St. John's Law Review

Volume 96, 2022, Number 2 Article 8

Was the Colonial Cyberattack the First Act of Cyberwar Against the U.S.? Finding the Threshold of War for Ransomware Attacks

Liam P. Bradley

WAS THE COLONIAL CYBERATTACK THE FIRST ACT OF CYBERWAR AGAINST THE U.S.? FINDING THE THRESHOLD OF WAR FOR RANSOMWARE ATTACKS

LIAM P. BRADLEY[†]

INTRODUCTION

On May 7, 2021, "DarkSide," a foreign hacker group, conducted a ransomware attack against the Colonial Pipeline ("Colonial").[1] That morning, Colonial discovered a "ransom note demanding cryptocurrency."[2] The attack forced the shutdown of the Colonial Pipeline, stopping the daily delivery of 2.5 million barrels (MMBbls) of "gasoline, jet fuel and diesel" to the East Coast.[3] The shutdown created fuel shortages, impacted financial markets, and panicked the public.[4] The resulting fuel shortages and economic impacts "triggered a comprehensive federal

[†] Senior Staff Member, *St. John's Law Review*, J.D. Candidate, 2023, St. John's University School of Law; B.S., 2018, United States Military Academy. Special thanks to Professor Margaret McGuinness for her constructive guidance throughout the writing process, Devlin Winkelstein and Nerea Cal for their continued mentorship, and the team down in Houston, TX for their insight on the energy industry.

[1] Dustin Carmack, *What We Know About DarkSide, the Russian Hacker Group that Just Wreaked Havoc on the East Coast*, HERITAGE FOUND. (May 20, 2021), https://www.heritage.org/cybersecurity/commentary/what-we-know-about-darkside-the-russian-hacker-group-just-wreaked-havoc [https://perma.cc/KDV3-QZPQ]; William Turton & Kartikay Mehrotra, *Hackers Breached Colonial Pipeline Using Compromised Password*, BLOOMBERG (June 4, 2021, 3:58 PM), https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password [https://perma.cc/RH94-G22G].

[2] Turton & Mehrotra, *supra* note 1.

[3] *Id.*; Eric Geller, *What You Need to Know About the Colonial Pipeline Hack*, POLITICO (May 10, 2021, 7:21 PM), https://www.politico.com/news/2021/05/10/colonial-pipeline-cyber-486726 [https://perma.cc/G92V-XPB5] (also noting that the ransomware attack targeted their payroll and regulation systems, and Colonial deactivated pipeline operations because of the uncertainty as to the extent of the attack).

[4] Christopher Bing & Stephanie Kelly, *Cyber Attack Shuts Down U.S. Fuel Pipeline "Jugular," Biden Briefed*, REUTERS (May 8, 2021, 12:54 AM), https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/ [https://perma.cc/DQ3F-KRG7].

response" on May 11, 2021.[5] On May 12, CEO Joseph Blount paid a ransom of nearly $5 million in bitcoin to restore control.[6] The federal government treated the attack as a cybercrime, ultimately seizing and returning some of the ransom payment.[7]

Ransomware attacks, like the attack against Colonial, are the leading type of cyberattack.[8] Norton Security estimated that in 2021, "there [would] be a ransomware attack on businesses every 11 seconds."[9] While a majority of cyberattacks are treated as matters for law enforcement, critical questions arise when the attack is a matter of national security.[10] At what point does a cybercrime become more than a cybercrime? At what point is the attack an act of war? Here, the Colonial cyberattack provides a case study for analyzing whether a ransomware attack on critical infrastructure constitutes an act of war. Creating a threshold for acts of cyberwar is critical to developing future strategies to deter cyberattacks and avoid a so-called "Cyber–Pearl Harbor."[11]

This Note argues that the Colonial cyberattack was an act of cyberwar because the attack crossed a six-factor threshold

---

[5] Action Update, The White House, Fact Sheet: The Biden-Harris Administration has Launched an All-of-Government Effort to Address Colonial Pipeline Incident (May 11, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/11/fact-sheet-the-biden-harris-administration-has-launched-an-all-of-government-effort-to-address-colonial-pipeline-incident/ [https://perma.cc/CW4Y-V7DP].

[6] David E. Sanger & Nicole Perlroth, *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity*, N.Y. TIMES (June 8, 2021), https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html [https://perma.cc/Q4VD-GSEM]; Carmack, *supra* note 1.

[7] Press Release, U.S. Dep't of Just., U.S. Att'y's Off., Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (June 8, 2021) [hereinafter DOJ Press Release], https://www.justice.gov/usao-ndca/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists [https://perma.cc/VD9K-NLC2].

[8] Samara Lynn & Catherine Thorbecke, *Why Ransomware Cyberattacks are on the Rise*, ABC NEWS (June 4, 2021, 5:00 AM), https://abcnews.go.com/Technology/ransomware-cyberattacks-rise/story?id=77832650 [https://perma.cc/Z4QL-P87K]; IBM SECURITY, X-FORCE THREAT INTELLIGENCE INDEX 4, 7 (2022).

[9] Clare Stouffer, *115 Cybersecurity Statistics and Trends You Need to Know in 2021*, NORTON (Aug. 9, 2021), https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html [https://perma.cc/7FDA-QQN6].

[10] *See, e.g.*, Andrew Burt & James C. Trainor, *Our Government's Approach to Cybersecurity is a Costly Mess. Here's What Would Fix the Problem,* TIME (Jan. 2, 2020, 12:44 PM), https://time.com/5757811/cybersecurity-attacks-agency/ [https://perma.cc/3MTS-GQJR].

[11] *See generally* Robert Kenneth Palmer, *Critical Infrastructure: Legislative Factors for Preventing a "Cyber–Pearl Harbor"*, 18 VA. J.L. & TECH. 289 (2014).

developed from both domestic and international "laws of war."[12] Therefore, the federal government can respond to the Colonial cyberattack with military force as authorized under 10 U.S.C. § 394 and subsequent presidential policy directives ("PPDs").[13] Under this statute, a military response could have been led by U.S. Cyber Command ("USCYBERCOM") or conventional military forces.[14]

Part I of this Note discusses ransomware and the current domestic and international legal frameworks behind cybercrime and cyberwarfare. Part II creates a six-factor threshold for cyberwar developed from the law and argues that the Colonial cyberattack crossed that threshold into cyberwar. Further, this Part describes what a military response under 10 U.S.C. § 394 would look like. Finally, while this Note identifies the ability to use military force, such force should only be used proportionally and as a means of self-defense or deterrence.

I. BACKGROUND

A. Law Governing Ransomware

1. Definition of Ransomware

Ransomware is a type of cyberattack, which has become more popular with a 148% increase in attacks in 2021.[15] The Federal Bureau of Investigation ("FBI") defines ransomware as "[A] type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return."[16] The U.S. Army's definition is similar, but recognizes the role of cryptocurrency in the ransom demand and the use of data encryption to hold the

---

[12] *Infra* Part II and Conclusion.

[13] *Infra* Section I.A.2.b.

[14] 10 U.S.C. § 394; Memorandum from President Barack Obama on U.S. Cyber Operations Policy to the Presidential Cabinet (Oct. 16, 2012) (on file with the National Security Archive). U.S. Cyber Command (USCYBERCOM) covers all military operations in the cyber domain. *About: Our History*, U.S. CYBER COMMAND, https://www.cybercom.mil/About/History/ [https://perma.cc/D2P2-MD2H] (last visited Sept. 7, 2022).

[15] Rob Sobers, *81 Ransomware Statistics, Data, Trends and Facts for 2021*, VARONIS (July 2, 2021), https://www.varonis.com/blog/ransomware-statistics-2021/ [https://perma.cc/4STM-7534].

[16] *Common Scams and Crimes: Ransomware*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware [https://perma.cc/87HG-8YT9] (last visited Sept. 7, 2022).

user hostage.[17] Overall, there are three components unique to ransomware: (1) "[a]n application that encrypts and decrypts data," (2) "[f]iles containing encryption keys," and (3) "software that allows anonymity on the Internet."[18] Then, there is the demand, which extorts the victim.[19] While this extortion is illegal,[20] victims that pay the ransom are currently not violating any U.S. laws.[21] However, ransomware is not limited to just the definitional confines of crime.[22] When transnational actors perpetrate ransomware attacks across international borders, their actions can be acts of war.[23] Determining if the attack has surpassed the criminal level requires an understanding of the legal distinctions between cybercrime and cyberwar, beginning with U.S. law and ending with international law.[24]

2. U.S. Law

a. Cybercrime

The federal government adjudicates cyberattacks as both breaches of the Computer Fraud and Abuse Act ("CFAA") and violations of traditional criminal codes, such as kidnapping or

---

[17] Ronna Weyland, *Ransomware: A Virtual Hostage Situation*, U.S. ARMY (Feb. 17, 2021), https://www.army.mil/article/243420/ransomware_a_virtual_hostage_situation.

[18] Ion Paraschiva, *WannaCry Ransomware Attack from Romanian Police Perspective*, 8 INT'L J. INFO. SEC. & CYBERCRIME 65, 66 (2019).

[19] Lawrence J. Trautman & Peter C. Ormerod, *Wannacry, Ransomware, and the Emerging Threat to Corporations*, 86 TENN. L. REV. 503, 538 (2019) (identifying computer ransomware as a "newly technologically-enabled extortion business model" in illicit business).

[20] *See, e.g.*, 18 U.S.C. § 875.

[21] *See* Mark Kauzlarich, *Should Ransomware Payments Be Made Illegal?*, WALL ST. J. (Sept. 7, 2021, 5:12 PM), https://www.wsj.com/articles/ransomware-payment-illegal-ban-11631047209 [https://perma.cc/5C5J-JPHD]. *But see* U.S. Dep't of Treasury, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Sept. 21, 2021), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf (noting that ransom payments are illegal if they violate U.S. sanctions).

[22] *See generally* Maj. Gen. Charles J. Dunlap, Jr., *"Cybervandalism" or "Digital Act of War?" America's Muddled Approach to Cyber Incidents will not Deter More Crises*, 42 N.C. J. INT'L L. 989 (2017).

[23] *Id.* at 990.

[24] *See* Jed Babbin, *When Should a Cyberattack be Declared an Act of War?*, WASH. TIMES (Aug. 4, 2021), https://www.washingtontimes.com/news/2021/aug/4/when-should-a-cyberattack-be-declared-an-act-of-wa/ [https://perma.cc/ZU5L-QUXB].

money laundering.[25] This Section will discuss cybercrime law at the state level before turning to the federal level to explain the law, the relevant actors, and the application of this law in the Colonial cyberattack.

Individual states include more relevant cybercrime laws because they are a more localized and responsive government than the federal government.[26] Some states provide ransomware definitions and offenses within their criminal code.[27] Unlike federal case law, which finds computer fraud even if the computer itself does not cause the transaction,[28] some states' case law recognizes that not every ransomware attack constitutes fraud if the proper cybersecurity measures are not in place.[29] Further, some states have pending legislation banning ransomware payments.[30] States even have their own cybercrime squads in law enforcement.[31] Although state claims are enforceable, most ransomware attacks are prosecuted at the federal level because of the jurisdictional difficulty, state law variations, and the interstate nature of cybercrime.[32]

---

[25] *See, e.g.*, 18 U.S.C. § 1030; 18 U.S.C. § 1202. *See also* 18 U.S.C. § 1203; 18 U.S.C. § 1956.

[26] *See generally* THE FEDERALIST NO. 46 (James Madison) (mentioning that the state governments are more focused on local issues and that popular measures in individual states can be enacted immediately). For a list of individual states' cybercrime laws, see COMPUTER CRIME STATUTES, NATIONAL CONFERENCE OF STATE LEGISLATURES (Sep. 8, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx [https://perma.cc/C6LB-7U35].

[27] *See*, *e.g.,* WYO. STAT. ANN. § 6-3-507 (West 2017); CAL. PENAL CODE § 523 (West 2018); TEX. PENAL CODE ANN. § 33.023 (West 2017).

[28] *See* Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur., 895 F.3d 455, 461–62 (6th Cir. 2018); McClellan v. Cantrell, 217 F.3d 890, 893 (7th Cir. 2000) ("Fraud is a generic term, which embraces all the multifarious means which human ingenuity can devise and which are resorted to by one individual . . . ." (quoting Stapleton v. Holt, 207 Okla. 443, 445 (1952)).

[29] *See* G&G Oil Co. of Ind., Inc. v. Cont'l W. Ins. Co., 165 N.E.3d 82, 89 (Ind. 2021) ("We do not think every ransomware attack is necessarily fraudulent.").

[30] *See* S. 6806A, 2021–22 Leg., Reg. Sess. (N.Y. 2021); H.R. H813, 2021 Gen. Assemb., Reg. Sess. (N.C. 2021); S. 726, 2021 Gen. Assemb., Reg. Sess. (Pa. 2021). *But see* H.R. 3892, 87th Leg., Reg. Sess. (Tex. 2021) (failed).

[31] *See, e.g.*, *Cyber Security*, TEX. DEP'T PUB. SAFETY, https://www.dps.texas.gov/section/cyber-security [https://perma.cc/SF67-8ZZE] (last visited Sept. 7, 2022) (noting a cyber operations team that "provides a Computer Security Incident Response Team (CSIRT) to State and Local government organizations in response to cyber-attacks").

[32] *See* Gabriole Zeviar-Geese, Note, *The State of the Law on Cyberjurisdiction and Cybercrime*, 1 GONZ. J. INT'L L. 119, 131–32 (1998); NCSL, *supra* note 26; H. MARSHALL JARRETT ET AL., PROSECUTING COMPUTER CRIMES 113 (2017) (noting that "the inexorable connection between the Internet and interstate commerce may

At the federal level, Congress initially balanced federal and state interests for cybercrime offenses.[33] However, federal jurisdictions now recognize that the interstate commerce requirement is sufficiently satisfied whenever a computer is connected to the internet, data is transmitted over the internet, or a defendant uses the internet to commit a crime.[34] Therefore, most cyberattacks are prosecuted under federal law through the Department of Justice ("DOJ") and investigated by the FBI.[35]

The federal government prosecutes cyberattacks as violations of the CFAA, 18 U.S.C. § 1030.[36] The CFAA, enacted in 1986, is the successor to the Comprehensive Crime Control Act of 1984, which "address[ed] the unauthorized access and use of computers and computer networks."[37] The CFAA expanded on this unauthorized access felony to include "seven types of criminal activity."[38] A summary of those seven offenses, with their corresponding section number and recommended sentencing guidelines, is available in Table 1 below.[39]

Table 1: CFAA Violations and Penalties

Section	Offense	Years
(a)(1)	Obtaining National Security Information	10 (20)
(a)(2)	Accessing a Computer and Obtaining Information	1 or 5 (10)
(a)(3)	Trespassing in a Government Computer	1 (10)
(a)(4)	Accessing a Computer to Defraud & Obtain Value	5 (10)
(a)(5)(A)	Intentionally Damaging by Knowing Transmission	1 or 10 (20)
(a)(5)(B)	Recklessly Damaging by Intentional Access	1 or 5 (20)
(a)(5)(C)	Negligently Causing Damage & Loss by Intentional Access	1 (10)
(a)(6)	Trafficking in Passwords	1 (10)
(a)(7)	Extortion Involving Computers	5 (10)

Note: Years in parentheses indicate the maxium number of years for second convictions.

sometimes be sufficient to satisfy the [federal] jurisdictional element of the statute at issue.").

[33] S. REP. NO. 99–432, at 4 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482.

[34] *See* Cont'l Grp., Inc. v. KW Prop. Mgmt., LLC, 622 F. Supp. 2d 1357, 1370 (S.D. Fla. 2009); NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1060 (S.D. Iowa 2009); U.S. v. Sutcliffe, 505 F.3d 944, 952 (9th Cir. 2007); U.S. v. MacEwan, 445 F.3d 237, 244 (3d Cir. 2006).

[35] *Cybersecurity Unit*, DOJ (Apr. 12, 2022), https://www.justice.gov/criminal-ccips/cybersecurity-unit [https://perma.cc/K3X9-RKKW] ("[T]he Criminal Division created the Cybersecurity Unit within the Computer Crime and Intellectual Property Section to serve as a central hub for expert advice and legal guidance."); *What We Investigate: Cyber Crime,* FBI, https://www.fbi.gov/investigate/cyber [https://perma.cc/R5AE-ZSCX] (last visited Sept. 7, 2022).

[36] *See* JARRETT ET AL., *supra* note 32, at 1; 18 U.S.C. § 1030.

[37] JARRETT ET AL., *supra* note 32, at 1.

[38] *Id.* at 3.

[39] The table is supplied by the authors. *Id.*

The CFAA also criminalizes conspiring or attempting to commit these cybercrimes.[40] Further, the CFAA provides for forfeiture of anything used to commit an offense or any benefit derived from it.[41] Finally, 18 U.S.C. § 1030(d) authorizes the FBI as the "primary authority to investigate offenses . . . for any cases involving espionage, foreign counterintelligence, [or] information protected . . . for reasons of national defense or foreign relations."[42]

The DOJ can also charge hackers with violations of other anti-fraud statutes depending on the effects of the ransomware.[43] For example, the DOJ can charge "ransomware attackers and developers with conspiracy to violate the federal wire fraud statute" under 18 U.S.C. § 1343.[44] Depending on the type of ransomware tactics employed, such as 'double extortion,' additional charges for disclosing trade secrets may be available under the Economic Espionage Act ("EEA").[45] Attacks that fraudulently obtain financial information may be pursued under the Gramm-Leach-Bliley Act,[46] while attacks targeting healthcare providers may be subject to violations of the Health Insurance Portability and Accountability Act of 1996 ("HIPPA").[47]

Finally, cybercrimes are also prosecuted under traditional criminal codes, as if the crime happened physically and not digitally.[48] For example, the DOJ has charged six Russian Main Intelligence Directorate ("GRU") agents with "conspiracy, computer hacking, wire fraud, aggravated identity theft, and false registration of a domain name" for causing blackouts in the Ukrainian electrical grid, interference in French elections, and delays in Pennsylvania hospital systems.[49] "[A]ggravated

---

[40] 18 U.S.C. § 1030(b). The punishments are provided in 18 U.S.C. § 1030(c).

[41] 18 U.S.C. § 1030(g); 18 U.S.C. § 1030(j).

[42] 18 U.S.C. § 1030(d)(2).

[43] PETER G. BERRIS & JONATHAN M. GAFFNEY, RANSOMWARE AND FEDERAL LAW: CYBERCRIME AND CYBERSECURITY 4 (2021).

[44] *See id.*; *see also* 18 U.S.C. § 1343.

[45] *See* 18 U.S.C. §§ 1831–1832, 1839(3); BERRIS & GAFFNEY, *supra* note 43.

[46] BERRIS & GAFFNEY, *supra* note 43, at 12; *see also* 15 U.S.C. § 6801 et seq.

[47] BERRIS & GAFFNEY, *supra* note 43, at 12. These regulations appear to affect the entities charged with protecting the information rather than the hackers themselves. *Id.*

[48] KRISTIN M. FINKLEA & CATHERINE A. THEOHARY, CYBERCRIME: CONCEPTUAL ISSUES FOR CONGRESS AND U.S. LAW ENFORCEMENT 4 (2012).

[49] Press Release, Dep't of Just., Off. of Pub. Affs., Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and

identity theft" is an example of a traditional crime being applied alongside CFAA offenses.[50] In addition, money laundering,[51] hostage taking,[52] and ransom seeking are additional offenses that may be charged.[53] If the ransomware attack is ideologically motivated or allocates ransom funds towards terrorist organizations, the DOJ can attach offenses for supporting terrorism.[54]

The DOJ and FBI classify cybercrimes as export enforcement, economic espionage, or sanctions-related criminal cases.[55] The DOJ charges cybercriminals through their National Security Division,[56] alongside their Cybersecurity Unit with the Computer Crime and Intellectual Property Section.[57] The FBI investigates and executes the DOJ's orders.[58] The FBI receives reports through their Internet Crime Complaint Center ("IC3") and spearheads thirty other agencies in cybercrime response operations as part of the National Cyber Investigative Joint Task Force ("NCIJTF").[59] There are no mandatory reporting requirements *between* the DOJ and other governmental agencies.[60] For the Colonial cyberattack, the FBI responded in

---

Other Disruptive Actions in Cyberspace (Oct. 19, 2020), https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and [https://perma.cc/ X6B7-D5WA].

[50] *See id.*; 18 U.S.C. § 1028A.

[51] 18 U.S.C. § 1956.

[52] 18 U.S.C. § 1203.

[53] 18 U.S.C. § 1202.

[54] *See, e.g.*, 18 U.S.C. § 2332b; 18 U.S.C. § 2339A.

[55] *See generally* U.S. DEP'T OF JUST., SUMMARY OF MAJOR U.S. EXPORT ENFORCEMENT, ECONOMIC ESPIONAGE, AND SANCTIONS-RELATED CRIMINAL CASES (2019), https://www.justice.gov/nsd/page/file/1044446/download [https://perma.cc/S8C2-FEWN].

[56] *Combatting National Security Cyber Threats*, DOJ (Sept. 10, 2015), https://www.justice.gov/nsd/about-division-0 [https://perma.cc/9VNF-GHCU].

[57] *Cybersecurity Unit*, *supra* note 35.

[58] *What We Investigate: Cyber Crime*, *supra* note 35.

[59] *Id.*

[60] *See id.* The agency's role is to "coordinate, integrate, and share infomation." *Id.* "Federal entities are encouraged to share CTIs [cyber threat indicators] and DMs [defensive measures] as broadly and as quickly as possible." OFF. OF THE DIR. OF NAT'L INTEL., DEP'T OF HOMELAND SEC., DEP'T OF DEF., & DEP'T OF JUST., SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 4–5 (2016), https://www.cisa.gov/sites/default/files/publications/Federal%20 Government%20Sharing%20Guidance%20under%20the%20Cybersecurity%20Information%20Sharing%20Act%20of%202015_1.pdf [hereinafter SHARING OF CYBER]. "Congress designed CISA [Cybersecurity Information Sharing Act of 2015] to create a voluntary cybersecurity information sharing process." *Id.* at 6. The National Security

partnership with the DOJ's Ransomware and Digital Extortion Task Force.[61]

The federal government consistently handles cyberattacks as crimes.[62] The FBI's cybercrime strategy imposes "risk and consequences on cyber adversaries."[63] This prosecution-focused strategy has several benefits.[64] First, cybercrimes have the same consequences as traditional crimes—forfeiture and imprisonment.[65] Further, "criminal charges educate the world about the persons specifically involved and the methods they use."[66] Charges also restrict the identified cybercriminal's physical travel to the U.S. or to countries where the U.S. has extradition treaties.[67] Finally, this strategy enforces sanctions to deter both those conducting attacks and third parties that may stand to benefit.[68]

Memorandum ("NSM"), recently signed by President Biden on January 19, 2022, only provides for the sharing of directives between the NSA and DHS. Action Update, The White House, Fact Sheet: President Biden Signs National Security Memorandum to Improve the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems (Jan. 19, 2022), https://www.whitehouse.gov/ briefing-room/statements-releases/2022/01/19/fact-sheet-president-biden-signs-national-security-memorandum-to-improve-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/ [https://perma.cc/52G4-TMW3].

[61] Both the DOJ's Criminal and National Security Divisions were involved as well. *See* DOJ Press Release, *supra* note 7.

[62] The agency interchangeably uses "cyber crime," "cyber threat," "malicious cyber activities," and "cyber attack[ ]." *What We Investigate: Cyber Crime*, *supra* note 35. *See generally, e.g.*, Affidavit in Support of an Application for a Seizure Warrant at 5–8, No. 3:21-mj-70945 (N.D. Cal. Jun. 7, 2021) [Hereinafter Affidavit].

[63] *FBI Strategy Addresses Evolving Cyber Threat*, FBI (Sept. 16, 2020), https://www.fbi.gov/news/stories/wray-announces-fbi-cyber-strategy-at-cisa-summit-091620 [https://perma.cc/2X7D-YKMG].

[64] *See generally* FINKLEA & THEOHARY, *supra* note 48.

[65] *Id.* at 3 ("[O]ne way of viewing cybercrimes is that they are digital versions of traditional offenses."); Affidavit, *supra* note 62, at 3 ("One of the chief goals of forfeiture is to remove the profit from crime by separating the criminal from his or her dishonest gains."); *see also* U.S. v. Newman, 659 F.3d 1235, 1242 (9th Cir. 2011); U.S. v. Casey, 444 F.3d 1071, 1073 (9th Cir. 2006).

[66] Austin Max Scherer, *Cybercrime: Seizing Illicit Proceeds of and Combating Ransomware Attacks*, 37 IELR 237, 238 (2021).

[67] *Id.* For example, see the detainment of Huawei CFO, Meng Wanzhou, by the Canadian government after the U.S. issued a warrant for her arrest. Moria Warburton & Sarah Berman, *Defense Tells Canada Court that Huawei CFO's Arrest Was Legal, but Not Her Detainment*, REUTERS (Mar. 31, 2021, 7:14 PM), https://www.reuters.com/article/us-usa-huawei-tech-canada/defense-tells-canada-court-that-huawei-cfos-arrest-was-legal-but-not-her-detainment-idUSKBN2BN3MD [https://perma.cc/MP69-FCZT].

[68] *See* Zachary K. Goldman & Damon McCoy, *Economic Espionage: Deterring Financially Motivated Cybercrime*, 8 J. NAT'L SEC. L. & POL'Y 595, 603–04 (2017).

Consistent with their strategy, the government prosecuted the DarkSide hackers for violating various federal statutes on computer hacking and money laundering.[69] The suspected violations were "Title 18, United States Code, Section 1030(a)(2)(C), Unauthorized Access to a Protected Computer to Obtain Information, Title 18, United States Code, Section 1030(a)(5)(A), Intentional Damage to a Protected Computer, Title 18, United States Code, Section 1030(a)(7)(C), Extortion Involving Computers . . . and Title 18, United States Code, Section 1956 (Money Laundering)."[70] These violations were investigated after "Victim X"—Colonial—paid 75 Bitcoin ("BTC"), approximately $4.3 million at the time, to the cryptocurrency address provided in the ransomware attack.[71] Then, the FBI tracked the ransom payment as it was transferred to different cryptocurrency addresses.[72] After a warrant was issued,[73] the FBI seized the tracked payments, securing 63.7 BTC, approximately $2.3 million, on June 8, 2021.[74] The press release did not mention any other cyber response measures to defend or recover Colonial's data.[75] Colonial still lost $2.2 million in its ransom payment—leaving Darkside with a payment valued $300,000 above DarkSide's normal "earnings per hack."[76]

But see id. at 606–07, for a discussion on the potential drawbacks for unknowingly involved third parties.

[69] Affidavit, *supra* note 62, at 5–8.

[70] *Id.* at 5.

[71] *Id.* at 6.

[72] *Id.* at 6–7.

[73] Warrant to Seize Property Subject to Forfeiture, No. 3:21-mj-70945-LB (N.D. Cal. Jun. 7, 2021) [Hereinafter Warrant].

[74] *See* DOJ Press Release, *supra* note 7.

[75] *Id. But see* Turton & Mehrotra, *supra* note 1. Colonial's own cybersecurity team along with Mandiant, a cybersecurity firm that is part of FireEye, Inc., conducted the sweep of any malicious cyber activity before Colonial reopened the pipeline. *Id.*

[76] It is difficult to determine actual time value of money because of Bitcoin's fluctuation when the date and time of the ransom payment and recovery are not disclosed. *See Bitcoin Price*, COINBASE, https://www.coinbase.com/price/bitcoin [https://perma.cc/BZH8-MLWW] (last visited Sept. 7, 2022); *see also* Ryan Browne, *Hackers Behind Colonial Pipeline Attack Reportedly Received $90 Million in Bitcoin Before Shutting Down*, CNBC (May 18, 2021, 4:19 PM), https://www.cnbc.com/2021/05/18/colonial-pipeline-hackers-darkside-received-90-million-in-bitcoin.html [https://perma.cc/8RR8-AT87] ("[T]he average [ransom] payment from organizations was likely $1.9 million" and that DarkSide made "$90 million in bitcoin ransom payments over the past nine months from 47 victims.").

While Colonial recovered some of its ransom payment, the federal government's cybercrime strategy was not a success.[77] Despite discouraging ransomware payments because they fuel future attacks and funds are not always recoverable,[78] most victims pay.[79] While cybercriminals are indicted, they are usually judgment-proof.[80] For example, Russian cybercriminals cannot be prosecuted because the U.S. lacks jurisdiction over them, and they cannot be prosecuted in Russia because hacking U.S. entities is not a violation of Russian law.[81] Furthermore, documents which expose DOJ and FBI methodologies are revealed to the public when used as evidence in court, which can frustrate their efforts to combat cybercrime.[82] Finally, the current strategy has not deterred cybercrime, as ransomware attacks were up 148% in 2021.[83]

b. Cyberwar

Cyberattacks may also be viewed from the cyberwarfare perspective, which threatens hackers with either a digital or kinetic military response.[84] Because there have been no openly declared acts of cyberwar perpetuated against the U.S., understanding what constitutes an act of cyberwar requires an examination of the legal framework, historical precedents, and guidance from policy leaders.[85]

---

[77] Robert Anderson, Jr., *How Government and Industry are Failing in Battle Against Ransomware Attacks*, THE HILL (Oct. 21, 2021, 7:30 AM), https://thehill.com/opinion/cybersecurity/577650-how-government-and-industry-are-failing-in-battle-against-ransomware [https://perma.cc/GVJ6-YZU2].

[78] Erick Tucker, *US Recovers Most of Ransom Paid After Colonial Pipeline Hack*, AP NEWS (June 7, 2021), https://apnews.com/article/technology-business-government-and-politics-8e7f5b297012333480d5e9153f40bd52 [https://perma.cc/7R2E-RW7A].

[79] *See* Anderson, *supra* note 77.

[80] *See* Scherer, *supra* note 66, at 239.

[81] *Id.* at 238–39 (noting that one "disadvantage is that, as long as some countries harbor [cybercriminals] and refuse to extradite or prosecute them, they can still live well and continue their criminal activities").

[82] *Id.*

[83] Sobers, *supra* note 15.

[84] Helena Roland, *The Survival of Critical Infrastructure: How Do We Stop Ransomware Attacks on Hospitals?*, 29 CATH. U. J.L. & TECH. 177, 188 (2020) (noting that cyberattacks can be viewed both a crime and as warfare). *See also* Paul K. Davis, *Deterrence, Influence, Cyber Attack, and Cyberwar*, 47 N.Y.U. J. INT'L L. & POL. 327, 339 (2015) (noting that cyberattacks may be accompanied by conventional military force, therefore, deterrence must cover both cyber and traditional war).

[85] *See* Isaac R. Porche III, *Fighting and Winning the Undeclared Cyber War*, RAND BLOG (June 24, 2019), https://www.rand.org/blog/2019/06/fighting-and-

The authority for the U.S. to respond with military force originates in the U.S. Constitution.[86] Further, a state of war may "exist without formal declaration by Congress."[87] Therefore, the President, as "Commander in Chief,"[88] can utilize force at his discretion.[89] Congress limited this discretion following the Vietnam War.[90] The War Powers Resolution permits the President to deploy U.S. troops—"introduce . . . Armed Forces into hostilities"—if there is "(1) a declaration of war, (2) specific statutory authorization, or (3) a national emergency created by attack upon the United States, its territories or possessions, or its armed forces."[91] Furthermore, the United States has used military force in response to attacks from non-state actors, as authorized under the Authorization for the Use of Military Force ("AUMF"), following 9/11.[92] Overall, this legal framework is flexible and permits military response for attacks that constitute hybrid warfare or levels below the threshold of traditional armed conflict.[93]

With regard to cyberwarfare, 10 U.S.C. § 394 authorizes a military response to cyberattacks and delegates response

---

winning-the-undeclared-cyber-war.html [https://perma.cc/97JN-ENBB] (noting that war is no longer openly declared, rather it exists in a "gray area below the threshold of total war").

[86] U.S. CONST. art. I, § 8, cl. 11.

[87] *See* Constitution Annotated, *Power to Declare War*, CONGRESS.GOV, https://constitution.congress.gov/browse/essay/artI_S8_C11_1/ [https://perma.cc/Z7UD-KB6Y] (last visited Sept. 7, 2022); *see also* Prize Cases, 67 U.S. 635, 660–61 (1862) ("The function to use the army and navy being in the President . . . must be subject to his discretion as a necessary incident to the use, in the absence of any Act of Congress controlling him.").

[88] U.S. CONST. art. II, § 2.

[89] *See In re* Neagle, 10 S. Ct. 658, 668–69 (1890) (recognizing the Executive's limited ability to deploy the military abroad); *see generally* U.S. v. Curtiss-Wright Export Corp., 299 U.S. 304 (1936), for a discussion of the President's lead role in foreign affairs.

[90] H.R. REP. No. 93–287, at 2352 (1973) (Conf. Rep.) ("President Kennedy would have been required to report to Congress in 1962 when he raised the number of U.S. military advisers in Vietnam from 700 to 16,000.").

[91] 50 U.S.C. § 1541(c).

[92] *See* AUMF, S.J. RES. 23, 107th Cong. (2001); *see also* Curtis A. Bradley & Jack L. Goldsmith, *Obama's AUMF Legacy,* 110 AM. J. INT'L L. 628, 635–36 (2016) (noting that "the administration fleshed out AUMF-related concepts" for "air strikes against al-Shabaab in Somalia, Al Qaeda in the Arabian Peninsula in Yemen, and the Khorosan Group in Syria").

[93] For a discussion on hybrid warfare see generally AARON F. BRANTLY ET AL., DEFENDING THE BORDERLAND: UKRAINIAN MILITARY EXPERIENCES WITH IO, CYBER, AND EW (Army Cyber Institute at West Point, 2017).

authority to the Executive branch.[94] The military, when properly authorized, may conduct "operations in cyberspace short of hostilities . . . or in areas in which hostilities are not occurring."[95] Furthermore, Presidential Policy Directive 20 ("PPD-20"), a leaked top-secret document by Edward Snowden,[96] delegated "[e]mergency [c]yber [a]ctions" to the Secretary of Defense ("SecDef").[97] This directive authorizes immediate cyber response operations to mitigate threats without briefing the President.[98] The responses are designed to be "nonlethal in purpose, action, and consequence," but are cyberattack dependent.[99] Military force is justified because of the "inherent right of self-defense . . . in international law to prevent imminent loss of life or significant damage with enduring national impact on . . . [g]overnment, U.S. critical infrastructure and key resources, or the mission of U.S. military forces."[100] Finally, although unclear to what extent, former President Trump removed many "restrictions governing the approval process for offensive cyberattacks conducted against U.S. adversaries under [PPD-20]."[101] While a military response exists, there is no redline for when a cyberattack would constitute an act of war and not a crime, according to U.S. doctrine.[102]

U.S. History offers precedents for when an attack is deserving of a military response.[103] The most apparent is when the U.S. declared war after the Japanese bombing of Pearl Harbor.[104] The second is the congressional response following

---

[94] 10 U.S.C. § 394.

[95] 10 U.S.C. § 394(b).

[96] *See* Luke Harding, *How Edward Snowden Went from Loyal NSA Contractor to Whistleblower*, GUARDIAN (Feb. 1, 2014, 6:00 EST), https://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract [https://perma.cc/ST76-PZYU].

[97] PPD-20, *supra* note 14, at 10.

[98] *Id.*

[99] *Id.*

[100] *Id.* (footnote omitted).

[101] Erica D. Borghard & Shawn W. Lonergan, *What do the Trump Administration's Changes to PPD-20 Mean for U.S. Offensive Cyber Operations?*, COUNCIL ON FOREIGN RELS. (Sept. 10, 2018, 10:18 AM), https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations [https://perma.cc/W526-HXQJ].

[102] *See generally* Jeffrey Greenley, *Set Computers to Stun: Proposed Cyberwar Rules of Engagement*, 38 U. DAYTON L. REV. 427, 439–46 (2013).

[103] *See generally* BARBARA SALAZAR TORREON & SOFIA PLAGAKIS, INSTANCES OF USE OF UNITED STATES ARMED FORCES ABROAD 1798–2021 (2021).

[104] Declaration of War on Japan, S.J. Res. 116, 77th Cong. (1941).

9/11 to grant the President the authorization "to use all necessary and appropriate force" against the terrorists that perpetrated the attack, any nation or organization that harbored the terrorists, or those that may commit future attacks.[105] Finally, Congress authorized military force against the Barbary pirates to protect U.S. commerce and sailors.[106]

In addition, experts and government officials provide insight into whether a cyberattack crosses the threshold for military force.[107] For instance, President Biden recently stated, "I think . . . if we end up in a war—a real shooting war with a major power—it's going to be as a consequence of a cyber breach."[108] Former Defense Secretary Leon Panetta warned of a possible "cyber-Pearl Harbor" in which "computer hackers . . . could dismantle the nation's power grid, transportation system, financial networks and government."[109] The Department of Homeland Security ("DHS") states that "[T]he warning signs are all present for a potential 'cyber 9/11' on the horizon."[110] In discussing cyberattacks, Sen. Susan Collins stated that, "[A] widespread attack on the power grid for the East Coast . . . would cause devastation," and a hacker-turned-security-strategist, Chris Thomas, opined that "If [a major cyberattack] happens, that's a major act of war."[111] Lastly, during a hearing before the Senate Armed Services Committee, the Under Secretary of Defense for Intelligence ("USDI") stated that "The determination

---

[105] Authorization for Use of Military Force ("AUMF"), S.J. Res. 23, 107th Cong. (2001).

[106] Act of Jan. 22, 1802, ch. 4, 2 Stat. 129 (1802).

[107] *See* James Berry Motley, *Grenada: Low-Intensity Conflict and the Use of U.S. Military Power*, 146 WORLD AFFS. 221, 232 (1983) ("[C]ivilian policymakers and senior military officers will have to decide 'when' military force is required to protect U.S. national interests.").

[108] Nandita Bose, *Biden: If U.S. Has 'Real Shooting War' it Could Be Result of Cyber Attacks*, REUTERS (July 28, 2021, 1:42 AM), https://www.reuters.com/world/biden-warns-cyber-attacks-could-lead-a-real-shooting-war-2021-07-27/ [https://perma.cc/N5P8-F4M2].

[109] Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. TIMES (Oct. 11, 2012), https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html [https://perma.cc/CG75-WJMB].

[110] *Secure Cyberspace and Critical Infrastructure*, DHS, https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure [https://perma.cc/L5ZQ-49P4].

[111] Katie Bo Williams & Cory Bennett, *Why a Power Grid Attack is a Nightmare Scenario*, HILL (May 30, 2016, 2:15 PM) (second alteration in original), https://thehill.com/policy/cybersecurity/281494-why-a-power-grid-attack-is-a-nightmare-scenario [https://perma.cc/E2D8-4D9M].

of what constitutes an 'act of war' in or out of cyberspace, would be made on a case-by-case and fact specific basis by the President."[112] "Specifically, cyber attacks that proximately result in a significant loss of life, injury, destruction of critical infrastructure, or serious economic impact should be closely assessed as to whether or not they would be considered an unlawful attack or an 'act of war.' "[113]

If a cyberattack warrants a military response, the two entities involved will be the DHS,[114] particularly the Transportation Security Administration ("TSA") and the Cybersecurity & Infrastructure Security Agency ("CISA"),[115] and the Department of Defense ("DoD"),[116] acting through USCYBERCOM.[117] In the event of a cyberattack, the DHS would provide the DoD with information about the attack that it collected from CISA per their collective information sharing initiative.[118] The DoD would receive this information through the DoD Cyber Crime Center ("DC3"), which "serves as [DoD's] operational focal point for voluntary cyberspace information sharing and incident reporting."[119] For cyberattacks on pipelines, the TSA's new directive mandates pipeline owners to report "confirmed and potential cybersecurity incidents" to CISA and employ a 24/7 Cybersecurity Coordinator.[120] Then, the President

---

[112] *Cybersecurity, Encryption and United States National Security Matters*: *Hearing Before the Comm. on Armed Servs.*, 114th Cong. 85 (2016) (statement of Marshall Lettre, Under Secretary of Defense for Intelligence) [hereinafter *Cybersecurity Hearing*]. Admiral Rogers, USCYBERCOM Commander, concurred with the USDI. *Id.* (statement of Admiral Michael Rogers, USCYBERCOM Commander & Director of the National Security Agency).

[113] *Id.*

[114] *See Department Organizational Chart*, DEP'T HOMELAND SEC. (Apr. 2, 2021), https://www.dhs.gov/sites/default/files/publications/21_0402_dhs-organizational-chart.pdf [https://perma.cc/CK7D-ULV3].

[115] *See* TRANSP. SEC. ADMIN., PIPELINE SECURITY GUIDELINES 6 (2d ed. 2021); *Cybersecurity*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/cybersecurity [https://perma.cc/42TY-QP7P] (last visited Sept. 7, 2022).

[116] *See* U.S. CYBER COMMAND, *supra* note 14.

[117] *Id.*

[118] *See* SHARING OF CYBER, *supra* note 60.

[119] DEP'T DEF., JOINT PUBLICATION 3–12 CYBERSPACE OPERATIONS I-13–14 (2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf [https://perma.cc/HG97-V4TP].

[120] Press Release, Dep't of Homeland Sec., DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators (May 27, 2021), https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators [https://perma.cc/D3D2-LUZU].

or DoD will decide if a military response is warranted.[121] Once the command is given to respond to the cyberattack with military force, USCYBERCOM will execute its mission.[122]

USCYBERCOM is "the nation's unified combatant command for the cyberspace domain," and is co-headquartered with the NSA.[123] Its mission is to "*defend forward* to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[124] USCYBERCOM's mission has three components: (1) "[E]nsure the U.S. military's ability to fight and win wars in any domain, including cyberspace;" (2) "preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident;" and (3) "strengthen cyber capacity, expand combined cyberspace operations, and increase bi-directional information sharing."[125] Depending on the mission selected, USCYBERCOM will carry out the military response or coordinate with other combatant commands if a conventional military response is authorized.[126]

3. International Law

While the U.S. has its own laws, precedents, and experts for differentiating an act of cyberwar from that of cybercrime, there is a transnational component of cyberattacks.[127] Therefore, an additional analysis of cybercrime and cyberwar is required on the international level.

---

[121] *See* 10 U.S.C. § 394; Williams & Bennet, *supra* note 111; *Cybersecurity Hearing*, *supra* note 112.

[122] U.S. CYBER COMMAND, *supra* note 14.

[123] *Id.*

[124] DEP'T OF DEF., SUMMARY DEPARTMENT OF DEFENSE CYBER STRATEGY 1 (2018).

[125] *Id.* at 2.

[126] See CYBERSPACE OPERATIONS, *supra* note 119, at IV-13–14, for organizational charts for both routine and crisis cyberspace command and control; *see id.* at IV-18–20, for further discussion about synchronizing cyber operations with conventional forces.

[127] Clive Walker & Ummi Hani Binti Masood, *Domestic Law Responses to Transnational Cyberattacks and Other Online Harms: Internet Dreams to Internet Nightmares and Back Again*, 10 NOTRE DAME J. INT'L COMPAR. L. 56, 63 (2020) ("In a sense, the operation of the network of networks that comprises the Internet is always transnational.").

a. Cybercrime

Although international cybercrime has been a problem since the 1980s and 90s,[128] there is "no UN legal instrument on cybercrime."[129] While cybercrime has not been addressed at the treaty level, there have been five United Nations ("U.N.") resolutions passed that relate to cybercrime but do not create any enforceable action.[130] However, the U.N. has passed a recent resolution for drafting a cybercrime treaty.[131] Despite the lack of international cybercrime laws, multi-national cooperation has been successful where cybercrime laws overlap.[132] Fortunately, one hundred and fifty-six countries have enacted some form of cybercrime legislation.[133] To further assist cooperation, there have been attempts to standardize international criminal codes regarding cybercrime, such as through the G8's "high-tech crimes and . . . mutual legal assistance" principles or the Budapest Convention on Cybercrime.[134] The Budapest Convention has been the most successful multilateral treaty on cybercrime, with sixty-six nations implementing standardized cybercrime laws into their domestic laws.[135] Nonetheless, prosecuting

---

[128] *See Major Cases*, FBI, https://www.fbi.gov/investigate/cyber/major-cases [https://perma.cc/9BUB-9HXT] (last visited Sept. 7, 2022) (noting, for example, that "[a] Russian's hacking of a U.S. bank in 1994 may have been the first online bank robbery").

[129] Summer Walker & Ian Tennant, *Time to Engage: The UN Wades into a Global Cybercrime Treaty Debate*, GLOB. INITIATIVE AGAINST TRANSNATIONAL ORGANIZED CRIME (May 7, 2021), https://globalinitiative.net/analysis/un-cybercrime-treaty-debate/ [https://perma.cc/3YSG-SDGQ].

[130] *See generally* G.A. Res. 55/63 (Jan. 22, 2001); G.A. Res. 56/121 (Jan. 23, 2021); G.A. Res. 57/239 (Jan. 31, 2003); G.A. Res. 58/199 (Jan. 20, 2004); G.A. Res. 64/211 (Mar. 17, 2010).

[131] G.A. Res. 75/282 (May 26, 2021).

[132] *See generally, e.g.*, Marco Gercke, *Regional and Internal Trends in Information Society Issues*, CYBERCRIME RSCH. INST. (Mar. 8–12, 2010), https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/events/2010/wg1/docs_wk1/Marco_Gercke_Regional_and_International_Trends_in_Information_Society_Issues_HIPCAR_WG-1_workshop01_20100308.pdf (noting the concept of "Dual Criminality" that allows for international cooperation either bilaterally or multilaterally depending on the legislation in common).

[133] *Cybercrime Legislation Worldwide*, UNITED NATIONS CONF. ON TRADE & DEV., https://unctad.org/page/cybercrime-legislation-worldwide [https://perma.cc/Z3YW-2244] (last visited Sept. 7, 2022).

[134] Communiqué, *Meeting of Justice and Interior Ministers of The Eight*, at 1–2, 6–7 (Dec. 10, 1997) (on file with author); *see generally* Council of Europe, *Convention on Cybercrime*, E.T.S. 185 (Nov, 23, 2001).

[135] Council of Europe, *Chart of Signatures and Ratifications of Treaty 185*, TREATY OFF. (Feb. 7, 2022), https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 [https://perma.cc/S3JB-93C8].

transnational cybercrimes still proves challenging because of disputes over extradition and jurisdiction, even among treaty members.[136]

b. Cyberwar

The international community provides more information regarding whether cyberattacks constitute acts of war because war involves more than one state or actor.[137] Furthermore, nations want to be justified in going to war and have developed the doctrine of *Jus Belli*—the law of war—for that specific purpose.[138] Three avenues inform nations on whether cyberattacks warrant a military response: international treaties, customary norms, and leading policy experts.[139]

The first source, international treaties, has a multitude of treaties on war,[140] but the Protocol II of the Geneva Convention,[141] the Hague Convention of 1907,[142] and U.N. Charter Article 39 provide specific provisions barring attacks on infrastructure.[143] Article 15 to Protocol II of the Geneva Convention states that "Works or installations containing dangerous forces, namely dams, dykes, and nuclear electrical

---

[136] *See* Jason P. Gonzalez et al., *Cases without Borders: The Challenge of International Cybercrime Investigations*, 30 CRIME & JUST. 15, 16 (2016) (noting some of the roadblocks to prosecuting international cybercrime, such as "dual criminality" and nations being unwilling to expose their citizens to another's legal system); Susan W. Brenner & Joseph J. IV Schwerha, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. MARSHALL J. COMPUTER & INFO. L. 347, 353 n.30 (2002).

[137] *See War*, BLACK'S LAW DICTIONARY (2d ed. 1910) (defining war as "[a] state of forcible contention; an armed contest between nations; a state of hostility between two or more nations or states").

[138] *Jus Belli*, BLACK'S LAW DICTIONARY (2d ed. 1910) (defining "*Jus Belli"* as "[t]he law of war" or "[t]he law of nations as applied to a state of war, defining in particular the rights and duties of the belligerent powers themselves, and of neutral nations" or "[t]he right of war; that which may be done without injustice with regard to an enemy").

[139] *See generally* HUGH THIRLWAY, THE SOURCES OF INTERNATIONAL LAW (2014).

[140] For a dynamic list of treaties see *List of Treaties*, WIKIPEDIA, https://en.wikipedia.org/wiki/List_of_treaties [https://perma.cc/YY4B-S5NE] (last visited Sept. 7, 2022).

[141] Protocol for the Protection of Works and Installations Containing Dangerous Forces, June 10, 1977, 1977 U.S.T. LEXIS 465, *28 [hereinafter Geneva Protocol II].

[142] Article 56 with regard to the property of municipalities. Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, Section III: Military Authority over the Territory of the Hostile State – Regulation, October 18, 1907, 1907 U.S.T. Lexis 29, *40 [Hereinafter Hague Convention of 1907].

[143] U.N. Charter art. 39.

generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces."[144] Article 56 to the Hague Convention of 1907 provides that "The property of municipalities . . . shall be treated as private property" and "[a]ll seizure of, destruction or willful damage . . . should be made the subject of legal proceedings."[145] Lastly, Article 39 of the U.N. Charter provides reports on acts constituting a threat to peace and international security and determines the state's right to self-defense.[146] For example, the U.N. recognized that the Houthi attacks against civilian infrastructure—the Saudi Aramco oil facilities—as a threat to Saudi Arabia's national security and as a threat to the global energy supply.[147] These treaties list violations of the "laws of war," and, if violated, justify a military response in self-defense under Article 51.[148]

The next source is customary law, which, according to the International Committee of the Red Cross ("ICRC"), "consists of rules that come from 'a general practice accepted as law' and exist independent of treaty law."[149] Given the lack of an international treaty regarding cyberwar or acts constituting cyberwarfare,[150] customary law is the primary source for understanding the international norms on acts of cyberwar.[151] The prevailing view on cyberattacks is that they constitute something less than an act of war.[152] The Tallinn Manual is the

---

[144] Geneva Protocol II, *supra* note 141, at *28 ("Article 15.–Protection of works and installations containing dangerous forces.").

[145] Hague Convention of 1907, *supra* note 142, at *40.

[146] U.N. Charter art. 39; U.N. Charter art. 51.

[147] Department of Political and Peacebuilding Affairs, Repertoire of the Practice of the Security Council: Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (2019) [hereinafter Security Council], https://www.un.org/securitycouncil/sites/www.un.org.securitycouncil/files/repertoire_22nd_supplement.pdf.

[148] *See generally* Laurie R. Blank, *Irreconcilable Differences: The Thresholds for Armed Attack and International Armed Conflict*, 96 NOTRE DAME L. REV. (2020); U.N. Charter art. 51.

[149] Customary law fills in the gaps that treaties on armed conflict do not cover. *Customary Law*, IRCR, https://www.icrc.org/en/war-and-law/treaties-customary-law/customary-law [https://perma.cc/72B5-NVV5] (last visited Sept. 7, 2022).

[150] Daniel Abebe, *Cyberwar, International Politics, and Institutional Design*, 83 U. CHI. L. REV. 1, 7 (2016).

[151] Kristen E. Eichensehr, *Cyberwar & International Law Step Zero*, 50 TEX. INT'L L.J. 357, 365–66 (2015) (noting that current international norms in both peacetime and wartime can be applied to cyberspace).

[152] Lawrence J. Trautman, *Is Cyberattack the Next Pearl Harbor*, 18 N.C. J.L. & TECH. 233, 254, 269 (2016).

leading guide on the rules of cyberwar and codifies the customary law of cyberwarfare.[153]

In its initial form, the Tallinn Manual recognizes obvious acts of cyberwar.[154] "The classic example is conducting cyber attacks . . . against military personnel or military objectives."[155] However, when it comes to non-state actors, the manual is less direct.[156] The manual does impose a quasi-respondeat superior doctrine, stating that "Under international law, States may be responsible for cyber operations that their organs conduct or that are otherwise attributable to them by virtue of the law of State responsibility."[157] However, such attribution is difficult.[158] Further, attribution implicates a nation.[159] To avoid implicating a nation, cyberwar is treated as hybrid warfare—below the threshold of declared war.[160] The Tallinn Manual outlines when a cyberattack equates to hybrid or traditional war.[161] The threshold is crossed, not when the actor plots or attacks, but rather by a determination of "the consequences of the operation and its surrounding circumstances."[162]

Finally, leading experts and organizations help interpret the existing law.[163] For example, the International Court of Justice

---

[153] *See generally* NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt, ed. 2017) [hereinafter Tallinn Manual 2.0].

[154] *See generally* NATO CCDCOE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt, ed. 2013) [hereinafter Tallinn Manual].

[155] TALLINN MANUAL 2.0, *supra* note 153, at 407.

[156] TALLINN MANUAL, *supra* note 154, at 17 (noting that cyber operations conducted by non-State actors may also violate State's sovereignty).

[157] *Id.* at 15.

[158] *See* William Banks, *Cyber Attribution and State Responsibility*, 97 INT'L L. STUD. 1039, 1046–48 (2021) (noting that hackers "complicate attributions by deliberately obscuring their identities or by staging their cyberattacks to appear as though they were caused by someone else" and "the inability to identify the source of a cyberattack potentially increases the risks of confusion and escalation").

[159] *See generally* G.A. Res. 56/83 (Jan. 28, 2002).

[160] *See* BRANTLY ET AL., *supra* note 93, at 8.

[161] *See* TALLINN MANUAL 2.0, *supra* note 153, at 329 ("A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful.").

[162] *Id.* at 328 ("In the cyber context, it is not the instrument used that determines whether the use of force threshold has been crossed, but rather, as described in Rule 69, the consequences of the operation and its surrounding circumstances."); *see also* U.N. Charter art. 2(4).

[163] *See* Frederick Pollock, *Sources of International Law*, 2 COLUM. L. REV. 511, 513 (1902) ("The answer given by the highest legal authorities . . . is that the

("ICJ") provided an interpretation of customary law in *U.S. v. Nicaragua*, ruling that the U.S. breached the "principle of the non-use of force" by arming the *contras* in Nicaragua, and that the U.S. was not justified in its actions under the collective self-defense provisions in Article 51.[164] Further, this case "recognize[d] a country's control over paramilitaries or other non-State actors" if the actors fully rely on the State.[165] Additionally, according to the International Criminal Tribunal for the Former Yugoslavia, nations bear responsibility if they provide support to a non-state actor or "ha[ve] sufficient overall control such that the group's acts are attributable to the State."[166]

In the cyberattack context, the experts in the North Atlantic Treaty Organization ("NATO") have advocated for an "overall control standard" as opposed to the "effect[ ] control standard."[167] The overall control standard was developed from the *Tadić* case, requiring that the state play a role in organizing, coordinating, or supporting the non-state actor, while the effective control standard, developed after the *Application of the Genocide Convention*, requires "smoking-gun" evidence.[168] Under the overall control standard, "it would be possible that Russian or Chinese incitement behind the cyber attacks on Estonia, Georgia, or the United States, if proven, would be sufficient to satisfy State attribution."[169]

Both U.S. and international law provide guidelines for determining whether a cyberattack is either an act of cybercrime or cyberwar. However, background on the victim and the attacker is necessary to answer the question.

---

opinions of experienced and approved publicists are valuable, not as mere opinions, but as evidence.").

[164] Military and Paramilitary Activities in and Against Nicaragua (Nicar. V. U.S.), Judgment, 1986 I.C.J. 118–20 ¶¶ 228–32 (June 27).

[165] Scott J. Shackleford, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, *in* CONFERENCE ON CYBER CONFLICT 198 (2010) (C. Czosseck & K. Podins eds., 2010).

[166] *Id.*; *see also* Prosecutor v. Tadić, Case No. IT-94-1-T, Opinion and Judgment, ¶¶ 117–22 (Int'l Crim. Trib. for the Former Yugoslavia May, 7, 1997) (discussing state attribution for the actions of non-state actors).

[167] Shackelford, *supra* note 165, at 204.

[168] *Id.* at 201. *See generally* Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. V. Serb./Montenegro), Judgment, 2007 I.C.J. 191 (Feb. 26).

[169] Shackelford, *supra* note 165, at 204.

B. Relevant Actors

1. Colonial Pipeline Company

> In 1961, a handful of energy companies came together to build what was then the single largest privately funded construction project in the history of the United States—a $370 million dollar pipeline that would deliver gasoline and other refined products from Houston, Texas to New York Harbor and points in-between.[170]

Today, the Colonial Pipeline Company is a privately-owned joint venture by five entities from different countries,[171] and is headquartered in Alpharetta, Georgia.[172] The 5,500-mile-long network of pipelines delivers fuel to "7 major airports, 90 military installations, and 270 delivery terminals across the South and East."[173] Colonial's four main pipelines transport 4.3 MMBbls per day of jet fuel, diesel, gasoline, and other products.[174] In 2020, "the company had operating revenue of $1.32 billion."[175] The pipeline has been described as a "superhighway for energy," [176] and the federal government classifies it as critical U.S. energy infrastructure.[177] The pipeline is so vital that it is used as a metric for fuel pricing on the New York Mercantile Exchange ("NYMEX").[178]

---

[170] Tim Felt, President and Chief Exec. Officer, Colonial Pipeline Co., Address at the Quadrennial Energy Review Stakeholder Meeting: Transmission, Storage and Distribution Issues Relation to Petroleum and Refined Products (May 27, 2014), https://www.energy.gov/sites/prod/files/2014/06/f16/tfelt_statement_qer_nola.pdf.

[171] Ownership of the pipeline is as follows: 28.1% to Koch Industries (USA), 23.4% to a joint venture between Kohlberg, Kravis Roberts & Co. (KKR) (USA) and South Korea's state-run National Pension Service (ROK), 16.6% to Caisse de dépôt du Québec (CAN), 16.6% to Royal Dutch Shell (NED), and 15.8% to IFM investors (ASTL). *See* Chris Isidore, *Who Owns the Colonial Pipeline? It's Complicated*, CNN BUS. (May 12, 2021, 1:02 PM), https://www.cnn.com/2021/05/12/investing/colonial-pipeline-ownership/index.html [https://perma.cc/WN4P-SH4V].

[172] Matt Kempner, *Things to Know about Atlanta's Colonial Pipeline, Hit by Ransomware*, ATLANTA J.-CONST. (May 10, 2021), https://www.ajc.com/news/heres-a-primer-on-atlantas-colonial-pipeline-hit-by-ransomware/TZ2U3EM6RBAQHEAMVO3UYUQHMI/ [https://perma.cc/NVG2-PKW8].

[173] Felt, *supra* note 170.

[174] Tim Fitzgibbon, *Energy Insights by McKinsey: Colonial Pipeline*, MCKINSEY & CO. (Dec. 2018), https://www.mckinseyenergyinsights.com/resources/refinery-reference-desk/colonial-pipeline/ [https://perma.cc/A5LC-VLYB]; Felt, *supra* note 170.

[175] Kempner, *supra* note 172.

[176] Felt, *supra* note 170.

[177] Affidavit, *supra* note 62, at 6.

[178] This is the price to deliver this product to "buyers at injection points across the Gulf coast," which is then "piped on to terminals throughout the eastern US."

The importance that the pipeline plays, not just in fuel delivery, but also in terms of its status of a financial index, has led Colonial to implement redundancy measures.[179] However, for this cyberattack, the company had not updated all of its security protocols, as the hackers utilized "a legacy [VPN]" with a "single-factor authentication"—a single password—to gain access.[180] Any cybersecurity regulations from the TSA were irrelevant because the processes were too new for the TSA to verify them.[181] Although Colonial shut down their pipeline, the action was a circumstance of the ransomware.[182] The outage not only stopped the flow of 2.5 MMBbls of fuel, but also changed the gasoline and diesel futures prices on the NYMEX by 0.6% and 1.1%, respectively.[183] Overall, the attack will end up "cost[ing] the company tens of millions of dollars."[184]

2. DarkSide

DarkSide is "the hacker group behind the [Colonial cyberattack]."[185] DarkSide is a "constellation of criminal

---

Pricing is then used as basis to compare with additional markets and locations. *See Oil Products: ARGUS US Gulf Colonial Pipeline 87 Conventional Gasoline Price Assessment*, ARGUS, https://www.argusmedia.com/en/methodology/key-prices/argus-colonial-pipeline-87-conventional-gasoline [https://perma.cc/NW4Y-DSR9] (last visited Sept. 7, 2022).

[179] Felt, *supra* note 170.

[180] Stephanie Kelly & Jessica Resnick-ault, *One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators*, REUTERS (Jun. 8, 2021, 8:06 PM), https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/ [https://perma.cc/5CGJ-K26E].

[181] U.S. GOVERNMENT OF ACCOUNTABILITY OFFICE [GAO], CRITICAL INFRASTRUCTURE PROTECTION: ACTIONS NEEDED TO ADDRESS SIGNIFICANT WEAKNESSES IN TSA'S PIPELINE SECURITY PROGRAM MANAGEMENT (2018), https://www.gao.gov/products/gao-19-48 [https://perma.cc/F3DW-4HQU]. Despite efforts to coordinate a government-run cybersecurity assessment, the TSA and Colonial never did one, and it is unclear if it would have helped given Colonial's employment of four cybersecurity firms. These assessments called "validated architecture design review" or "VADR" only started in December of 2018. Ellen Nakashima, Lori Aratani, & Douglas MacMillan, *Colonial Hack Exposed Government's Light-Touch Oversight of Pipeline Cybersecurity*, WASH. POST (May 30, 2021, 7:00 AM), https://www.washingtonpost.com/business/2021/05/30/colonial-pipeline-tsa-regulation/ [https://perma.cc/5U4W-2Y9R].

[182] Sara Morrison, *How a Major Oil Pipeline Got Held for Ransom*, VOX (Jun. 8, 2021, 12:50 PM), https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices [https://perma.cc/HZT9-PZKK].

[183] Bing & Kelly, *supra* note 4.

[184] *Colonial Pipeline Boss Confirms $4.4m Ransom Payment*, BBC (May 19, 2021), https://www.bbc.com/news/business-57178503 [https://perma.cc/7P72-AUGK].

[185] Emily DeCiccio, *Hacker Group DarkSide Operates in a Similar Way to a Franchise, New York Times Reporter Says*, CNBC (June 2, 2021, 7:19 PM),

actors . . . emanat[ing] from Russia and its former Soviet states, as well as North Korea, China, Syria, and Iran."[186] According to cybersecurity expert Brian Krebs, "DarkSide, like a great many other malware strains, has a hard-coded do-not-install list of countries which are . . . former Soviet satellites that mostly have favorable relations with the Kremlin."[187] "[S]ince August 2020, [DarkSide] has used ransomware cyberattacks to hack various companies in the U.S. and Europe."[188] "They have attempted to extort companies with threats, for instance, of leaking personal data."[189] Further, DarkSide utilizes a "double extortion" tactic, "where the hackers not only encrypt and lock the user's data, but also threaten to make it public if the ransom is not paid."[190] DarkSide is a sophisticated syndicate that even provides "web chat support to victims, build[s] intricate data leak storage systems with redundancy, and perform[s] financial analysis of victims prior to attacking."[191]

Despite specific geographical targets, DarkSide's motives appear to be financial.[192] In fact, DarkSide employs a "ransomware-as-a-service" business model, "in which hackers develop and sell their ransomware attack tools to those wishing to carry out an attack."[193] It is described as "something like a franchise, where individual hackers can come and receive the ransomware software and use it, as well as, use DarkSide's reputation."[194] DarkSide, despite being a criminal enterprise, even has "a code of ethics and states the hackers will never attack hospitals, schools, universities, non-profit organizations, and government agencies."[195]

---

https://www.cnbc.com/2021/06/02/hacker-group-darksides-operates-in-a-similar-way-to-a-franchise-new-york-times-reporter-says.html [https://perma.cc/7W4T-P8WS].

[186] Carmack, *supra* note 1.

[187] *Id.*

[188] Ewan Palmer, *What is DarkSide? Russia-Linked Hacker Group Behind Colonial Pipeline Shutdown*, NEWSWEEK (May 11, 2021, 6:22 AM), https://www.newsweek.com/darkside-hacker-group-russia-colonial-pipeline-1590352 [https://perma.cc/M7QB-TQN7].

[189] *Id.*

[190] *Id.* They sometimes donate the ransom to charities. *Id.*

[191] Snir Ben Shimol, *Return of the Darkside: Analysis of a Large-Scale Date Theft Campaign*, VARONIS (July 6, 2021), https://www.varonis.com/blog/darkside-ransomware/ [https://perma.cc/EMV7-A864].

[192] *See* Palmer, *supra* note 188.

[193] *Id.*

[194] DeCiccio, *supra* note 185.

[195] Palmer, *supra* note 188.

DarkSide's motives behind the Colonial cyberattack and any potential state affiliation remain unclear.[196] Its motive is unclear because, despite DarkSide's apolitical press releases,[197] anyone can attack using DarkSide's software or reputation.[198] Regardless, because DarkSide offers about 10% to 25% in profits from the crimes of its affiliates, it can be viewed as complicit.[199] President Vladimir Putin is known to provide a "safe harbor for these cyber criminals to operate in Russia,"[200] and President Biden has indicated that, although there was "no evidence" that the Russian government was behind the attack, "there is evidence that the actors' ransomware is in Russia."[201]

DarkSide quickly distanced itself from the affiliate that attacked Colonial because the cyberattack went beyond their normal scope of attacks.[202] DarkSide implemented quality control measures to "avoid social consequences in the future."[203] The Colonial cyberattack was such an unacceptable crime that DarkSide surprisingly terminated the affiliate program "[d]ue to pressure from the U.S."[204] However, the U.S. denied disrupting DarkSide's network, which was the catalyst for DarkSide's decision.[205] Despite shutting its proverbial cyber-doors, DarkSide may have reemerged under a new name, "BlackMatter."[206]

---

[196] *See* DeCiccio, *supra* note 185.

[197] Mary-Ann Russon, *US Fuel Pipeline Hackers 'Didn't Mean to Create Problems'*, BBC NEWS (May 10, 2021), https://www.bbc.com/news/business-57050690 [https://perma.cc/5C6J-H49G]. DarkSide said, "We do not participate in geopolitics, do not need to tie us with a defined government and look for . . . our motives." *Id.* "Our goal is to make money and not creating problems for society." *Id.*

[198] DeCiccio, *supra* note 185.

[199] *See* Shimol, *supra* note 191.

[200] Carmack, *supra* note 1.

[201] Palmer, *supra* note 188.

[202] *See* Russon, *supra* note 197.

[203] *Id.*

[204] Michael Schwirtz & Nicole Perlroth, *DarkSide, Blamed for Gas Pipeline Attack, Says It is Shutting Down*, N.Y. TIMES (June 8, 2021), https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html [https://perma.cc/HZ2L-AR4U].

[205] Ellen Nakashima, *U.S. Government Denies Disrupting Russian Ransomware Ring that Hacked Colonial Pipeline*, WASH. POST (May 19, 2021, 4:59 PM), https://www.washingtonpost.com/business/2021/05/19/darkside-hack-colonial-cyber-command/ [https://perma.cc/77PU-EXMB].

[206] David Uberti & Catherine Stupp, *New Hacking Group Shows Similarities to Gang That Attacked Colonial Pipeline*, WALL ST. J. (Aug. 5, 2021, 5:30 AM), https://www.wsj.com/articles/new-hacking-group-shows-similarities-to-gang-that-attacked-colonial-pipeline-11628155802 [https://perma.cc/J6KB-2G3X].

II. ANALYSIS OF THE COLONIAL PIPELINE CYBERATTACK AS AN ACT OF CYBERWAR

A. Colonial Cyberattack is Cyberwar

The framework that emerges from domestic and international law is that a cyberattack constitutes an act of cyberwar when (1) a foreign actor (2) attacks critical infrastructure (3) causing significant damage which (4) experts and (5) precedents agree (6) warrant an inherent right to self-defense.[207] Further, that actor may be attributable to a nation under the overall control standard.[208] Applying this framework, the ransomware was an act of cyberwar and the attack may be attributable to the Russian Federation because of the attack's origin.

First, DarkSide is a foreign actor, and the President confirmed the ransomware's Russian origin.[209] Second, the pipeline is part of critical U.S. energy infrastructure.[210] Third, this attack left widespread economic damage triggered by the shutdown.[211] The outage created fuel shortages,[212] manipulated financial markets,[213] and created "tens of millions" in damage.[214] Any argument that the damage was self-inflicted ignores that the shutdown was a consequence of the ransomware.[215]

Next, the Colonial cyberattack was the type of attack which experts agree warrants a military response. The President,[216] members of Congress,[217] and cybersecurity experts have stated that a cyberattack on critical infrastructure would be an act of war.[218] The Senate Armed Forces Committee hearing stated that cyberattacks on critical infrastructure should be analyzed as acts of war.[219] Finally, the Tallinn Manual states that cyberattacks on privately-owned infrastructure could "violate a State's

---

[207] This is a summary from *supra* Part I.

[208] *See supra* Section I.B.2.

[209] Carmack, *supra* note 1; Palmer, *supra* note 188.

[210] *Energy Sector*, CISA, https://www.cisa.gov/energy-sector [https://perma.cc/3KZT-SZRG] (last visited Sept. 7, 2022); Affidavit, *supra* note 62.

[211] Bing & Kelly, *supra* note 4.

[212] *Id*.

[213] *Id.*

[214] BBC, *supra* note 184.

[215] Morrison, *supra* note 182; Tallinn Manual 2.0, *supra* note 153.

[216] Bose, *supra* note 108.

[217] Williams & Bennett, *supra* note 111.

[218] *Id.*

[219] *Cybersecurity Hearing*, *supra* note 112.

sovereignty."[220] Therefore, the Colonial cyberattack aligns with expert opinion because the attack targeted privately-owned critical infrastructure.[221]

In addition, historical U.S. precedent supports a military response. The U.S. responded with military force to attacks on commercial enterprises during the Barbary Wars.[222] A military response to the Colonial cyberattack would be similar because Colonial is a commercial enterprise.[223] In addition, the U.S. has and continues to use military force against non-state actors following 9/11.[224] Because DarkSide is a non-state actor, a military response is comparable to a U.S. drone strike against potential terrorists.[225]

Finally, the Colonial cyberattack triggers an inherent right to self-defense because of several violations of the "law of war."[226] The attack breached Article 15 of Protocol II because it caused an outage of critical infrastructure.[227] The attack also constitutes a violation of Article 56's protection of private property under the Hague Convention because it targeted a privately-owned pipeline.[228] In addition, the U.N. has recognized rebel attacks against pipelines as national security threats under Article 39 and recognized Saudi Arabia's right to self-defense under Article 51 because the attack threatened energy markets.[229] Therefore, the Colonial cyberattack should warrant the same right of self-defense for the U.S. because the attack threatened energy markets and supplies.[230]

Further, DarkSide can be attributed to the Russian Federation because, similar to *Nicar. v. U.S.*, or the *Tadić* case, Russia satisfies the overall control standard by providing a "safe harbor" for hackers.[231] However, nations prefer to avoid all-out war and will, therefore, avoid attribution, opting for hybrid

---

[220] Tallinn Manual 2.0, *supra* note 153, at 18.

[221] Isidore, *supra* note 171.

[222] *See* Act for the Protection of Commerce and Seamen of the United States, Against the Tripolitan Cruisers, ch. 4, 2 Stat. 129 (1802).

[223] Isidore, *supra* note 171.

[224] *See* Bradley & Goldsmith, *supra* note 92.

[225] *See id.*; Carmack, *supra* note 1.

[226] *See* Blank, *supra* note 148, at 257–58.

[227] See Geneva Convention Protocol II, *supra* note 141, at *28.

[228] See Hague Convention of 1907, *supra* note 142, at *40.

[229] *See* Security Council, *supra* note 147; U.N. Charter art. 39; U.N. Charter art. 51.

[230] Bing & Kelly, *supra* note 4.

[231] *See* Carmack, *supra* note 1; *supra* pp. 508–09.

warfare instead.[232] Nonetheless, the Colonial cyberattack satisfies the six-factor threshold to constitute an act of cyberwar. Therefore, the U.S. may respond with military force.[233]

B. Outlining a Military Response

USCYBERCOM is authorized to retaliate through the statutory scheme and series of policy directives that enable USCYBERCOM to intervene under 10 U.S.C. § 394.[234] When the Colonial cyberattack occurred, DC3 would have received information about the attack from CISA per their voluntary sharing initiative.[235] Then, the SecDef could have authorized military force to respond to the attack with Presidential approval.[236] Alternatively, PPD-20 would have permitted the SecDef to authorize emergency cyber operations without briefing the President.[237] Either decision to use force would not have required congressional approval because the War Powers Resolution permits use of force for attacks creating a "national emergency."[238] National emergencies are not unprecedented for cyberattacks,[239] and, for this crisis, North Carolina declared a state of emergency.[240] Once issued, USCYBERCOM would have developed a military response to retaliate against DarkSide.[241] Then, USCYBERCOM would conduct a proportionate cyber military response to disable DarkSide.[242] Alternatively, USCYBERCOM could coordinate with other commands to

---

[232] For an example of how hybrid warfare has reduced Russia's need for military intervention in Ukraine see BRANTLY ET AL., *supra* note 93, at 39.

[233] *See* U.N. Charter art. 51.

[234] 10 U.S.C. § 394.

[235] *See* JOINT PUBLICATION 3–12, *supra* note 119, at I-13–I-14; SHARING OF CYBER, *supra* note 60.

[236] 10 U.S.C. § 394.

[237] PPD-20, *supra* note 14.

[238] 50 U.S.C. § 1541(c).

[239] *See* Cory Bennett, *Obama Declares Cyberattacks a 'National Emergency,'* HILL (Apr. 1, 2015, 9:13 AM), https://thehill.com/policy/cybersecurity/237581-obama-declares-cyberattacks-a-national-emergency [https://perma.cc/2XMX-XPLT]; Davey Winder, *Trump Declares National Emergency as Foreign Hackers Threaten U.S. Power Grid*, FORBES (May 2, 2020, 4:24 AM), https://www.forbes.com/sites/daveywinder/2020/05/02/trump-declares-national-emergency-as-foreign-hackers-threaten-us-power-grid/?sh=f3f66133497f [https://perma.cc/W4PW-UJYG].

[240] *State of Emergency Declared in NC to Help Prevent Fuel Shortage Following Colonial Pipeline Hack*, ABC NEWS (May 11, 2021), https://abc11.com/colonial-pipeline-gas-prices-shortage-hack/10607059/ [https://perma.cc/FQY3-BMZ3].

[241] JOINT PUBLICATION 3–12, *supra* note 119, at IV-13–IV14, IV-18–IV-20.

[242] *Id.* at IV-13–IV-14, IV-18, IV-21.

conduct conventional military strikes against DarkSide's personnel or equipment.[243]

CONCLUSION

The Colonial cyberattack constituted an act of cyberwar because it crossed the six-factor threshold developed from domestic and international "laws of war." Therefore, the U.S. has the inherent right to a military response in self-defense. In addition, the hybrid warfare aspect means that the U.S. has a choice. The U.S. can prosecute ransomware attacks as cybercrimes, if justice can be reasonably adjudicated, or strike with military force. Nevertheless, the U.S. must be vigilant to maintain this delineation between criminal acts and acts of war in cyberspace to avoid endless military intervention. With the President's warning of an imminent Russian cyberattack against the U.S.,[244] NATO recognizing cyberattacks as an Article 5 trigger,[245] and the recent Iranian cyberattack on Albania's critical infrastructure,[246] the delineation between cybercrime and cyberwar is more critical than ever.

---

[243] *Id.*

[244] Statements and Releases, White House, Statement by President Biden on our Nation's Cybersecurity (Mar. 21, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/ [https://perma.cc/G2DX-EWN8].

[245] *NATO Will Defend Itself*, NATO (Aug. 29, 2019, 16:38), https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en [https://perma.cc/NSV8-EMHR] (noting NATO Secretary General Jens Stoltenberg's statement that "a serious cyberattack could trigger Article 5").

[246] Edmund Blair, Alex Richardson, & William Maclean, *Albania Cuts Iran Ties over Cyberattack, U.S. Vows Further Action*, REUTERS (Sept. 7, 2022, 2:46 PM), https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-attack-pm-says-2022-09-07/ [https://perma.cc/TE4B-U77D].