SURGING TOWARDS RANSOMWARE: DOES THE DEPARTMENT OF DEFENSE HAVE THE LEGAL AUTHORITY TO LEVERAGE CRYPTOCURRENCY AND COMBAT CYBER THREATS?

*Mari Dugas**

After the Colonial Pipeline attack in May 2021, ransomware based cyberattacks against America's critical infrastructure suddenly affected Americans' everyday lives and became a topic outside of cybersecurity circles.

While Colonial Pipeline seemed like a turning point in the proliferation of ransomware, ransomware is not a new phenomenon. It is a growing threat to national security. There are thorny legal questions about a novel use of technology to counter adversaries in cyberspace, particularly outside of the context of active military hostilities.

This paper explores whether one federal entity in particular, the Department of Defense (DOD) has legal authority to combat the threat of ransomware. Mieke Eoyang, Deputy Assistant Secretary of Defense (DASD) for Cyber Policy, confirmed in congressional testimony that DOD "currently works to counter the ransomware threat as part of [its] mission to defend the Nation in cyberspace," but DOD is generally limited in any action it takes by provisions of international law that the U.S. follows, domestic law, and its own internal policies.

This paper discusses the Constitution and domestic U.S. law that may place restrictions on DOD's ability to target ransomware actors and the international legal limits on potential DOD actions against ransomware actors. I ultimately conclude that DOD's ability to target ransomware actors exists in a legal grey area that would benefit from explicit congressional authorizations to the executive branch.

* J.D. 2022, New York University School of Law. The views presented in this paper reflect the author's alone and do not represent the views or policies of the Department of Defense or the U.S. Government.

Introduction

On May 19, 2021, Colonial Pipeline announced that it had paid $4.4 million to cyber attackers as it grappled with responding to one of the most prominent ransomware attacks on a private company in the United States.[1] The Colonial Pipeline attack quickly caused national ripple effects, most vividly in the form of gas shortages across the Eastern Seaboard and Southeast.[2] Ransomware based cyberattacks against America's critical infrastructure suddenly affected Americans' everyday lives and became a topic outside of cybersecurity circles. While the Colonial Pipeline attack seemed like a turning point in the proliferation of ransomware, ransomware is not a new phenomenon. It is a growing threat to national security.

The Biden Administration has acknowledged the need for a more robust government response to rising ransomware attacks against critical infrastructure (CI).[3] President Biden issued a broad executive order

1. Collin Eaton & Dustin Volz, *Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*, Wall St. J. (May 19, 2021), https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636 [https://perma.cc/3X6E-684H]. Ransomware is defined by the Department of Homeland Security as "a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption." *Stop Ransomware*, CISA, https://www.cisa.gov/stopransomware [https://perma.cc/P9A8-DR7U].

2. Vanessa Romo, *Panic Drives Gas Shortages After Colonial Pipeline Ransomware Attack*, NPR (May 11, 2021), https://www.npr.org/2021/05/11/996044288/panic-drives-gas-shortages-after-colonial-pipeline-ransomware-attack [https://perma.cc/VT7R-HGJV].

3. *See, e.g.*, *Fact Sheet: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure*, White House (Jul. 28, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/ [https://perma.cc/H8ST-7N64]; *Evolving the U.S. Approach to Cybersecurity: Raising the Bar Today to Meet the Threats on Homeland Security: Hearing Before the H. Comm.*

directing federal agencies and contractors to improve their cybersecurity and defensive measures to shore up cyber defenses against ransomware.[4] Federal agencies have heeded the call. The Justice Department stood up a ransomware task force at the direction of Deputy Attorney General Lisa O. Monaco, which offered prosecutorial guidance to U.S. attorneys who bring cases against ransomware actors.[5] The Treasury Department sanctioned a Russian cryptocurrency exchange, accusing it of facilitating criminal ransomware payments, and updated guidance on ransomware payments.[6] The State Department convened a "counter-ransomware initiative" in October 2021, with thirty allied countries, to discuss "cryptocurrency, resilience, disruption, and diplomacy."[7] The meeting likely signals the administration's commitment to tackling the ransomware problem and its acknowledgement that not only must the whole of the U.S. government be committed to combatting the threat posed by ransomware, but so too must our allies and partners. The collective response by the federal government highlights both a recognition of the seriousness of the issue and a willingness to impose costs on ransomware actors who would threaten U.S. security and interests.

One federal player in particular will be the focus of this analysis: the Department of Defense (DOD). DOD is tasked with "provid[ing] the military forces needed to deter war and ensure our nation's security."[8] U.S. Cyber Command (CYBERCOM) is the combatant com-

---

On Homeland Security, 117th Cong. 15 (2021) (statement of Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency) ("ransomware has become a scourge on nearly every facet of our lives, and it's a prime example of the vulnerabilities that are emerging as our digital and our physical infrastructure increasingly converge. Earlier this year, we saw the Colonial Pipeline attack shutter gas stations along the East Coast and the JBS attack cause certain food prices to rise. We have also seen ransomware attacks on schools, police departments, hospitals, and small businesses around the country, and they are growing in number, scale, and sophistication.").

4. Exec. Order No. 14,028, 3 C.F.R. 556 (2022).

5. Memorandum from Lisa O. Monaco, Deputy Att'y Gen., U.S. Dep't of Justice, to All Federal Prosecutors (Jun. 3, 2021), https://www.justice.gov/opa/press-release/file/1402001/download [https://perma.cc/4BWS-9AMB].

6. Press Release, Dep't of Treasury, Treasury Continues to Counter Ransomware as Part of Whole-of-Government; Sanctions Ransomware Operators and Virtual Currency Exchange (Nov. 8, 2021), https://home.treasury.gov/news/press-releases/jy0471 [https://perma.cc/TMM2-N92R].

7. David E. Sanger, *U.S. Holds Global Meeting to Fight Ransomware, Minus the World's No. 1 Culprit*, N.Y. Times (Oct. 14, 2021), https://www.nytimes.com/2021/10/14/us/politics/global-ransomware-meeting.html. Notably, Russia was excluded from the global summit in the face of allegations that it is a significant source of cybercrime.

8. *About*, U.S. Dep't of Defense, https://www.defense.gov/About (last visited Dec. 10, 2021) [https://perma.cc/69D5-QK3H].

mand tasked with executing the DOD's mission in cyberspace and thought to be one of the entities operating against ransomware actors in cyberspace.[9] General Paul Nakasone, the four-star commander of CYBERCOM and Director of the National Security Agency, publicly acknowledged the ransomware problem not long after President Biden's made it an imperative for the federal government.

> Even six months ago, we probably would have said, 'Ransomware, that's criminal activity . . . But if it has an impact on a nation, like we've seen, then it becomes a national security issue. If it's a national security issue, then certainly [DOD and CYBERCOM] are going to surge towards it.[10]

Mieke Eoyang, Deputy Assistant Secretary of Defense (DASD) for Cyber Policy, also confirmed in her congressional testimony that DOD "currently works to counter the ransomware threat as part of [its] mission to defend the Nation in cyberspace."[11]

---

9. *See, e.g.*, Ellen Nakashima & Dalton Bennett, *A Ransomware Gang Shut Down After Cybercom Hijacked Its Site and It Discovered It Had Been Hacked*, WASH. POST (Nov. 3, 2021) https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html [https://perma.cc/H75R-XRY7]; Julian E. Barnes, *U.S. Military Has Acted Against Ransomware Groups, General Acknowledges*, N.Y. TIMES (Dec. 5, 2021), https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html; Sean Lyngaas, *US Military's Hacking Unit Publicly Acknowledges Taking Offensive Action to Disrupt Ransomware Operations*, CNN (Dec. 5, 2021), https://www.cnn.com/2021/12/05/politics/us-cyber-command-disrupt-ransomware-operations/index.html [https://perma.cc/YB3L-HWY4].

10. Nomaan Merchant, *General Promises US 'Surge' Against Foreign Cyberattacks*, AP (Sept. 14, 2021), https://apnews.com/c4c8dace4708035d059be0fcd10e9e18 [https://perma.cc/6B82-NL4X].

11. *Hearing to Receive Testimony on Recent Ransomware Attacks before the S. Subcomm. On Cybersecurity of the S. Comm. On Armed Services*, 117th Cong. (2021) (testimony by Mieke Eoyang, Deputy Assistant Secretary of Defense for Cyber Policy; Kevin Kennedy, Director of Operations, United States Cyber Command; Ronald Foy, Deputy Director for Global Operations, United States Joint Staff). Some commentators have noted the downsides of DOD engagement against ransomware actors, however. *See, e.g.*, Gavin Wilde, *On Ransomware, Cyber Command Should Take a Backseat*, JUST SECURITY (Nov. 30, 2021), https://www.justsecurity.org/79361/on-ransomware-cyber-command-should-take-a-backseat/ [https://perma.cc/T2TE-CGD5] ("If the DOD's Cyber Command is made the operational, budgetary, and political centerpiece of a counter-ransomware strategy, we risk doubling down on the sclerotic pace of U.S. investment in other areas, including those most at risk from cybercrime."); Jason Healy, *When Should U.S. Cyber Command Take Down Criminal Botnets?*, LAWFARE (Apr. 26, 2021), https://www.lawfareblog.com/when-should-us-cyber-command-take-down-criminal-botnets [https://perma.cc/S83Y-889W] ("Cyber Command's operation was not part of an ongoing conflict or war (where U.S. citizens expect their uniformed military services—the specialists in legitimate, large-scale violence—to take the lead) but was in response to criminal activity. . .It is simply not in the model of U.S. civil-military relations to allow the military to have such far-reaching powers, especially when there isn't a raging military conflict.").

There are a number of ways DOD could counter ransomware actors and impose hefty costs to deter future attacks. The White House has alluded to potential options, stating that "US Cyber Command and National Security Agency [have] dedicat[ed] people, technology, and expertise . . . [that] enable and support whole of government efforts, including actions against criminals, their *infrastructure*, and *their ability to profit from their crimes*."[12] The *Washington Post* has speculated that such actions could include damaging command and control infrastructure used by criminals to launch ransomware attacks.[13] In November 2021, reporting alleged that CYBERCOM, the Federal Bureau of Investigation (FBI), the Secret Service, and other multinational partners were involved in an operation to take the notorious Russian cybergang REvil offline.[14] While Nakasone or his counterparts did not comment on the REvil takedown allegations directly, he publicly stated a few days later that the Command "has made a lot of progress" tackling the ransomware threat and has a lot more to do in the future.[15]

Federal authorities could also impose costs by denying ransomware actors profits from their sprees since ransomware is fundamentally a money-making scheme. In the wake of the Colonial Pipeline attack, public reports surfaced that DOJ and FBI had returned the ransom paid by Colonial Pipeline.[16] According to the *Washington*

12. *Fact Sheet: Ongoing Public U.S. Efforts to Counter Ransomware*, WHITE HOUSE (Oct. 13, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/ [https://perma.cc/7G8U-J8D4] (emphasis added).

13. Nakashima & Bennett, *supra* note 9.

14. Joseph Menn & Christopher Bing, *Exclusive: Governments Turn Tables on Ransomware Gang REvil by Pushing It Offline*, REUTERS (Oct. 21, 2021), https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/ [https://perma.cc/6FQY-XRNP]. REvil has been identified by components of the U.S. Government as a significant ransomware actor. Members of REvil were indicted by the U.S. Department of Justice (DOJ) for hacking Kaseya, "a multi-national information technology software company." In 2021, DOJ seized $6.1 million traceable to ransomware payments from a Russian national, "charged with conducting Sodinokibi/REvil ransomware attacks against multiple victims, including businesses and government entities." *Ukrainian Arrested and Charged with Ransomware Attack on Kaseya*, DEP'T JUST. OFF. PUBLIC AFF. (Nov. 8, 2021), https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya [https://perma.cc/BRL8-Q395].

15. Katie Bo Lillis & Sean Lyngaas, *Cyber Command Head Says US Has Carried Out A 'Surge' Against Ransomware*, CNN (Nov. 3, 2021), https://www.cnn.com/2021/11/03/politics/nakasone-ransomware-surge/index.html [https://perma.cc/59LR-WACU].

16. Ellen Nakashima, *Feds Recover More than $2 Million in Ransomware Payments from Colonial Pipeline Hackers*, WASH. POST (June 7, 2021), https://www.washingtonpost.com/business/2021/06/07/colonial-pipeline-ransomware-payment-recovered/.

Post, the FBI reportedly gained access to the criminals' cryptocurrency wallet and seized the funds, which allowed the government to essentially pay Colonial Pipeline back what it had paid the ransomware actors.[17]

There are thorny legal questions about a novel use of technology to counter adversaries in cyberspace, particularly outside of the context of active military hostilities. This paper explores whether DOD has broad authority to leverage, whether by seizure, denial, or destruction, cryptocurrency of a ransomware actor. DOD is limited in its actions by provisions of international law that the U.S. follows, domestic law, and its own internal policies. This paper will not interrogate the policy benefits to undertaking such actions or make a normative judgement on what role DOD has in countering ransomware, vis-à-vis other elements of the U.S. Government.

Part II of the paper introduces the basics of cryptocurrency and ransomware to better understand why ransomware actors may pose a national security threat. Part III discusses the Constitution and domestic U.S. law that place restrictions on DOD's ability to target ransomware actors. Part IV lays out international legal limits on potential DOD actions against ransomware actors. In Part V, I conclude that DOD's ability to target ransomware actors exists in a legally grey area that would benefit from explicit congressional authorizations to the executive branch.

PART I: CRYPTOCURRENCY AND RANSOMWARE ACTORS

A. *Cryptocurrency is the Basis of Ransomware Attacks*

Ransomware attacks have been on the rise worldwide and are a money-making machine for malicious cyber actors. An analysis by Emsisoft Malware Lab estimates that ransomware has cost "hundreds of billions of dollars of economic damage in 2020," and that companies paid at least $18 billion cumulatively in ransom.[18] Some of the most recent high profile ransomware victims in the U.S. include Colonial Pipeline, JBS (one of the largest distributors of meat in the country), hospitals, schools, and local government offices.[19]

17. *Id*.

18. *The Cost of Ransomware in 2021: A Country-by-Country Analysis,* EMISOFT MALWARE LAB (Apr. 27, 2021), https://blog.emsisoft.com/en/38426/the-cost-of-ransomware-in-2021-a-country-by-country-analysis/.

19. Indeed, one of the critical infrastructure ransomware attacks of 2019, an attack on an Alabama hospital, has spurred the first wrongful death suit from a ransomware attack. An Alabama mother is suing the hospital for the wrongful death of her baby,

At its core, ransomware is profitable because actors can evade detection by transacting in cryptocurrency, which offers a layer of identity protection. Bitcoin is the most ubiquitous cryptocurrency (created by the elusive Satoshi Nakamoto)[20]—and sometimes used interchangeably with the term cryptocurrency itself—though it is just one type of cryptocurrency.[21] The technical concept behind Bitcoin and the blockchain is a series of algorithms forming the basis of "time stamped transactions that are unanimously verified by a distributed network of validators. . . ."[22] In lay terms, Nakamoto created Bitcoin to facilitate peer-validated transactions that maintain privacy and enable trust directly between the sender and the receiver, creating an alternative payment system outside of financial traditional institutions.[23] The blockchain is based on encryption; you hold one key (accessed and controlled by your master "seed phrase"), and the receiver of a transaction has the other key needed to unlock the funds.[24] Without both keys, the transaction cannot be completed.[25]

While cryptocurrencies are not fully anonymous and untraceable because blockchain transactions occur on a public ledger, they do of-

---

who she alleges died because a ransomware attack took the mechanized monitoring capabilities offline. If the suit is successful, this would be the first confirmed death resulting from a ransomware attack. Kevin Poulsen et al., *A Hospital Hack, a Baby in Distress—Lawsuit Alleges First Death from Ransomware*, WALL ST. J. (Oct. 1, 2021), https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116 [https://perma.cc/V2YM-FPQF].

20. SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM (2008) The concept of Bitcoin was published under the name Satoshi Nakamoto, although the author's (or authors') true identity remains unknown. Nakamoto is speculated to own over 1 million Bitcoins, which would be worth about $55 billion as of 2021. Paul Vigna, *Who Is Bitcoin Creator Satoshi Nakamoto? What We Know—and Don't Know*, WALL ST. J. (Dec. 7, 2021), https://www.wsj.com/articles/who-is-bitcoin-creator-satoshi-nakamoto-what-we-knowand-dont-know-11638020231 [https://perma.cc/D935-RPKW].

21. As of January 2022, Bitcoin is still the most popular cryptocurrency. Other popular cryptocurrencies include Ethereum, Binance Coin, and Tether. Kat Tretina & John Schmidt, *Top 10 Cryptocurrencies in January 2022*, FORBES (Jan. 3, 2022), https://www.forbes.com/advisor/investing/top-10-cryptocurrencies/ [https://perma.cc/SP5S-U89A].

22. Ollie Leech, *What is the Bitcoin White Paper*, COINDESK (June 16, 2021), https://www.coindesk.com/what-is-the-bitcoin-white-paper/ [https://perma.cc/2XK4-SUJE].

23. Nakamoto at 6, *supra* note 20.

24. *What is a Recovery Phrase?*, COINBASE, https://www.coinbase.com/learn/crypto-basics/what-is-a-seed-phrase (Coinbase refers to a seed phrase as a recovery phrase).

25. Benedict George, *A Crypto Must-Know: Public vs. Private Keys,* COINDESK (Aug. 5, 2022), https://www.coindesk.com/learn/a-crypto-must-know-public-vs-private-keys/.

fer a layer of removal from personally identifiable information.[26] Someone looking in from the outside may be able to see the value of your transactions, but not your name, where you live, or other personal information.[27] Conversely, your bank statements or credit card bills link transactions directly to you. Cryptocurrency transactions are therefore more accurately pseudonymous.[28] Your name will not appear on the blockchain, but your cryptocurrency wallet address will. With the right intelligence and knowledge of the wallet's seed phrase (your passcode to access funds in your wallet), law enforcement or other authorities can trace transactions to specific ransomware events.[29] Obtaining the private key, the seed phrase, could happen through law enforcement implanting a spyware tool that captures

26.) *Protect Your Privacy*, BITCOIN, https://bitcoin.org/en/protect-your-privacy (last visited Sept. 12, 2022). ("All Bitcoin transactions are public, traceable, and permanently stored in the Bitcoin network. Bitcoin addresses are the only information used to define where bitcoins are allocated and where they are sent.").

27. Cyber RAR Podcast, *Crypto & Lowrise Jeans: Cybersecurity on the Blockchain, Interview with Corinna Fehst*, at 10:30 (Sept. 7, 2022), https://cyberrar.simplecast.com/episodes/crypto-lowrise-jeans-cybersecurity-on-the-blockchain-Y2SbfzCy/transcript. ("On public blockchains. I mean, you, you have pseudonymized identities, right? You have your wallet addresses. And then the blockchain allows basically in the vast majority of cases, anyone to see which wallets are interacting with one another . . . .").

28. Ezra Galston, *Untraceable Bitcoin is a Myth*, WALL ST. J. (June 16, 2021), https://www.wsj.com/articles/untraceable-bitcoin-is-a-myth-11623860828. *See also* Dean Korsak & Erik Fuqua, *Decrypting Bitcoin and Blockchain for Military Lawyers*, JAG REP. (Sept. 23, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3931436 at 3.

29. *See, e.g.*, Nicole Perloth et al., *Pipeline Investigation Upends Idea That Bitcoin Is Untraceable*, N.Y. TIMES (June 9, 2021), https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html. ("'It is digital bread crumbs,' said Kathryn Haun, a former federal prosecutor and investor at venture-capital firm Andreessen Horowitz. 'There's a trail law enforcement can follow rather nicely.'"). In the Colonial Pipeline case, the FBI "was able to track multiple transfers of bitcoin and identify that approximately 63.7 bitcoins, representing the proceeds of the victim's ransom payment, had been transferred to a specific address, for which the FBI has the 'private key,' or the rough equivalent of a password needed to access assets accessible from the specific Bitcoin address. This bitcoin represents proceeds traceable to a computer intrusion and property involved in money laundering and may be seized pursuant to criminal and civil forfeiture statutes." Press Release, Dep't Just., Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (June 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside [https://perma.cc/UWG4-2YHL]. *See also* Affidavit in Support of an Application for a Seizure Warrant, Case 3:21-mj-70945-LB (June 7, 2021), https://www.justice.gov/opa/press-release/file/1402056/download.

keystrokes (and thus your key) or direct intelligence from someone with knowledge of the key, for example.[30]

Further limiting the anonymity of cryptocurrency are exchanges. Exchanges are third-party companies that enable the transfer of blockchain digital assets, such as cryptocurrency, into fiat currency or different digital currencies.[31] Exchanges obtain personal information about customers and operate similar to financial institutions, but unlike these financial institutions they are not insured by the Federal Deposit Insurance Company, making them a target for federal law enforcement seeking information about the identity of cryptocurrency wallet holders during criminal or civil investigations.[32]

B. Ransomware on the Rise

Ransomware relies on cryptocurrency as the financial vehicle for profits. Ransomware is a form of malware that encrypts a victim's system, network, or files and demands a payment to unlock the encryption.[33] There are multiple variants of ransomware that have been frequently deployed recently, including TrickBot, DarkSide, Egregor, Mamba, Ryuk, and Qbot.[34] Ransomware attacks require an initial attack vector, some sort of successful exploitation or initial foothold, to gain access to the victim's system in order to lock the systems and hold them for ransom. This can take the form of a phishing attack,

30. Paul Ducklin, *How Could the FBI Recover BTC from Colonial's Ransomware Payment?*, NAKED SECURITY BY SOPHOS (June 9, 2021), https://nakedsecurity.sophos.com/2021/06/09/how-could-the-fbi-recover-btc-from-colonials-ransomware-payment/ [https://perma.cc/X4K4-SC38].

31. *See, e.g.*, *How Does a Crypto Exchange Work?*, SOFI INVEST (Sept. 23, 2022) https://www.sofi.com/learn/content/how-crypto-exchanges-work/ ("When you set up an account with a crypto exchange, it enables you to buy and sell cryptocurrencies like bitcoin (BTC), ether (ETH), litecoin (LTC), polkadot (DOT), dogecoin (DOGE), and so on. Depending on the exchange, you can purchase crypto using a fiat currency like the U.S. dollar, or trade one form of crypto for another.").

32. *Advisory to FDIC-Insured Institutions Regarding FDIC Deposit Insurance and Dealings with Crypto Companies*, Federal Deposit Insurance Corporation (July 29, 2022), https://www.fdic.gov/news/financial-institution-letters/2022/fil22035b.pdf (noting that "FDIC insurance does not protect a non-bank's customers against the default, insolvency, or bankruptcy of any non-bank entity, including crypto custodians, exchanges, brokers, wallet providers, or other entities that appear to mimic banks but are not, called 'neobanks.' ").

33. STOPRANSOMWARE, https://www.cisa.gov/stopransomware ("Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.").

34. *Fact Sheets and Information: Specific Ransomware Variants,* STOPRANSOMWARE, https://www.cisa.gov/stopransomware/fact-sheets-information. Some of these variants are synonymous with the gangs who proliferate them, for example, the Ryuk cybercrime gang uses the aptly named Ryuk variant, *id*.

gaining access through unpatched systems, or exploiting an open-source software vulnerability as part of a sophisticated supply chain attack.[35] Once the initial foothold has been established, the ransomware encrypts files until payment—usually in the form of cryptocurrency—is provided, rendering the files unreadable and unusable.

Targets of ransomware attacks vary widely, but since the attacks are ultimately profit-seeking endeavors, ransomware actors have gradually shifted focus to a few key industries that are more likely to pay ransom instead of seeking technical solutions, such as restoring systems from backups. In 2021, ransomware actors targeted the healthcare industry, the financial sector, industrial control systems, state and local governments, IT services, and the education sector.[36] In the midst of the COVID-19 pandemic, ransomware attacks against healthcare facilities (which are defined in the U.S. as critical infrastructure)[37] accounted for almost 50% of all healthcare data breaches.[38] The *HIPAA Journal* estimates that every compromised patient record costs the healthcare industry $408 per personal record, a higher cost than any other industry.[39]

Educational institutions are also targeted by ransomware, with the average cost of each ransomware attack reaching an estimated $447,000.[40] These two industries do not frequently allocate their resources to cybersecurity and other measures that may help harden an organization against ransomware attacks.[41] The financial sector, which

35. MULTI-STATE INFO. SHARING & ANALYSIS CTR., RANSOMWARE GUIDE, (Sept. 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf.

36. *See, e.g.*, *Trellix Advanced Threat Research Report*, TRELLIX (Oct. 2021), https://www.trellix.com/en-us/advanced-research-center/threat-reports/oct-2021.html; Rob Sobers, *81 Ransomware Statistics, Data, Trends, and Facts for 2021*, VARONIS (July 5, 2022), https://www.varonis.com/blog/ransomware-statistics-2021/.

37. PRESIDENTIAL POLICY DIRECTIVE 21, CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCY (Feb. 12, 2013) [hereinafter PPD-21] (citing USA Patriot Act of 2001, 42 U.S.C. § 5195I).

38. DEP'T HEALTH AND HUM. SERV., 2021 FORECAST: THE NEXT YEAR OF HEALTHCARE CYBERSECURITY 8 (2021), https://hhs.gov/sites/default/files/2021-hph-cybersecurity-forecast.pdf.

39. Steve Alder, *Healthcare Data Breach Costs Highest of Any Industry at $408 Per Record*, HIPPA J. (July 12, 2018), https://www.hipaajournal.com/healthcare-data-breach-costs-highest-of-any-industry-at-408-per-record/.

40. *BlueVoyant Report Reveals Ransomware is the Number 1 Cyber Threat Facing Higher Education*, BLUEVOYANT (Feb. 23, 2021), https://www.bluevoyant.com/news/bluevoyant-report-reveals-ransomware-is-the-number-1-cyber-threat-facing-higher-education/.

41. Sixty-six percent of universities in the U.S. lack standard email security configurations, making phishing attacks more likely to go undetected. *Id*. Meanwhile,

does traditionally allocate significant resources to cybersecurity, was not immune from ransomware either. The Department of Treasury notes that as of October 2021, the volume of ransomware payments by banks in the U.S. is on pace to double compared to the previous year.[42]

PART II: CONSTITUTIONAL AUTHORIZATION TO TARGET RANSOMWARE ACTORS

A. Congressional Authorization of DOD Actions in Cyberspace

With a better picture of the threat, and public statements from DOD senior leaders acknowledging that DOD is addressing the ransomware threat, I look at the underlying legal authority for such potential actions. Since ransomware actors, particularly those not formally affiliated with a nation state, fall outside of what would typically be considered a military target, understanding this legal authority is a timely exercise.

The root of DOD's power is the U.S. Constitution. DOD's source of authority stems from the President's plenary Article II powers. The President is the "Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States,"[43] while Congress is bestowed the power "to declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water; to raise and support Armies. . .; to provide and maintain a Navy; [and] to make Rules for the Government and Regulation of the land and naval Forces."[44] U.S. military operations are therefore authorized pursuant to executive and congressional constitutional powers.

---

only fifty percent of healthcare organizations conduct cybersecurity risk assessments and organizations only dedicate six percent or less of their annual IT budget to cybersecurity, Heather Landi, *Could Patients be at Risk During a Hospital Cyberattack? It Depends How Far Hackers are Willing to Go, Expert Says*, FIERCE HEALTHCARE (Nov. 23, 2020).

42. Ian Talley, *U.S. News: Suspected Ransomware Payments Have Nearly Doubled This Year*, WALL ST. J. (Oct. 16, 2021), https://www.wsj.com/articles/suspected-ransomware-payments-for-first-half-of-2021-total-590-million-11634308503 [https://perma.cc/ET2J-VH2G]; Sean Lyngass, *US Financial Institutions Report Major Increase in Ransomware Payments to Cybercriminals*, CNN (Oct. 15, 2021), https://www.cnn.com/2021/10/15/politics/ransomware-payments-increase/index.html [https://perma.cc/2T8H-EKEK] (noting that bank payments have reached $600 million in reported ransomware payments).

43. U.S. CONST. art. II, § 2.

44. U.S. CONST. art. I, § 8.

Given the concurrent constitutional power structure for military and national security affairs, the President is limited when acting alone in this realm. The President's powers with respect to the military and national security are at their strongest when supported by an affirmative delegation of power by Congress since both Congress and the President have roles to play in the national security realm.[45] Justice Jackson's famed concurrence in *Youngstown Sheet and Tube Co. v. Sawyer* established a tier of permissible national security delegations. The President's national security power is at its height when she acts "pursuant to an express or implied authorization of Congress."[46] "[In the] absence of either a congressional grant or denial of authority, [the President] can only rely upon his own independent powers," or exists in a "twilight zone."[47] A President acting in a twilight zone "may have concurrent authority" with Congress, thus expanding her powers beyond those "independent powers" that are specifically granted in the Constitution.[48] Finally, when the President acts in contrast to congressional action, or takes actions that are "incompatible with the expressed or implied will of Congress," the President's power is at its lowest, meaning the actions are more likely to be unconstitutional.[49]

Congress has generally chosen to provide DOD with cyberspace authorities through National Defense Authorization Acts (NDAAs). Congress has provided clear authority to DOD to defend against nation-state cyber threats from China, Iran, North Korea, and Russia.[50] The 2019 NDAA authorizes the Secretary of Defense to "develop, prepare, and coordinate; make ready all armed forces for purposes of;

45. *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson J., concurring) ("When the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain. Therefore, congressional inertia, indifference or quiescence may sometimes, at least as a practical matter, enable, if not invite, measures on independent presidential responsibility. In this area, any actual test of power is likely to depend on the imperatives of events and contemporary imponderables rather than on abstract theories of law.").

46. *Id*. at 635.

47. *Id.* at 637.

48. *Id*.

49. *Id*.

50. For the purposes of this paper, I will also assume that the operations discussed here are squarely within the definition of a Traditional Military Activity (TMA), rather than a clandestine action, which would trigger alternative oversight and congressionally mandated limitations. For a thorough examination of TMAs versus clandestine activities in cyberspace and Congress' attempts to clarify how to categorize cyberspace operations, *see* Laura B. West, *The Rise of the "Fifth Fight" in Cyberspace: A New Legal Framework and Implications for Great Power Competition*, 229 MIL. L. REV. 273 (2021).

and, when appropriately authorized to do so, *conduct, military cyber activities or operations in cyberspace*, including clandestine military activities or operations in cyberspace, to defend the United States and its allies, including in response to malicious cyber activity carried out against the United States or a United States person by a foreign power."[51]

Interestingly, the NDAA authorization is conditioned upon defending against or responding to malicious cyber activity carried out by a foreign power. As discussed in Part II, ransomware actors are generally criminal gangs, unaffiliated with nation states, although some may receive tacit protection from the countries they reside in, who turn a blind eye to their criminal activity.[52]

The next section of the NDAA, codified at 10 U.S.C. § 394 (b), sheds light on what DOD can do in cyberspace against the aforementioned foreign powers. The section provides:

> "that the activities or operations referred to in [the previous section] when appropriately authorized, include the conduct of military activities or operations in cyberspace short of hostilities (as such term is used in the War Powers Resolution (Public Law 93-148; 50

51. National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1632, 132 Stat. 1636, 2123 (2018) (codified at 10 U.S.C. § 394) [hereinafter NDAA FY-2019]. Similarly, the NDAA authorizes CYBERCOM specifically to take action in cyberspace, but only against named foreign adversaries. Section 1642 authorizes CYBERCOM to "take appropriate and proportional action in foreign cyberspace" in order "to disrupt, defeat, and deter" ongoing adversarial activity in the cyber domain, though only [when] two conditions have been met: (1) there is "an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempt[s] to influence American elections and democratic political processes" and (2) the entity deemed responsible for the campaign is Russia, China, North Korea, or Iran. *Id*.

52. *See, e.g*., Frank Bajak, *How the Kremlin Provides a Safe Harbor for Ransomware,* AP (Apr. 26, 2021), https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7eb3841be45dff2d93ed3102999 [https://perma.cc/83GL-VPP7]. Notably, the NDAA itself does not provide a definition of a foreign power, the Foreign Intelligence Surveillance Act of 1978 (FISA) is one statute that can guide what may be intended, but in practice is not relied on for this NDAA provision. . . Under FISA, a "'foreign power' means— (1) a foreign government or any component thereof whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation therefor; (5) a foreign-based political organization, not substantially composed of United States persons; (6) an entity that is directed and controlled by a foreign government or governments; or (7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction." 50 U.S.C. § 1801. Under this definition, a ransomware gang would be unlikely to be defined as a foreign power without proof of such direct links.

> U.S.C. 1541 et seq.)) or in areas in which hostilities are not occurring, including for the purpose of preparation of the environment, information operations, force protection, and deterrence of hostilities, or counterterrorism operations involving the Armed Forces of the United States."[53]

A strict reading of this section shows that the activities in cyberspace must comply with the previous section of the NDAA (10 U.S.C. § 394), which, as stated before, does not offer an express authorization for DOD actions against ransomware actors who are unaffiliated with foreign states. Section 394(b) gives broad latitude to the types of actions that are permissible below the use of force and is not an exhaustive list. At its narrowest reading, the NDAA authorizes a broad suite of actions against the aforementioned foreign powers, suggesting that the NDAA does not intend to expressly authorize actions in cyberspace against ransomware actors who are unaffiliated with nation states.

Overall, previous NDAAs do not offer express authorizations for DOD to target criminal cyber actors who are unaffiliated with a foreign government. The closest provision to an express authorization is in the FY-2022 NDAA, which requires the Secretary of Defense to undertake an assessment of DOD's ability to respond to ransomware threats.[54] In particular, the DOD assessment should include an assessment on USCYBERCOM's specific ability to respond and combat the threat of ransomware.[55] Such an assessment could reasonably create a pathway to a more direct congressional authorization to target ransomware actors in subsequence NDAAs. In the meantime, however, the lack of express congressional authorization is not a death knell to DOD's authorities. We are left in Justice Jackson's "twilight" zone,[56] where the President can rely on her express powers.

B. Presidential Powers to Act in Cyberspace

The President is the commander in chief of the armed forces, which the executive branch has historically construed broadly to mean

53. 10 U.S.C. § 394 (b).

54. National Defense Authorization Act for FY-2022, 117 S. 1605, Pub. L. 117-81, (2021). The Department must "conduct a comprehensive assessment of the policy, capacity, and capabilities of the Department of Defense to diminish and defend the United States from the threat of ransomware attacks." *Id*., § 1510 (a)(1).

55. *Id*., (a)(1)(B)(ii) (I), (II). The assessment must include "the threshold at which United States Cyber Command should respond to such a threat; and (II) the capacity for United States Cyber Command to respond to such a threat without harmful effects on other United States Cyber Command missions."

56. *Youngstown*, 343 U.S. at 637.

that the President has wide latitude over military operations that are below the threshold of the use of force or armed conflict. While Congress has the power to declare war, "it is the longstanding view of the Executive Branch that this authority may include the use of armed force when the anticipated nature, scope, and duration of the operations do not rise to the level of 'war' under the Constitution . . . ."[57]

This conclusion is consistent with federal courts' broad reading of the President's Article II powers in national security and military matters. Dean of the University of Texas School of Law Bobby Chesney coined the term "national security fact deference" to explain the judiciary's deference to the executive branch.[58] As Chesney explains, courts have consistently deferred to the executive branch when matters of national security are litigated. Among the seminal cases is *U.S. v. Curtiss-Wright Export Corp.*, in which the Supreme Court opined that the executive is the "sole [government] organ" when it comes to international relations.[59] More modern cases too have affirmed this deference in the context of counterterrorism. In *Hamdi v. Rumsfeld*, a landmark case on Guantanamo detainees' rights, the Supreme Court affirmed that "core strategic matters of warmaking belong in the hands of those who are best positioned and most politically accountable for making them," the executive branch.[60] However, the Court limited its holding on deference with a plurality noting that courts must have some involvement and provide detainees an ability to be heard in court, balanced against the government's interest in continuing its sensitive military operations unhindered by court processes.[61]

Most recently, the Supreme Court revisited its deference to the executive in national security affairs vis-à-vis congressional powers in *Zivotofsky v. Kerry*. Addressing the power to recognize foreign governments, the Court held that "[t]he Executive is not free from the ordinary controls and checks of Congress merely because foreign affairs are at issue. . . . Nonetheless, it is for the President alone to make the specific decision of what foreign power he will recognize as legitimate, and his position must be clear."[62] The Supreme Court noted more broadly that prior congressional acquiescence to executive action can be "pertinent" to the determination of whether an executive

57. Paul C. Ney, *Some Considerations for Conducting Legal Reviews of U.S. Military Cyber Operations*, HARV. INTL. L. J. (Mar. 2, 2020).

58. Bobby Chesney, *National Security Fact Deference*, 95 VA. L. REV. 6, 1362 (Oct. 2009).

59. United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 305 (1936).

60. Hamdi v. Rumsfeld, 542 U.S. 507, 531 (2004).

61. *Id*. at 535.

62. Zivotofsky v. Kerry, 576 U.S. 1, 3 (2015).

action is legal "when the President acts in the absence of express congressional authorization, not when he asserts power to disregard a statute. . . ."[63] A prior case, *Dames & Moore v. Reagan*, held that "[p]ast practice [by the executive] does not, by itself, create power, but 'long-continued practice, known to and acquiesced in by Congress, would raise a presumption that the [action] had been [taken] in pursuance of its consent."[64] *Zivotofsky* may therefore signal a slight narrowing of the power of congressional acquiescence in national security matters.

Absent full DOD legal reviews on the subject, public acknowledgement of DOD actions targeting ransomware actors supports the assumption that DOD's actions are generally considered legal.[65] We know from public statements about DOD legal reviews for cyberspace operations that operations are analyzed for compliance with domestic law, including to ensure that operations are consistent with the President's Article II powers.[66] These statements suggest that DOD, internally at least, has concluded it is legal to go after ransomware actors. According to DOD, "[the] President has authority under Article II of the U.S. Constitution to direct the use of the Armed Forces to serve important national interests, and it is the longstanding view of the Executive Branch that this authority may include the use of armed force when the anticipated nature, scope, and duration of the operations do not rise to the level of 'war' under the Constitution, triggering Congress's power to declare war."[67] However, while Congress has affirm-

63. *Id*. at 64. *See also* Medellin v. Texas, 552 U. S. 491, 528 (2008) ("Congressional acquiescence is pertinent when the President's action falls within the second category—that is, when he 'acts in absence of either a congressional grant or denial of authority.' ").

64. Dames & Moore v. Regan, 453 U.S. 654, 686 (1981). The case is one of many with similar holdings about the extent to which congressional acquiescence may be considered in national security affairs. *See, e.g.,* INS v. Chadha, 462 U.S. 919, 975 (1983) ("The silence of Congress after consideration of a practice by the Executive may be equivalent to acquiescence and consent that the practice be continued until the power exercised be revoked.") (citing United States v. Midwest Oil Co., 236 U.S. 459, 481 (1915)).

65. Erica Lonergan & Lauren Zabierek, *What Is Cyber Command's Role in Combating Ransomware?*, LAWFARE (Aug. 18, 2021), https://www.lawfareblog.com/what-cyber-commands-role-combating-ransomware (presuming a legality of the operations in question. "It is apparent that Cyber Command currently has authority to engage cybercriminals in some circumstances, seemingly beyond 'hunt forward' and partnering operations. This was demonstrated by its reported fall 2020 campaign against the Trickbot botnet run by Russian criminals. Moreover, in June 2021, Deputy Assistant Secretary of Defense for Cyber Policy Mieke Eoyang testified in front of the Senate Armed Services Subcommittee on Cybersecurity, affirming the military's role in countering ransomware attacks.").

66. *See, e.g.*, Ney, *supra* note 57, at 28–29.

67. *Id*. Further, "the Supreme Court has long affirmed the President's power to use force in defense of the nation and federal persons, property, and instrumentali-

atively authorized some types of cyber operations through the NDAA, these statutory grants of authority arguably do not extend explicitly to the ransomware problem set. We are left then with congressional silence in the face of DOD actions that could amount to congressional acquiescence to an exercise of executive power. Determining whether to act in the face of congressional silence may ultimately be a call for DOD policymakers, rather than lawyers.

C. Additional Constitutional Concerns: The Fourth Amendment

Notwithstanding congressional authorizations and the President's Article II powers, additional constitutional provisions could be implicated by leveraging cryptocurrency as part of a cyber operation against ransomware actors, including the Fourth Amendment, which protects against unreasonable searches and seizures.[68] There is limited case law directly addressing whether there is a reasonable expectation of privacy (REP) on the blockchain, but a Fifth Circuit case has explicitly denied that there is any REP with respect to a person's personal information on the blockchain. When the transaction history or personal information is obtained through a valid law enforcement subpoena of a cryptocurrency exchange, the Fourth Amendment's third-party doctrine is not implicated.[69]

Obtaining personal information or data about someone, including malicious cyber actors, could, under certain circumstances, be considered a search. When a search by law enforcement or another government actor occurs, the Fourth Amendment generally prohibits an unlawful search or seizure. If the Fourth Amendment is applicable, any action that constitutes a search or seizure, generally, cannot be performed without a law enforcement warrant. Since DOD is not a law enforcement actor, it could be constrained by the Fourth Amendment in its activities against ransomware actors since it does not have avenues to obtain warrants, nor should it arguably since such law enforcement activity would go counter to the Department's role and mission.

The Fourth Amendment has expanded in the digital age, for example, to protect against law enforcement obtaining a person's cellsite location data.[70] However, "[t]he [Supreme Court] had long held that the Fourth Amendment does not protect information we voluntarily

ties. Accordingly, the President has constitutional authority to order military cyber operations even if they amount to use of force in defense of the United States." *Id*.

68. U.S. CONST. amend. IV.

69. United States v. Gratkowski, 964 F.3d 307, 310 (5th Cir. 2020).

70. *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).

disclose to others."[71] Accordingly, federal courts have applied the Fourth Amendment[72] to cryptocurrency exchanges, generally finding that there is not a reasonable expectation of privacy as to the personal information held by these exchanges.[73] Using cryptocurrency "is (at least for now) far more voluntary than owning a cell phone, and cryptocurrency protocols particularly are not comprehensive windows into a person's life and movements; instead [cryptocurrency transactions are] now much more like bank records[,]" meaning a person transacting in cryptocurrency, on a cryptocurrency exchange, may be more protected by the Fourth Amendment.[74]

However, given the congressional authorizations to target foreign cyber actors connected to China, Iran, North Korea, and Russia, ransomware actors may be more likely to be considered foreign actors without Fourth Amendment protections, regardless of the physical location of their data. Courts have taken a strong consistent stance in the surveillance context against the applicability of the Fourth Amendment to foreign actors. Peter Machtiger summarizes incidental collection and surveillance case law in the Fourth Amendment context:

> "The [*Hasbajrami*] court noted that 'the Fourth Amendment does not apply extraterritorially to the surveillance of persons abroad,

71. Elizabeth Goiten, *The Government Can't Seize Your Digital Data. Except by Buying It*., WASH.POST (Apr. 26, 2021), https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/ [https://perma.cc/8L5R-8W5K].

72. "The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. But the fact of diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely. *Smith v. Maryland* and *United States v. Miller*, after all, did not rely solely on the act of sharing. Instead, they considered the nature of the particular documents sought to determine whether there is a legitimate expectation of privacy concerning their contents." *Carpenter*, 138 S. Ct. at 2219. *See also* Smith v. Maryland, 442 U. S. 735, 740 (holding that when an individual "seeks to preserve something as private," and expects "that society is prepared to recognize [this] as reasonable," law enforcement must first get a lawful subpoena.); United States v. Miller, 425 U. S. 435, 441–43 (holding that there is no expectation of privacy in financial records held by a bank).

73. *See Gratkowski*, 964 F. 3d at 311 (discussing the applicability of the third party doctrine, as most recently articulated by the Supreme Court in *Carpenter*, 138 S. Ct. 2206). *See also Miller*, 425 U.S. at 442–43 ("The lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act, the expressed purpose of which is to require records to be maintained because they have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings.").

74. Paul Belonick, *Transparency is the New Privacy: Blockchain's Challenges for the Fourth Amendment*, 23 STAN. TECH. L. REV. 114, 158 (2020). A full discussion of the 4th Amendment and its applicability to transactions on the blockchain and determining the location of data is outside the scope of this paper.

> including United States citizens.' Next, the court relied on the 'incidental overhear' doctrine, according to which an additional warrant is not required when, 'in the course of executing a warrant or engaging in other lawful search activities, [officers] come upon evidence of other criminal activity outside the scope of the warrant or the rationale justifying the search, or the participation of individuals not the subject of the initial warrant or search.'"[75]

Machtiger notes that the court gave weight to the government's purpose of preventing terrorism domestically, and that such resulting incidental collection is reasonable. There could likewise be a stronger case for not applying the Fourth Amendment if the target is otherwise targetable under congressional authorizations to DOD. "[L]aw enforcement agents do not need to obtain a separate warrant to collect conversations of persons as to whom probable cause did not previously exist with individuals whose oral or wire communications are being collected through a lawful wiretap or bug, where those conversations on their face contain evidence of criminal activity."[76] Extending this reasoning to DOD in the ransomware context could mean bypassing law enforcement involvement and the warrant requirement if a search or seizure does indeed occur.

PART III: INTERNATIONAL LIMITS ON TARGETING RANSOMWARE ACTORS

If we assume that potential cyber operations against ransomware actors are constitutionally permissible, we must then consider whether any specific prohibitions exist under international law. Generally, domestic law must provide positive authority (an express authorization), while international law must not provide an express prohibition on actions.[77] The following section explores whether actions targeting the

75. Peter G. Machtiger, *Updating the Fourth Amendment Analysis of U.S. Person Communications Incidentally Collected Under FISA Section 702*, HARV. NAT'L SEC. J. ONLINE (Feb. 7, 2021) (quoting United States v. Hasbajrami, 945 F.3d 641, 662 (2d Cir. 2019)). However, this can be distinguished from Machtiger's discussion of FISA 702 surveillance since the blockchain is not necessarily located in the U.S.

76. *Hasbajrami*, 945 F.3d at 664.

77. This is commonly referred to as the Lotus Principle, named after *The Case of the S.S. Lotus*. S.S. 'Lotus' (Fr. v. Turk.), 1927 P.C.I.J (ser. A) No. 10 (Sept. 7) at 19. Scholar An Hertogen rephrased the principle as "whatever is not explicitly prohibited by international law is permitted," although other scholars have refuted this as an accurate holding of the Lotus case. An Hertogen, *Letting* Lotus *Bloom*, 26 EUROPEAN J. OF INT'L L. 901, 902 (Feb. 12, 2016). *Cf* Hugh Handeyside, *The Lotus Principle in ICJ Jurisprudence: Was the Ship Ever Afloat?*, 29 MICH. J. OF INT'L L. 71, 76 (2007).

cryptocurrency used by ransomware actors would be permitted under international law prohibitions against destruction.

A. Use of Force and Applicability of International Law to Cyberspace

This section addresses the development of relevant international law provisions to understand whether impermissible destruction can be applied to cryptocurrency in the context of countering ransomware actors in cyberspace. The United Nations (U.N.) Charter is a foundational component of international law. Article 2(4) of the Charter criminalizes the aggressive use of force by States as crimes against international, peace and security, stating that "[a]ll members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[78] The Article is recognized as a norm of customary international law (CIL) as well. However, cyber operations represent a conundrum for lawyers, since they do not always resemble or easily equate to traditional attacks, thereby making their categorization difficult. The question of whether cyber operations reach the level of a use of force has been hotly debated, although the general U.S. government position is that cyber operations are below the use of force.[79]

Academic consensus generally supports the notion that some but not all cyber operations may rise to the level of a use of force, but such an analysis is dependent on the particular facts of the operation and the effects it causes. Andrew Moore writes that "the interpretation of Article 2(4)'s prohibition against force should evolve to include coercive uses of the cyber instrument that have destructive effects in the physical world . . . ," while Michael Schmitt has articulated that "[w]hatever force is, then, it is not economic or political pressure. Therefore, a cyber operation that involves such coercion is definitely not a prohibited use of force."[80]

78. U. N. Charter art. 2, ¶4.

79. Ney, *supra* note 57 (In his speech at the US Cyber Command Legal Conference, then-DOD General Counsel Ney stated that "the vast majority of military operations in cyberspace do not rise to the level of a use of force. . .").

80. Andrew Moore, *Article 2(4)'s Prohibition Against the Use of Force: Customary Law and Potential Models*, 64 NAVAL L. REV. 1, 3 (2015); Michael N. Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, 56 VILL. L. REV. 569, 574 (2011). *See also* Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT'L L. 525, 537 (2012) (writing that while some cyber operations can cause physical consequences, "treating all forms of cyber attack as a use of force would require an implausibly broad reading of Article 2(4) that includes non-physical damage."); Ashley Deeks, Noam Lubell & Daragh Murray, *Machine Learning, Artificial Intelligence,*

Another limiting factor on the applicability of international law to cyberspace is the Geneva Convention, which applies in "all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them."[81] Whether this threshold is met by cyber operations is another source of academic and policy debate.[82] Schmitt, the editor of the Tallinn Manual, which provides nonbinding guidance for the application of international law to cyberspace, argues that an armed conflict in cyberspace is triggered when a state "either intended to cause injury, death, damage or destruction (and analogous effects), or such consequences are foreseeable, [and IHL] principles apply . . . even though classic armed force is not being employed."[83] In general, however, there is little to no international consensus on the question; "the [Tallinn] International Group of Experts agreed that cyber operations resulting in physical damage or injury are unambiguously uses of force, no consensus could be reached as to when cyber operations not having those consequences qualify."[84] Under Schmitt's definition, a cyber operation that either impairs use of or destroys a cryptocurrency wallet could be regarded as an armed attack, and inter-

and the Use of Force by States, 10 J. NAT'L SECURITY L. & POL'Y 1, 8 (2019) ("[Some] cyber operations implicate the use of force to the extent that the offensive cyber operations constitute (cyber) armed attacks and the responsive cyber operations represent acts of self-defense.").

81. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 2, Aug. 12, 1949, 75 U.N.T.S. 970. Defined alternatively, an international "armed conflict exists whenever there is a resort to armed force between States. . . ." *Prosecutor v. Dusko Tadic aka "Dule" (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction)*, IT-94-1, (International Criminal Tribunal for the former Yugoslavia (ICTY), Oct. 2, 1995).

82. *See* Zen Chang, *Cyberwarfare and International Humanitarian Law*, 9 CREIGHTON INT'L & COMP. L.J. 29 (Dec. 2017). For a critique of the Tallinn Manual, *see* Tarah Wheeler, *In Cyberwar, There Are No Rules: Why the World Desperately Needs Digital Geneva Conventions*, FOREIGN POL'Y (Sept. 12, 2018), https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/ [https://perma.cc/784Y-RJQZ] ("No definition of a cyber-related war crime can be effective without international legitimacy. If a group of experts actually did convene to create binding digital Geneva Conventions, it's unclear from what source it would derive its authority. NATO sponsored the Tallinn conference, but the Tallinn Manual is nonbinding and was not an official NATO publication. Moreover, the alliance itself is currently on shaky ground, and there's no guarantee that the United States would abide by any agreement.").

83. Michael N. Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, 84 INT'L REV RED CROSS 365, 374 (Jun. 2002) (emphasis omitted).

84. Michael N. Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum*, 8 HARV. NAT'L SEC. J. 239, 245 (2017).

national law limitations and requirements will apply, but the view certainly is not dispositive.

Paul Ney, then-General Counsel of DOD, publicly articulated the U.S. view on the applicability of international law to cyberspace in 2020. Ney stated at the CYBERCOM annual legal conference that "existing international law applies to State conduct in cyberspace."[85] DOD's view, according to Ney, is that a cyber operation may reach the use of force under the U.N. Charter under certain circumstance, and DOD lawyers should consider, among other things, whether "the operation causes physical injury or damage" to answer the question.[86] Similarly, Harold Koh, then the senior lawyer for the Department of State, opined that "cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force."[87] The connection to physical injury suggests that more often than not, cyber operations may not reach the threshold of a use of force.

As an example, deleting a cryptocurrency wallet, "sinkholing," would practically have no physical ramifications. The deletion of a seed phrase would result in the owner of the wallet not being able to access cryptocurrency.[88] The cryptocurrency, at that point, is simply code that has value ascribed to it. Deleting a large amount of cryptocurrency seed phrases in bulk, thereby blocking access to a large amount of cryptocurrency, leaves the cryptocurrency still in existence and in circulation technically. You can arguably never truly delete cryptocurrency because the code continues to exist, it is just

85. Ney, *supra* note 57. *See also* U. S. SENATE COMM. ON ARMED SERVS., ADVANCE QUESTIONS FOR VADM MICHAEL S. ROGERS, USN NOMINEE FOR COMMANDER, U.S. CYBER COMMAND 14 (2014), http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf ("[p]er [DOD] guidance, all military operations must be in compliance with the laws of armed conflict-this includes cyber operations. The law of war principles of military necessity, proportionality and distinction will apply when conducting cyber operations.").

86. Ney, *supra* note 57.

87. Harold Koh, *International Law in Cyberspace: Address to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012*, 54 HARV. INT'L. L. J 1 (Dec. 2012).

88. As described in the tech publication *Wired*, "[s]inkholing is a technique for manipulating data flow in a network; you redirect traffic from its intended destination to the server of your choosing. It can be used maliciously, to steer legitimate traffic away from its intended recipient, but security professionals more commonly use sinkholing as a tool for research and reacting to attacks." Lily Hay Newman, *Hacker Lexicon: What Is Sinkholing?*, WIRED (Jan. 2, 2018), https://www.wired.com/story/what-is-sinkholing/ [https://perma.cc/D7XQ-NTTT]. To illuminate the concept, if an attacker was conducting a distributed denial of service (DDOS) attack, a cyber-defender could sinkhole the traffic to a different network or server where there is not a victim, thus rendering the attack ineffective.

inaccessible with current technology.[89] However, deleting the seed phrase leaves that amount of cryptocurrency inaccessible, at least until quantum computing catches up.[90] Until then, the sinkholed cryptocurrency could, at its most destructive, increase the value of the resource.[91]

B. Law of Armed Conflict Analysis

I assume *arguendo* that cyber operations such as deleting a seed phrase would not rise to the level of a use of force in cyberspace, and *jus ad bellum* (the law leading up to war) applies as opposed to *jus in bello* (the law governing the conduct of war).[92] The DOD Law of War Manual, which provides legal guardrails and incorporates policy for how the U.S. military can fight wars, states that the DOD should act consistent with the law of war rules and principles in all military operations, regardless of whether they reach the threshold of use of force.[93] Under the Law of Armed Conflict (LOAC), operations must comply with the necessity of military objectives, along with additional constraints. Put succinctly, "these constraints include 'military necessity,' which permits only acts of force necessary to accomplish legitimate military objectives; 'distinction,' which distinguishes between combatants and civilians; and 'proportionality,' which counsels that the anticipated loss of life or injury to civilians or damage to civilian ob-

89. *How Do I Delete a Crypto Address Associated with my Coinbase Account?,* COINBASE HELP CENTER, https://help.coinbase.com/en/coinbase/managing-my-account/other/delete-crypto-address (last accessed Mar. 5, 2022) ("It is not possible to delete a crypto address from your Coinbase account. Deleting addresses from any wallet is highly discouraged since any funds sent to an address which has had its private key deleted will be lost forever.").

90. Advances in quantum computing may inch us closer to the day when the encryption undermining cryptocurrency and the blockchain can be broken mathematically, although this is not currently possible. *See, e.g.*, Bryan Walsh, *Running the International Quantum Race*, AXIOS (Dec. 11, 2021), https://www.axios.com/united-states-china-quantum-computing-d1e1d32a-9851-49e2-a93c-bfb8995ee6e7.html [https://perma.cc/SL6Q-GZQ6]; Daniel Garisto, *China Is Pulling Ahead in Global Quantum Race, New Studies Suggest*, SCIENTIFIC AM. (July 15, 2021), https://www.scientificamerican.com/article/china-is-pulling-ahead-in-global-quantum-race-new-studies-suggest/ [https://perma.cc/2BFJ-4XV6].

91. Nathan Reiff, *Cryptocurrency Burning*, INVESTOPEDIA (Jan. 24, 2022), https://www.investopedia.com/tech/cryptocurrency-burning-can-it-manage-inflation/ [https://perma.cc/4AR3-QAZV].

92. U.S. DEP'T DEF., LAW OF WAR MANUAL § 1.11 (2016) [hereinafter DOD LAW OF WAR MANUAL].

93. *Id*., § 3.1 ("DoD practice has often been to act consistently with law of war rules, even in certain cases where these rules might not technically be applicable as a matter of law.").

jects not be in excess of military advantages anticipated from a specific act."[94]

The Law of War Manual expressly contemplates cyber operations that "disrupt, deny, degrade, or *destroy* information resident in computers and computer networks, or the computers and networks themselves."[95] The Law of War Manual closely tracks The Hague and Geneva Conventions limitations on destruction, stating that outside the context of an armed attack, "enemy property may not be seized or destroyed unless imperatively demanded by the necessities of war."[96]

Legal manuals written for individual armed services (Army, Air Force, Navy, Marines, for example) offer guidance on targeting (and implicitly destroying) specifically enemy economic sources. The comparison between cryptocurrency and economic sources may be instructive to the ransomware context. The Air Force published a manual on the law of war in 1980, which stated that: "[i]t is permissible to attack economic targets that give only indirect support to enemy operations, so long as that support is effective and a definite military advantage can be foreseen."[97] Likewise, the 1987 Commander's Handbook on the Law of Naval Operations authorized targeting "economic targets of the enemy that indirectly but effectively support and sustain the enemy's war-fighting capability."[98]

Just Security Editor-in-Chief Ryan Goodman offers a LOAC analysis for the destruction of economic instruments under which im-

94. C. Robert Kehler, Herbert Lin & Michael Sulmeyer, *Rules of Engagement for Cyberspace Operations: A View from the USA,* 3 J. OF CYBERSECURITY 69, 69 (Feb. 2, 2017). *See also* DOD LAW OF WAR MANUAL § 2.

95. DOD LAW OF WAR MANUAL § 16.1.2.1 (emphasis added).

96. *Id*., § 5.17. Article 23(g) of the 1907 Hague Regulations states that it is prohibited "to destroy or seize the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war." Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons during War on Land, art. 1 (Oct 18, 1907). Similarly, Article 53 of the Geneva Convention states that "[a]ny destruction by the Occupying Power of real or personal property belonging individually or collectively to private persons, or to the State, or to other public authorities, or to social or cooperative organizations, is prohibited, except where such destruction is rendered absolutely necessary by military operations." Geneva Convention Relative to the Protection of Civilian Persons in Time of War, art. 53, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

97. U.S. AIR FORCE, COMMANDER'S HANDBOOK ON THE LAW OF ARMED CONFLICT, July 25, 1980, 2-3(a) (AFP 110-34). "As long ago as the 1870s, for example, international courts recognized that the destruction of Confederate bales of cotton was justified during the American Civil War, since the sale of cotton provided funds for importing almost all Confederate arms and ammunition." *Id*.

98. RICHARD J. GRUNWALT, DIRECTOR, OCEANS L. & POL'Y DEP'T, NAVAL WAR COLLEGE, ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS (1989).

pacting cryptocurrency may not be allowed under international law. Goodman writes that "potential substitution effects" need to be taken into account in a LOAC analysis. In other words, "[if] a source of economic support to a military can be easily substituted by another source, the military advantage gained from the destruction or neutralization of the former is presumably more speculative."[99] Goodman's analysis rests on a military gaining an advantage for the applicability of this provision of international law.

The first legal hurdle in complying with the LOAC analysis is meeting the military necessity requirement. Relatedly, the second portion of a LOAC analysis is humanity. Under the DOD Law of War Manual, "suffering, injury, or destruction unnecessary to accomplish a legitimate military purpose must be avoided in cyber operations."[100] If we assume that impairing someone's access to cryptocurrency is considered destruction, then the action is barred if it is unnecessary to accomplish a legitimate military objective.

While ransomware actors pose a national security threat and the U.S. military appears to be focusing efforts and resources to the response, ransomware groups are generally criminal gangs, not connected to nation state militaries. However, preventing destruction to U.S. critical infrastructure may be categorized as a valid military objective in order to achieve DOD's mission of defending the homeland.[101] Additionally, while an analysis of the military necessity and "economic substitution" may be appropriate to address destroying physical cash stores, for example, it may not work as easily in the cryptocurrency and ransomware contexts.[102] Goodman ultimately concludes that while targeting "war sustaining" targets like cash stores may have seemed novel in 2016, the "historical record also includes States' express and implicit acknowledgements that their adversaries could lawfully attack war sustaining objects," despite the dual-use nature of these economic targets, suggesting a general acceptance of economic sources as military necessary under the correct circumstances.[103] We can assume then, that both military necessity

99. Ryan Goodman, *Targeting 'War-Sustaining' Objects in Non-International Armed Conflict,* 110 AM. J. OF INT'L. L. 1, 17 (June 9, 2016).

100. DOD LAW OF WAR MANUAL § 16.2.2.

101. DOD's mission is to "provide the military forces needed to deter war and ensure our nation's security." *About*, DEP'T DEFENSE, https://www.defense.gov/about/ (last visited Mar. 11, 2022).

102. Marty Lederman, *Is it Legal to Target ISIL's Oil Facilities and Cash Stockpiles?*, JUST SECURITY (May 27, 2016), https://www.justsecurity.org/31281/legality-striking-isils-oil-facilities-cash-stockpiles/ [https://perma.cc/8QGS-ATXU].

103. Goodman at 19, *supra* note 99.

and humanity can be complied with under LOAC in the context of targeting cryptocurrency assets of ransomware actors.

Finally, proportionality must be adhered to in such an operation. Proportionality requires that an action not be unreasonably excessive.[104] A proportionality analysis would weigh the military necessity of the action with any expected incidental damages. The analysis here is tenuous, as assessing the potential for incidental damage from destroying the cryptocurrency of a ransomware actor is speculative. The potential economic implications and downstream impacts that sinkholing cryptocurrency can cause have not been observed yet and may not be implicated by one single instance of sinkholing cryptocurrency. This potential for economic damage in this instance could be the result of cumulative operations, which is difficult to assess *ex ante*. In the face of the military necessity of protecting the homeland from destructive ransomware attacks, these speculative damages likely would not sway a decision maker's proportionally calculus. Conversely, the Law of War Manual advises that "economic harms in the belligerent State resulting from such disruptions, such as civilian businesses in the belligerent State being unable to conduct e-commerce, generally would not need to be considered in a proportionality analysis." However, since ransomware actors are not affiliated with a state, and effects in a digital economy may not easily be confined to one state, it is not clear this factor should not be considered in the context of cryptocurrency.

Conclusion

The culmination of the domestic and international legal landscapes leaves the door open as to whether DOD could leverage cryptocurrency of a ransomware actor, but absent express prohibitions, DOD could reasonably conclude that such operations are legal. Conducting cyber operations that impact cryptocurrency of a ransomware actor do not have clear congressional authorizations, but rather exist in an area of constitutional law where great deference is afforded to executive branch actions. International law and LOAC requires a robust examination of military necessity and proportionality, which if satisfied, can provide legal support to potential operations. Given the ever-changing nature of cryptocurrency technology however, there are not clear answers.

The legality of cyber operations is hotly debated in both domestic and international legal communities and a consensus has yet to be reached on even the most foundational questions, like whether cyber

104. DOD Law of War Manual § 2.4.

operations rise to the level of a use of force. The legal status of cryptocurrency is similarly ripe for different legal debate. The convergence of these two topics necessitates clearer legal authorities for the executive branch if ransomware continues to fall within DOD's purview.

Congressional lawmaking could clarify the limits of potential DOD actions with respect to ransomware actors. Congress has actively legislated DOD cyber activities through the National Defense Authorization Acts, weighing in on many legal debates as they develop, such as whether cyber operations are traditional military activities. Legislating through the NDAA has its pros and cons, however. On one hand, the authorizations for activities in cyberspace are clarified and amended frequently with every passing NDAA, which can lead to confusion and a lack of foundation legal framework with which to analyze these issues. Conversely, by legislating through the NDAA, Congress perhaps gives itself more flexibility and stays in tune with the rapidly changing nature of cyberspace, allowing authorities to reflect the current operating environment and DOD needs. As an alternative, Michael Garcia at the Third Way argued that Congress should instead create an Omnibus Cyber Bill to legislate on all issues touching cyberspace.[105] Given the speed of innovation in cyberspace though (by the U.S. and its adversaries), such an Omnibus Cyber Bill might be a short-term solution that is quickly outpaced by developing technology, muddying legal analyses on authority even further.

Regardless of the vehicle, the ability of DOD to address the ransomware threat could be clarified by Congress by either creating a more permissible legal landscape for operations or closing the door to potential cyber operations against ransomware actors. A broad grant of power to go after ransomware actors will certainly weigh in favor of a LOAC analysis when analyzing the ongoing threat of ransomware actors. The threat of ransomware is certainly not diminishing and clarifying the legal limitations of DOD's cyber options will be a critical component in any successful "surge" against ransomware.

105. Michael Garcia, *The Militarization of Cyberspace? Cyber-Related Provisions in the National Defense Authorization Act,* THIRD WAY (Apr. 5, 2021), https://www.thirdway.org/memo/the-militarization-of-cyberspace-cyber-related-provisions-in-the-national-defense-authorization-act [https://perma.cc/8345-ZEZY].