because the U.S. has a policy of not negotiating with terrorists' demands for ransom payments.[106] Indeed, the U.S. will not pay ransoms to terrorists even in situations involving hostages.[107] The rationale behind this policy is that paying ransoms would only encourage more hostage

100. *See* Lapienyte, *supra* note 98 (noting DarkSide operates in a manner that Russia desires).

101. Carmack, *supra* note 99.

102. Turley, *supra* note 77.

103. Terrorism Act 2000, c.11, § 1(2)(e) (U.K.).

104. Turley, *supra* note 77 (noting President Biden when facing questions regarding the payment to DarkSide answered "No comment").

105. *See id.* (noting deputy national security advisor Anne Neuberger stated "Colonial is a private company, and we'll defer information regarding their decision on paying a ransom to them.")

106. *See id.*; *see* Audrey Kurth Cronin, *Hostage Negotiations and Other Talks with Terrorists: Price v. Principle*, GEO J. INT'L AFFAIRS 104, 106 (2015).

107. Cronin, *supra* note 106, at 106 ("Unlike most European governments, the U.S. government has a clear policy that it will not pay ransoms.").

situations.[108] As noted above, the FBI recognizes that paying ransomware encourages and incentivizes further ransomware attacks.[109] Like hostage situations, where human life may be at stake, ransomware can also put human life at stake when critical infrastructure is locked down. When ransomware payments are made, cyber gangs are rewarded, the cycle continues, and the risk to Americans is perpetuated. However, if ransomware is recognized as terrorism, organizations would not be allowed to pay the ransom because it would be illegal. Organizations that pay could potentially be prosecuted for providing material support for terrorism. This Comment will explore this topic next and the additional benefits of recognizing ransomware as terrorism.

B. The Benefits of Recognizing Ransomware Attacks as Terrorism

Under 18 U.S.C. § 2339B(a)(1), individuals who knowingly provide material support or resources to an FTO or an organization that has engaged in terrorism can be fined and possibly imprisoned.[110] Outside of the cyber context, the federal government has the ability to prosecute individuals who pay ransoms to FTOs holding human hostages.[111] In a similar manner, the government should prosecute individuals who pay ransomware demands for providing material support for terrorism.

While the State Department can designate a cyber gang like DarkSide an FTO, this may be difficult to do for every cyber gang because the identity of the organization committing the attack is

---

108. *Id.* at 106 ("[T]he logic is that kidnappers should be punished, not rewarded, and that future hostage-takers will be dissuaded by the show of force . . ."); Tom Cole, *Negotiating with Terrorists*, CONGRESSMAN TOM COLE (Aug. 29, 2016), https://cole.house.gov/media-center/weekly-columns/negotiating-terrorists.

109. *Ransomware*, FBI, *supra* note 28.

110. 18 U.S.C. § 2339B(a)(1) ("Whoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined . . . or imprisoned . . . or both . . . To violate this paragraph, a person must have knowledge that the organization is a designated terrorist organization[,] . . . that the organization has engaged or engages in terrorist activity . . . or that the organization has engaged or engages in terrorism . . .").

111. Cronin, *supra* note 106, at 106.

not always known or may be learned after the payment has been made. Additionally, some cyber gangs commit attacks under various names. However, 18 U.S.C. § 2339B also allows prosecution if the person making the payment knew that the cyber gang engages or has engaged in acts of terrorism.[112] This route of prosecution would be a viable method of payment deterrence.

Recognizing ransomware as terrorism would not only help to curb ransomware in general by disincentivizing further attacks, but it would also comply with how the majority of Americans want the government to address ransomware. A recent study revealed that nine out of ten Americans believe ransomware attacks should be treated as terrorism.[113] The same study found that nearly four out of five Americans want the law to forbid private companies from making ransomware payments to cyber gangs.[114] The American population's stance on treating ransomware as terrorism is consistent with the opinion of many cybersecurity experts.[115] A recent survey of companies lends further support to this interpretation. It showed that 22% of respondents believe it is morally wrong to pay ransomware even if the attack compromises critical business systems and data.[116] Another survey showed that over half of the companies that said they would pay a ransom also said they would refuse to pay if they were required to report payments to the government and suffer the publicity.[117] Companies recognize that ransomware payments are not viewed favorably by the public.[118]

---

112. 18 U.S.C. § 2339B(a)(1).

113. Danny Bradbury, *Majority of Americans Say Ransomware Attacks Should Be Considered Terrorism*, IT PRO (Jan. 7, 2022), https://www.itpro.com/security/ransomware/361921/majority-of-americans-say-ransomware-should-be-considered-terrorism.

114. *Id.*

115. Spadafora, *supra* note 44 (explaining that a survey of 1,506 information technology security leaders from different countries around the world found 60% believe ransomware should be treated like terrorism).

116. *Id.*

117. HELP NET SEC., *supra* note 44 ("37% of respondents would pay the ransom but 57% would reverse that decision if they had to publicly report the payment, as required by the Ransomware Disclosure Act, a U.S. Senate bill that would require organizations to report ransomware payments within forty-eight hours.").

118. *See id.* ("37 % of respondents would pay the ransom but 57% would reverse that decision if they had to publicly report the payment, as required by the Ransom Disclosure

Recognizing ransomware as terrorism would eliminate the problems ransomware insurance causes by fueling ransomware attacks. Recognizing ransomware as terrorism would prompt organizations to actively defend their computer systems because ransomware payments would be illegal,[119] and by consequence, insurance for such payments would be as well. As a result, cyber gangs would be less incentivized to launch attacks because they are less likely to succeed and less likely to be paid.

Recognizing ransomware as terrorism would also address problems caused by countries that provide a safe harbor to cyber gangs. If the government were to recognize ransomware as terrorism, safe harbor countries would be affected through the international community. Although the international community has criminalized hostage situations through the Geneva Conventions,[120] it has not yet transferred this law to cyberspace. But if the U.S. government were to treat ransomware on par with terrorism, it is likely that other governments will follow the U.S.'s example. As a result, governments that create a safe harbor for cyber gangs would be internationally pressured to dismantle the gang operations.[121]

Finally, the federal government would form a consistent posture against ransomware payments if it were to recognize ransomware as terrorism. The IRS would no longer allow companies to cast the financial burden of ransomware payments on the American people by writing off payments as business expenses. Given the growing and unsettling effect that cyber gangs are having on Americans and the disproportionate effect

---

Act, a U.S. Senate bill that would require companies to reprot ransomeware payments within 48 hours.").

119. *See* Hathaway, *supra* note 33 ("[T]he U.S. Department of Justice should determine and make clear that paying a ransom is illegal. This step would likely force organizations to further invest in their security and ability to withstand and recover from an incident (i.e., increase their resilience).").

120. *See* American Red Cross, *Summary of the Geneva Conventions of 1949 and Their Additional Protocols*, INT'L HUMANITARIAN L., April 2011 at 4 (mentioning Articles 33 and 34 which prohibit the taking of hostages).

121. *See* Hathaway, *supra* note 33 ("U.S. Representative Jim Langevin recently stated that 'if the international community can identify areas where a country is clearly looking the other way and it has a concentration of bad actors and they're not doing enough to shut down these bad actors, there's a role for international, multi-nation efforts to hold nations accountable.'").

such crime has on minority communities, it is especially critical that the federal government take notice and act to form a unified response to ransomware.

C. *A Potential Problem: Will Criminalizing Ransomware Payments Encourage Cyber Gangs to Target Critical Organizations?*

A common argument against criminalizing ransomware payments is that it will encourage cyber gangs to create situations where payment cannot be refused by targeting critical organizations.[122] Hospitals, energy providers, and water-treatment plants would be pressured into violating the law by paying the ransom to avoid the harm that may result from downtime.[123] However, this type of attack is already occurring at an extraordinary rate.[124] This is because ransomware attacks by nature are characterized by intimidation, coercion, and extortion, making organizations with little capacity for downtime the prime targets.[125]

If payments are legal, critical organizations will still be the primary target for cyber gangs simply because they are less able to tolerate taking their computer systems offline compared to noncritical organizations. Instead of continuing this cycle, the government should consider other ways of deterring cyber gangs from targeting critical organizations. In particular, the government should consider empowering organizations to defend

---

122. *See* Marañon & Wittes, *supra* note 51.

123. *See id.*

124. *See* Office of Information Security, *Ransomware Trends 2021*, U.S. DEP'T OF HEALTH & HUM. SERVS. at 5 (June 3, 2021), https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf (noting forty-eight ransomware incidents targeting healthcare industry between January 1, 2021, and May 25, 2021); *see* Joe Tidy, *The Ransomware Surge Ruining Lives*, BBC (Apr. 30, 2021), https://www.bbc.com/news/technology-56933733 (explaining that cyber gangs routinely target schools and hospitals with ransomware attacks).

125. *See* Hathaway, *supra* note 33 ("Ransomware gangs have been hijacking the IT systems, data, and operations of our hospitals, schools, corporations, and critical infrastructure services — thereby disrupting civil order and stability by interfering with the peace, security, and normal functioning of our communities. The ransomware operators' principal tactics include intimidation, coercion, and extortion until the victim entity capitulates to their demands in order to avoid future injury or secondary effects.").

themselves through regulated hackbacks performed by licensed cybersecurity firms.

D. A Solution: Hackbacks Should be Legalized to Deter Cyber Gangs

The term "hackback" can have two meanings. It can be used to refer to any "defensive measure" by which the victim of an attack uses to intrude on the malicious actor's computer system.[126] It can also be used in a narrower sense to refer to self-defense measures that have either a damaging effect on the malicious actor's computer or that provide ongoing access to it.[127] Those who use the latter definition usually distinguish hackbacks from active self-defense, which is considered a less aggressive response.[128] For purposes of this Comment, "hackback" will be used to refer to any defensive measure where the malicious actor's computer is accessed.

In general, the law criminalizes hackbacks.[129] As noted above, the CFAA is widely considered to impose criminal liability for hacking because it imposes liability on anyone who hacks into another computer, including foreign computers.[130] Additionally, the DOJ states that hackbacks may be illegal even if the victim hacks with good intentions or to prevent further damage to its own system.[131] This stance against hackbacks conflicts with the general legal principle that an entity may use reasonable force to defend its property.[132] Why should the rules of self-defense be different in cyberspace than in the physical world?

---

126. *See* CHESNEY, *supra* note 7, at 201.

127. *See id.*

128. *See id.*

129. *See* Sam Parker, *Shot in the Dark: Can Private Sector "Hackbacks" Work?*, 13 J. NAT'L SEC. L. & POL'Y 211, 211 (2022).

130. *See* 18 U.S.C. §§ 1030 (a)(5)(C), (e)(2)(B).

131. *See* H. MARSHALL JARRETT ET AL., PROSECUTING COMPUTER CRIMES 180 (2015) (noting the DOJ advises victims of an attack not to "take any offensive measures" on its own, including "'hacking back' into the attacker's computer" in part because "[d]oing so may be illegal regardless of the motive.").

132. Zach West, *Young Fella, if You're Looking for Trouble I'll Accommodate You: Deputizing Private Companies for the Use of Hackback*, 63 SYRACUSE L. REV. 119, 130 (2012).

There are valid concerns about legalizing hackbacks. A primary concern is one of attribution; whether the hackback will be targeted against the correct malicious actor.[133] While many companies argue that they should be able to hack back to retrieve their decryption keys and that they have the technical capabilities and expertise to do so, some experts advise against hackbacks for the same reason. For example, the DOJ warns against hackbacks[134] reasoning there is a legitimate potential to harm innocent network users because it can be difficult to identify the malicious actor.[135] Additionally, cyber gangs are constantly evolving their techniques to stay ahead of law enforcement;[136] it is concerning whether organizations will be able to keep up with these changes.

Another major concern is that hackbacks can result in unintended conflicts with the international community.[137] Foreign governments may attribute the hackback to the U.S. government or simply hold the U.S. government responsible for

133. *See* JARRETT ET AL., *supra* note 131, at 180; *see* Steve Ranger, *Hacking Back is a Terrible Idea, But Companies Are Still Keen to Try it*, ZDNET (Dec. 1, 2017), https://www.zdnet.com/article/hacking-back-is-a-terrible-idea-but-some-companies-are-still-keen-to-try-it.

134. *See id.*

135. *See* Steve Ranger, *supra* note 133; *see* Corey E. Thomas, *Why Companies Shouldn't Try to Hack Their Hackers*, HARV. BUS. REV. (May 24, 2017), https://hbr.org/2017/05/why-companies-shouldnt-try-to-hack-their-hackers; *see* Don Mclean, *The Problems with Hacking Back*, AFCEA INT'L (May 30, 2018), https://www.afcea.org/signal-media/problems-hacking-back (arguing that the main problem with hacking back is identifying the real malicious actor and that innocent bystanders can be harmed in the process of hacking back).

136. *See* Thomas, *supra* note 135.

137. *See* Robert Knake, *Instead of Hacking Back, U.S. Companies Should Let Cyber Command Do it for Them*, COUNCIL ON FOREIGN RELS. (May 30, 2018, 10:00 AM), https://www.cfr.org/blog/instead-hacking-back-us-companies-should-let-cyber-command-do-it-them (stating some cybersecurity experts are concerned about private companies hacking back because they could initiate conflicts that will require the military to resolve); *see* Mclean, *supra* note 135 (explaining that hackbacks are illegal under international law and transnational hacking in response to a cyberattack could cause conflict with foreign nations); *see* West, *supra* note 132, at 136.

it.[138] If the U.S.'s relations are strained with a particular country, a hackback could escalate the situation to armed conflict.[139]

A potential solution to this dilemma is to license cybersecurity firms that have been vetted by the government to hack back. These experts should be licensed to perform hackbacks only after receiving sufficient training to recognize when a hackback should or should not be launched based on attribution and international relations. Training would help to eliminate the potential for conflicts with foreign governments and harm to innocent network users. As a team, the cybersecurity experts would assess whether a hackback would be a proper response to the attack and they would work collaboratively to mitigate damages and retrieve the organization's decryption keys and data.[140] The government could either review the actions of the cybersecurity firms periodically or in real-time to verify compliance within appropriate guidelines.

Could adequate training and oversight from the government really alleviate the primary concerns with hackbacks? In short, yes. Under the CFAA, the government has an exception to the law against hacking.[141] The government already engages in successful hackbacks either through its own cyber experts or through contracted experts.[142] Indeed, the training that the specialists would receive alleviates these concerns because the government already has the skills necessary to avoid harming innocent third parties and international conflict.

Additionally, there are significant benefits to legalizing hackbacks. While the FBI has the skills necessary to hack back, it does not have the resources to help most organizations suffering

---

138. *See* West, *supra* note 132, at 136.

139. *See id.* (discussing the escalatory impact hackbacks may have on international relations).

140. *See* Josephine Wolff, *When Companies Get Hacked, Should They Be Allowed to Hack Back?*, THE ATLANTIC (July 14, 2017), https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679 (noting professor of law Jeremy Rabkin has argued for the government to compile a list of cybersecurity firms that have been vetted and approved to hackback as a way of providing companies with the option of self-defense).

141. 18 U.S.C. § 1030(f); *see* West, *supra* note 132, at 139–40.

142. CHESNEY, *supra* note 7, at 218 (noting that most domestic legal systems permit government agencies to engage in unauthorized access).

from ransomware attacks.[143] There is evidence that some U.S. companies already engage in hackbacks and would be willing resources for self-defense.[144] Many cybersecurity experts already have the technical knowledge on how to perform a hackback.[145] By using these available resources, the government would reduce the pressure it is experiencing to combat ransomware on its own. Thus, hackbacks performed by a team of trained specialists would be a viable method of halting current attacks, deterring future ones, and avoiding ransomware payments.

In 2012, an observer commented, "While the U.S. government slowly formulates a coherent cyber-policy and plays politics over cyber-legislation, U.S. companies lose billions of dollars."[146] Ten years later, we find our nation in the same, or perhaps worse, situation. The current legal frameworks surrounding ransomware and hackbacks do not work.[147] The federal government should heed the American people's call to modernize legal interpretations of terrorism and to activate reasonable cyber self-defense measures so our nation as a whole is prepared to engage with and meet the challenges presented by cyberspace.

IV. CONCLUSION

The Colonial ransomware attack had a major impact on Americans. It caused fuel shortages and increased gas prices along the East Coast and beyond.[148] Ransomware attacks are increasing,[149] partly because many countries that are hostile to the U.S. provide these gangs safe harbor.[150] However, organizations in the U.S. are not adequately protecting their

143. Wolff, *supra* note 140 (noting former homeland security assistant secretary, Stewart Baker, argues that the government is too preoccupied with protecting their own data to provide resources to outside organizations).

144. *See* West, *supra* note 132, at 143–44.

145. See *id.* at 133 (noting that cybersecurity officials are currently developing hackback technologies).

146. *Id.* at 135.

147. *See supra* notes 33-50, 129-132, and accompanying text.

148. *See* Trushinski, *supra* note 53 (reporting gas prices rose to their highest since 2018 and eighteen states declared a state of emergency because of the Colonial attack).

149. *See* Emsisoft Malware Lap, *supra* note 2 (noting the increase of ransomware attacks facing the United States).

150. Hathaway, *supra* note 33; *see also* Bajak, *supra* note 37.

computer systems; often organizations opt to pay a ransom instead of taking preventative measures by investing in adequate security.[151] The federal government's stance on ransomware payments is inconsistent: sometimes the government incentivizes payment while other times it discourages payment.[152] Payments ultimately continue the ransomware cycle that is scarring the U.S. through the disruption of critical infrastructure and services. Notably, the effects of ransomware attacks are felt most severely by females and minority groups.[153] Cyber gangs often target schools and organizations in low-income areas with fewer resources to combat ransomware.[154]

This Comment argues that we can curb ransomware by recognizing it as terrorism. Under 18 U.S.C. § 2331, ransomware can be recognized as terrorism because it creates an environment that is dangerous by disrupting critical services. Ransomware is used with the intent to intimidate and coerce organizations and the public by holding hostage critical services and infrastructure until a ransom is paid.[155] The public ultimately bears this cost. Ransomware can also be recognized as terrorism under the State Department's definition, which is used to designate certain organizations as FTOs. Specifically, ransomware is most often propagated by foreign entities.[156] Under such circumstances, it threatens the U.S.'s national security by damaging foreign relations and the lives and safety of Americans. It impacts economic interests by causing financial damage to the victim organizations, and in turn, the people who relied on those organizations for resources. Cyber gangs demonstrate political

---

151. *See* HELP NET SEC., *supra* note 44 (recent survey of organizations found that less than one-third of the respondents implement basic security mechanisms that would disrupt ransomware attacks); *45% Companies Don't Have Cybersecurity Leader: Study*, *supra* note 47 (survey revealed 45% of respondents state their organization lacks reliable cybersecurity leadership).

152. *See* Suderman & Gordon, *supra* note 21.

153. Seals, *supra* note 60.

154. *See supra* notes 71-73 and accompanying text; *see also* Miller, *School Districts Struggle to Defend Against Rising Ransomware Attacks*, *supra* note 66 (noting an increase in cybercriminal attacks on "vulnerable" school districts).

155. 18 U.S.C. §§ 2331(1)(B)(i)-(ii); *see generally* Turley, *supra* note 77 (arguing why ransomware gangs should be designated as terrorists).

156. *See generally* Hathaway, *supra* note 33.

motivation by targeting the U.S. as an enemy of the country providing the gangs with safe harbor.[157]

Recognizing ransomware as terrorism would have several benefits. First, it would make ransomware payments illegal, and it would be possible to prosecute those who pay a ransom for providing material support for terrorism. Second, it would be consistent with what the majority of Americans want and would ensure organizations take proactive measures to defend their systems instead of waiting to address an attack after it happens. Third, it would create a government posture that is unified against ransomware and ransom payments. Finally, recognizing ransomware as terrorism would encourage the international community to take a unified stance against ransomware, which would put pressure on the countries providing safe harbor to the cyber gangs.

A major concern about making ransomware payments illegal is that this will encourage cyber gangs to attack critical organizations on which life depends, such as hospitals.[158] However, hackbacks are a viable solution to prevent this from happening. By licensing certain cybersecurity firms with adequate training to hack back, we can deter cyber gangs through regulated self-defense. Thus, combining the recognition of ransomware as terrorism with carefully regulated measures of self-defense will decrease ransomware attacks and lessen the effects that such terrorism has on our nation.

157. *See* Hathaway, *supra* note 33 (noting that countries with a long record of hostility against the United States channel these political motivations to form symbiotic relationships with cybercriminals, leveraging these proxies and their cyber expertise to commit international crimes using ransomware); *see also supra* notes 93-101 and accompanying text.

158. Marañon & Wittes, *supra* note 51.