

Maurer School of Law: Indiana University

Digital Repository @ Maurer Law

Articles by Maurer Faculty

Faculty Scholarship


Fall 2022

The Law and Politics of Ransomware

Asaf Lubin

Maurer School of Law - Indiana University, lubina@iu.edu

Follow this and additional works at: <https://www.repository.law.indiana.edu/facpub>

 Part of the [Criminal Law Commons](#), [Insurance Law Commons](#), [International Law Commons](#), and the [Internet Law Commons](#)

Recommended Citation

Lubin, Asaf, "The Law and Politics of Ransomware" (2022). *Articles by Maurer Faculty*. 3063.
<https://www.repository.law.indiana.edu/facpub/3063>

This Article is brought to you for free and open access by the Faculty Scholarship at Digital Repository @ Maurer Law. It has been accepted for inclusion in Articles by Maurer Faculty by an authorized administrator of Digital Repository @ Maurer Law. For more information, please contact rvaughan@indiana.edu.

The Law and Politics of Ransomware

Asaf Lubin*

ABSTRACT

What do Lady Gaga, the Royal Zoological Society of Scotland, the city of Valdez in Alaska, and the court system of the Brazilian state of Rio Grande do Sul all have in common? They have all been victims of ransomware attacks, which are growing both in number and severity. In 2016, hackers perpetrated roughly four thousand ransomware attacks a day worldwide, a figure which was already alarming. By 2020, however, ransomware attacks reached a staggering number, between twenty thousand and thirty thousand per day in the United States alone. That is a ransomware attack every eleven seconds, each of which cost victims on average nineteen days of network downtime and a payout of over \$230,000. In 2021 global costs associated with ransomware recovery exceeded \$20 billion.

This Article offers an account of the regulatory challenges associated with ransomware prevention. Situated within the broader literature on underenforcement, the Article explores the core causes for the limited criminalization, prosecution, and international cooperation that have exacerbated this wicked cybersecurity problem. In particular, the Article examines the forensic, managerial, jurisdictional, informational, and resource allocation challenges that have plagued the fight against digital extortions in the global commons.

To address these challenges, the Article makes the case for the international criminalization of ransomware. Relying on existing international regimes—namely, the 1979 Hostage Taking Convention, the 2000 Convention Against Transnational Crime, and the customary prohibition against the harboring of terrorists—the Article makes the claim that most ransomware attacks are already criminalized under

* Dr. Asaf Lubin is an Associate Professor of Law at Indiana University Maurer School of Law, Fellow at IU's Center for Applied Cybersecurity Research, Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University, Affiliated Fellow at the Information Society Project at Yale Law School, and a Visiting Scholar at the Federmann Cyber Security Center at Hebrew University of Jerusalem. This work was supported by funding from the Federmann Cyber Security Center in conjunction with the Israeli National Cyber Directorate. The work benefited from the excellent comments of participants at workshops and events organized by the University of Geneva, New York University, the U.S. Secret Service Cyber Policy, Strategy and Outreach Division, the Information Society Project at Yale Law School, Third Way, The Berkman Klein Center for Internet and Society at Harvard University, the Israeli National Cyber Directorate, Chicagoland Junior Scholars Workshop, and the Federmann Cybersecurity Center at Hebrew University.

existing international law. In fact, the Article draws on historical analysis to portray the criminalization of ransomware as a “fourth generation” in the outlawry of *Hostis Humani Generis* (enemies of mankind).

The Article demonstrates the various opportunities that could arise from treating ransomware gangs as international criminals subject to universal jurisdiction. The Article focuses on three immediate consequences that could arise from such international criminalization: (1) expanding policies for naming and shaming harboring states, (2) authorizing extraterritorial cyber enforcement and prosecution, and (3) advancing strategies for strengthening cybersecurity at home.

TABLE OF CONTENTS

I.	INTRODUCTION	1179
II.	THE PROBLEM OF RANSOMWARE	1183
	A. Defining Ransomware	1183
	B. Existing Regulation and its Limits	1186
	1. Domestic Law	1186
	2. International Law	1192
	C. The Causes of Ransomware	
	Underenforcement.....	1196
	1. Information Asymmetries	1196
	2. Clashing Jurisdiction.....	1197
	3. The Tragedy of the Commons	1200
	4. Managerial Deficits.....	1200
	5. Forensic and Diplomatic	
	Challenges	1202
III.	REDEFINING THE CRIME OF RANSOMWARE.....	1203
	A. Ransomware and the Outlawry of	
	Hostis Humani Generis	1203
	B. Outlawing by Extension and Analogy	
	or by Treaty Design?	1205
	1. New International Instrument	1206
	2. Analogy and Extension.....	1207
IV.	BUILDING THE RANSOMWARE ENFORCEMENT	
	TOOLKIT.....	1210
	A. Naming and Shaming Harboring	
	States	1211
	B. Extraterritorial Enforcement and	
	Prosecution	1212
	C. Enhancing Cybersecurity at Home	1213
V.	CONCLUSION	1215

I. INTRODUCTION

On 10 June 2019, the quaint town of Lake City, Florida suffered a major ransomware attack, bringing most municipal activities and services to a halt.¹ An employee of the town opened a malicious email with a compromised document that infected the city's computers with a ransomware.² Beginning at 7:30 am, "the computers did not work and neither did the telephones. Even cellphones were wiped of contacts Nearly all of the city's systems—including its water and gas payment systems—were unusable. The copy machines, also linked to the computer network, did not work."³ With about sixteen terabytes of information effectively locked and online payment systems inoperable, the city was running blind.⁴ City employees were forced to go back to "paper receipts and hand-written building permits."⁵

Ransomware attacks are designed to deny access to a computer system or data, usually by encrypting it, until the victim pays extortion payments to the attacker.⁶ The ransomware used in Lake City's attack was the Ryuk malware.⁷ According to the United Kingdom's National Cyber Security Centre (NCSC), "Ryuk was first seen in August 2018

1. See Patricia Mazzei, *Another Hacked Florida City Pays a Ransom, This Time for \$460,000*, N.Y. TIMES (June 27, 2019), <https://www.nytimes.com/2019/06/27/us/lake-city-florida-ransom-cyberattack.html> [<https://perma.cc/7CNR-NC3S>] (archived Aug. 12, 2022).

2. See *2nd Florida City in Just a Week to Pay Hackers Big Ransom for Seized Computer systems*, CBS NEWS (June 26, 2019), <https://www.cbsnews.com/news/ransomware-attack-lake-city-florida-pay-hackers-ransom-computer-systems-after-riviera-beach/> [<https://perma.cc/VAE9-CDR7>] (archived Aug. 12, 2022).

3. Frances Robles, *A City Paid a Hefty Ransom to Hackers. But Its Pains Are Far From Over.*, N.Y. TIMES (July 7, 2019), <https://www.nytimes.com/2019/07/07/us/florida-ransom-hack.html> [<https://perma.cc/WT5X-2XBZ>] (archived Aug. 12, 2022).

4. *Id.*

5. Antonio Villas-Boas, *A Florida City Was Forced to Use Pen and Paper and Pay a \$500,000 Ransom After Hackers Took Control of its Computers*, BUS. INSIDER (June 27, 2019), <https://www.businessinsider.com/lake-city-florida-ransomware-cyberattack-hackers-bitcoin-payment-2019-6> [<https://perma.cc/C2XS-KGMS>] (archived Aug. 12, 2022).

6. The Departments of Justice, Homeland Security, and Health and Human Services define a ransomware as a "type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted." See U.S. DEPT OF JUST., RANSOMWARE: WHAT IT IS AND WHAT TO DO ABOUT IT, <https://www.justice.gov/criminal-ccips/file/872766/download> (last visited Sept. 21, 2022) [<https://perma.cc/SF95-JZKR>] (archived Aug. 12, 2022).

7. See Catalin Cimpanu, *Florida City Fires IT Employee After Paying Ransom Demand Last Week*, ZDNET (July 1, 2019), <https://www.zdnet.com/article/florida-city-fires-it-employee-after-paying-ransom-demand-last-week/> [<https://perma.cc/6PP6-Z2M3>] (archived Aug. 12, 2022).

and has been responsible for multiple attacks globally.”⁸ The NCSC further determined that Ryuk is “often not observed until a period of time after the initial infection—ranging from days to months—which allows the [malicious] actor time to carry out reconnaissance inside an infected network, identifying and targeting critical network systems and therefore maximising the impact of the attack.”⁹

Just like clockwork, days after the initial infection, a ransom demand made its way to Lake City officials. At first the city attempted to restore its systems to full operability with the help of the Federal Bureau of Investigation (FBI) and a consulting firm,¹⁰ hired by its municipal risk pool, Florida League of Cities.¹¹ Unfortunately, like many other cities across America, Lake City did not devote sufficient resources to cybersecurity and lacked basic features that could have prevented its computer networks from being vulnerable to this attack, or at least allow for faster recovery.¹² Indeed, within two weeks from the incident, the city manager made a decision to fire the city’s information technology (IT) director for failures relating to the incident.¹³

Failing to restore network operability, the city’s risk pool hired a ransomware negotiations company called Coveware that communicated with the hackers and brought their ransom demands down to from eighty-six Bitcoins (about \$700,000 based on the rate at the time) to forty-two Bitcoins (roughly \$460,000), of which the city only paid the \$10,000 deductible with the League of Cities paying the

8. NAT’L CYBER SEC. CTR., ADVISORY: RYUK RANSOMWARE TARGETING ORGANISATIONS GLOBALLY (June 21, 2019), <https://www.ncsc.gov.uk/files/RYUK%20Advisory%20draft%20CP%20June%202019.pdf> [<https://perma.cc/Y6NP-YG9C>] (archived Aug. 12, 2022).

9. *Id.*

10. *See* Robles, *supra* note 3. The exact scope of the FBI’s involvement in the case is not publicly known but it would seem to have been limited to restoration attempts of the data. *See id.*

11. A risk pool is a “nonprofit, mission-driven organization formed by a group of local government entities, usually within one state, to finance a risk, typically by pooling or sharing that risk. The entities themselves own and govern the pool. Technically, in most states, a pool is not an insurer, does not issue insurance policies, and is not regulated by the state insurance commissioner—at least not to the same degree as a commercial insurer. But the services a pool provides are virtually indistinguishable from insurance.” John Rappaport, *How Private Insurers Regulate Public Police*, 130 HARV. L. REV. 1539, 1557–58 (2017). According to one estimate, “[a]cross America, more than 500 of these pools exist, covering everything from transit authorities to counties.” Jonathan G. Steiner, *The Risk Pool Advantage*, N.H. MUN. ASS’N (2010), <https://www.nhmunicipal.org/town-city-article/risk-pool-advantage> [<https://perma.cc/4FGG-9A7Z>] (archived Aug. 13, 2022).

12. *See* Villas-Boas, *supra* note 5.

13. *See* Patty Matamoros & Francesca Stewart, *UPDATE: Lake City Fires Employee After Paying Ransom in Malware Attack*, WCJB (June 26, 2019), <https://www.wcjb.com/content/news/City-of-Lake-City-moves-Forward-after-Cyber-Attack-511802711.html> [<https://perma.cc/6CCQ-HL8F>] (archived Aug. 13, 2022).

rest.¹⁴ Ultimately, even with the encryption key provided by the hackers, each terabyte of encrypted data took “about 12 hours to recover,” and nearly “a month after the onset of the attack,” the city was still not able to return to full operations.¹⁵ Moreover, the city’s own budget reports have indicated that beyond the ransom the city had to pay upward of \$350,000 in expenses relating to the ransomware attack as well as other costs associated with equipment and software to update system security and IT infrastructure across the city.¹⁶

Lake City is not alone. From a power distribution company in India,¹⁷ through the Royal Zoological Society of Scotland,¹⁸ to the court system of the Brazilian state of Rio Grande do Sul,¹⁹ ransomware is anywhere and everywhere. In the United States, ransomware has become so prevalent that it has been identified as a national security concern triggering the involvement of the U.S. Cyber Command and the National Security Agency.²⁰ In recent years, ransomware attacks targeted a regional hospital in Indiana,²¹ a school district in

14. Renee Dudley, *The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks*, PROPUBLICA (Aug. 27, 2019), <https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks> [https://perma.cc/6MC3-JFCS] (archived Aug. 13, 2022).

15. See Robles, *supra* note 3.

16. See LAKE CITY, FLA., FY 19 BUDGET AMENDMENT #1, (2019), https://www.lcfla.com/sites/default/files/fileattachments/finance/page/1635/budget_amendment_1_-_2019.pdf [https://perma.cc/65PH-A64H] (archived Aug. 13, 2022).

17. See Pierluigi Paganini, *Systems at a Power Company in India infected by a ransomware*, SEC. AFFS. (Mar. 30, 2018), <https://securityaffairs.co/wordpress/70836/hacking/power-company-ransomware.html> [https://perma.cc/DE96-XRDN] (archived Aug. 13, 2022).

18. See David Paul, *National Trust and Edinburgh Zoo Latest Victims of Blackbaud Hack*, DIGIT NEWS (July 29, 2020), <https://digit.fyi/national-trust-and-edinburgh-zoo-latest-victims-of-ransomware-hack/> [https://perma.cc/9RS5-8K9U] (archived Aug. 13, 2022).

19. See Garrett Thompson, *Brazilian Courts Face Ransomware for Second Time in Recent Months*, BINARY DEF. (May 3, 2021), https://www.binarydefense.com/threat_watch/brazilian-courts-face-ransomware-for-second-time-in-recent-months/ [https://perma.cc/USY5-PH5K] (archived Aug. 13, 2022).

20. See 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> [https://perma.cc/DF45-WYT6] (archived Aug. 13, 2022).

21. See Vic Ryckaert, *Hackers Held Patient Data Ransom, So Greenfield Hospital System Paid \$50,000*, INDIANAPOLIS STAR (Jan. 17, 2018), <https://www.indystar.com/story/news/crime/2018/01/17/hancock-health-paid-50-000-hackers-who-encrypted-patient-files/1040079001/> [https://perma.cc/QY5F-PSBA] (archived Aug. 13, 2022).

Michigan,²² a courthouse in Texas,²³ and a port in California.²⁴ Even Lady Gaga is not immune.²⁵

The problem has become so profound that comedian John Oliver devoted a segment of *Last Week Tonight* to it, noting that the threat has gone from a “trickle to an absolute flood.”²⁶ Ransomware is growing not just in numbers, but also in severity. In 2016, hackers perpetrated roughly four thousand ransomware attacks a day worldwide, a figure which was already alarming.²⁷ By 2020, however, “attacks leveled out at 20,000 to 30,000 per day in the U.S. alone.”²⁸ That is a ransomware attack every eleven seconds,²⁹ each of which cost victims on average nineteen days of network downtime and a payout of over \$230,000.³⁰ In 2021, global costs associated with ransomware recovery exceeded \$20 billion.³¹ Some now predict that by 2031 ransomware will cost

22. See Khristopher J. Brooks, *Ransomware Attack Shuts Down Some Michigan Schools*, CBS NEWS (Jan. 2, 2020), <https://www.cbsnews.com/news/ransomware-attack-shuts-down-richmond-michigan-school-district/> [<https://perma.cc/4B56-G6ZE>] (archived Aug. 13, 2022).

23. See Travis Bubenik, *Hackers Target Texas Courts in Ransomware Attack*, COURTHOUSE NEWS SERV. (May 11, 2020), <https://www.courthousenews.com/hackers-target-texas-courts-in-ransomware-attack/> [<https://perma.cc/Z2L5-CACK>] (archived Aug. 13, 2022).

24. See Alfred Ng, *Ransomware attack hits Port of San Diego*, CNET (Sept. 28, 2018), <https://www.cnet.com/news/port-of-san-diego-hit-with-disruptive-ransomware-attack/> [<https://perma.cc/53QG-4BAU>] (archived Aug. 13, 2022).

25. See Daniel Kreps, *Celeb Law Firm Refuses Hacker Ransom as Lady Gaga Files Leak*, ROLLING STONE (May 15, 2020), <https://www.rollingstone.com/music/music-news/lady-gaga-hack-1000092/> [<https://perma.cc/PW2Y-LRNJ>] (archived Aug. 13, 2022).

26. For the full segment, see John Oliver, *Ransomware: Last Week Tonight*, HBO (Aug. 15, 2021), <https://www.youtube.com/watch?v=WqD-ATqw3js> [<https://perma.cc/8N64-UQTG>] (archived Aug. 24, 2022).

27. FED. BUREAU OF INVESTIGATIONS, HOW TO PROTECT YOUR NETWORK FROM RANSOMWARE 2 (July 14, 2016), <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> [<https://perma.cc/5K63-2GLB>] (archived Aug. 24, 2022).

28. David Corchado, *Why Ransomware Attacks Are on the Rise*, INVESTIS DIGIT. (May 19, 2021), <https://www.investisdigital.com/blog/technology/why-ransomware-attacks-are-rise> [<https://perma.cc/QA88-USUH>] (archived Aug. 24, 2022).

29. *Id.*

30. *Ransomware Demands Continue to Rise as Data Exfiltration Becomes Common, and Maze Subdues*, COVEWARE (Nov. 4, 2020), <https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report> [<https://perma.cc/4E87-R5QC>] (archived Aug. 24, 2022).

31. See Corchado, *supra* note 28; see also SOPHOS, THE STATE OF RANSOMWARE 2021 3 (Apr. 2021), <https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf> [<https://perma.cc/HY87-WTZK>] (archived Aug. 24, 2022) (noting that on average in 2021 “only 65% of the encrypted data was restored after the ransom was paid” and that the “average bill for rectifying a ransomware attack, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc. was US \$1.85 million”).

victims “around \$265 billion (USD) annually . . . with a new attack (on a consumer or business) every 2 seconds.”³²

This Article offers an account of the regulatory challenges associated with ransomware prevention. Situated within the broader literature on underenforcement, Part I of this article explores the core causes for the limited criminalization, prosecution, and international cooperation that have exacerbated this wicked cybersecurity problem. In particular, the Article examines the forensic, managerial, jurisdictional, informational, and resource allocation challenges that have plagued the fight against digital extortions in the global commons.

To address these challenges, Part II of the Article makes the case for the international criminalization of ransomware. Relying on existing international regimes—namely, the 1979 Hostage Taking Convention, the 2000 Convention Against Transnational Crime, and the customary prohibitions against the crimes of Piracy and Terrorism—the Article makes the claim that certain types of ransomware attacks are already criminalized under existing international law. In fact, the Article draws on each of these case studies to portray the criminalization of ransomware as a “fourth generation” in the outlawry of *Hostis Humani Generis* (enemies of mankind).

Finally, Part III of the Article demonstrates the various opportunities that could arise from treating ransomware gangs as international criminals subject to universal jurisdiction. The Article focuses on three immediate consequences that could arise from such internationalization: (1) expanding policies for naming and shaming harboring states, (2) authorizing extraterritorial cyber enforcement and prosecution, and (3) advancing strategies for strengthening cybersecurity at home.

II. THE PROBLEM OF RANSOMWARE

A. *Defining Ransomware*

Ransomware is a type of malware that targets data with the intention of either rendering that data permanently inaccessible through encryption or threatening further disclosure unless a ransom is paid.³³ The propagation methods of ransomware vary from

32. David Braue, *Global Ransomware Damage Costs Predicted to Exceed \$265 Billion By 2031*, CYBERCRIME MAG. (June 2, 2022), <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/> [https://perma.cc/7KEN-ANVK] (archived Aug. 24, 2022).

33. See Lawrence J. Trautman & Peter C. Ormerod, *Wannacry, Ransomware, and the Emerging Threat to Corporations*, 86 TENN. L. REV. 503, 505–06 (2019) (explaining how the WannaCry virus “operates by encrypting a victim’s data and demanding payment of a ransom in exchange for data recovery”).

compromised mobile applications to infected websites or email attachments.³⁴ Of late, a significant number of attacks have taken place via “remote desktop protocol . . . that do[es] not rely on any form of user interaction.”³⁵

The hackers typically demand payments in cryptocurrencies as they are less regulated and harder to control using existing Anti-Money-Laundering laws.³⁶ In particular, the application of “Know Your Customer” and other “Customer Identification Procedures” is complicated by the decentralization and anonymization associated with these digital coins.³⁷

Ransom attacks come with deadlines. “If the victim decides to break the deadline, attackers either increase the price or delete the decryption key.”³⁸ Moreover, paying the ransom may not necessarily end the operation. “Some programs also infect other devices on the network, enabling further attacks. Other examples of ransomware also infect victims with malware, such as Trojans that steal login credentials.”³⁹

According to British-based security software and hardware company SOPHOS, “[i]n 2021, 46% of organizations that had data

34. See FED. TRADE COMM’N, CYBERSECURITY FOR SMALL BUSINESS: RANSOMWARE,

https://www.ftc.gov/system/files/attachments/ransomware/cybersecurity_sb_ransomwar_e.pdf (last visited Aug. 23, 2022) [<https://perma.cc/8EB6-MBZU>] (archived Aug. 24, 2022) (detailing the various methods in which a criminal can start a ransomware attack).

35. Alexander S. Gillis & Ben Lutkevich, *Definition: Ransomware*, TECHTARGET, <https://www.techtarget.com/searchsecurity/definition/ransomware> (last visited Aug. 23, 2022) [<https://perma.cc/JLZ8-56TG>] (archived Aug. 24, 2022). Noting further that attackers may use one of four different “approaches” in the conduct of their ransomware operations: (1) “Encrypting Ransomware” is the classic “data kidnapping attack” where the negotiations and digital currency extortion revolve around access to the encryption keys to decrypt the data; (2) Screen Locking Ransomware involves locking users outside of their computers, where unlocking will depend on the payment of ransom; (3) “Doxfare” ransomware involves threatening to publish data unless ransom is paid; (4) “Scareware” ransomware involves the generation of an endless cycle of pop-up notifications that prevent access to the computer or its data. The only way to stop the generation of new pop-ups is by the payment the ransom. Each of these four attack approaches can be executed on mobile devices instead of regular computers. *Id.*

36. See generally VANSA CHATIKAVANI, MATTHEW DAVIE, JOSE FERNANDEZ DA PONTE, BRAD GARLINGHOUSE, YUSUF HUSSAIN, PAUL MALEY & SEBASTIAN SERRANO, WORLD ECON. F., NAVIGATING CRYPTOCURRENCY REGULATION: AN INDUSTRY PERSPECTIVE ON THE INSIGHTS AND TOOLS NEEDED TO SHAPE BALANCED CRYPTO REGULATION (Sept. 2021), https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf [<https://perma.cc/5MP9-BYVF>] (archived Aug. 24, 2022).

37. See generally *id.*

38. Andreja Velimirovic, *Ransomware Types and Examples*, PHOENIXNAP (Jan. 13, 2021), <https://phoenixnap.com/blog/ransomware-examples-types> [<https://perma.cc/6EU7-JLWF>] (archived Aug. 24, 2022).

39. *Id.*

encrypted in a ransomware attack paid the ransom.”⁴⁰ Of those who paid, “11% of organizations said they paid ransoms of \$1 million or more.”⁴¹ Each of these payments helps fuel the criminal enterprise behind ransomware, thereby inviting further attacks. The unfortunate reality is that for each individual victim, payment makes financial sense, even if that means off-loading costs and forcing negative effects on society writ large.

Ransomware attacks are targeting every industry and walk of life, from law firms to hospitals to academic institutions to insurance companies to police departments. But ransomware is even a bigger problem than that. Recently, ransomware gangs have begun targeting private individuals and small mom-and-pop shops.⁴² In the words of John Oliver, ransomware is now “so pervasive that it’s affecting pipelines and grandmothers.”⁴³ Generally speaking, hackers try to focus their efforts on victims who share two common features: first, they lack expertise and resources to ensure effective cybersecurity hygiene; and second, they have inherent incentives to end business interruptions quickly and bring operations back online.⁴⁴

The European Union Agency for Cybersecurity (ENISA) noted in its 2021 annual threat landscape report that “the frequency and the complexity of ransomware increased . . . and became one of the greatest threats that organisations face today regardless of the sector to which they belong.”⁴⁵ In fact, ENISA went further to suggest that we are now living through the “golden era of ransomware,” that it “has become a national security priority,” and that it has “not yet reached the peak of its impact.”⁴⁶

40. Sally Adam, *The State of Ransomware 2022*, SOPHOS NEWS (Apr. 27, 2021), <https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/> [<https://perma.cc/LZ6Y-RLRL>] (archived Aug. 24, 2022). SOPHOS’s study is based on a survey of 5,600 IT professionals from 31 countries. *Id.*

41. *Id.*

42. See SOPHOS, *THE STATE OF CONSUMER HOME CYBERSECURITY 2021* 10 (July 2021), <https://www.sophos.com/en-us/medialibrary/pdfs/consumer/sophos-the-state-of-consumer-home-cybersecurity-2021.pdf> [<https://perma.cc/HN55-QUUZ>] (archived Aug. 24, 2022) (noting that “nearly 1 in 5 consumers have firsthand experience with ransomware” and that the majority of ransomware attacks targeting private individuals occurred in the Northeast).

43. Oliver, *supra* note 26.

44. See generally Danny Palmer, *Ransomware: Over Half of Attacks Are Targeting These Three Industries*, ZDNET (Jan. 31, 2022), <https://www.zdnet.com/article/ransomware-over-half-of-attacks-are-targeting-these-three-industries/> [<https://perma.cc/3G78-TK45>] (archived Aug. 24, 2022) (noting that the banking, utilities, and retail industries are particularly vulnerable, but that all industries are ultimately “at risk from attacks”).

45. EUROPEAN UNION AGENCY FOR CYBERSECURITY, *ENISA THREAT LANDSCAPE 2021: APRIL 2020–MID-JULY 2021* 25 (Ifigenia Lella et al. eds., 9th ed. 2021).

46. *Id.*

B. Existing Regulation and its Limits

Considering this evolving threat environment, it is concerning to realize just how fragmented and patchy global and domestic regulatory responses have been so far. In this subpart I will examine both existing domestic laws within the United States (the primary target of ransomware attacks⁴⁷) as well as public international law.

1. Domestic Law

Within the limits of this Article, I am unable to offer a complete account of all the domestic mechanisms within the United States to regulate and enforce against ransomware. Instead, I wish to highlight two key concerns: (a) patchy and nonuniform state legislation; and (b) ad hoc and indecisive federal enforcement. Combined, these two factors generate an environment within which ransomware gangs continue to thrive.

a. Patchy and Nonuniform State Legislation

A handful of states have adopted legislation that criminalizes aspects of ransomware. For example, § 523 of the California Penal Code makes it a punishable offence to “introduce ransomware into any computer, computer system, or computer network” where the intent is to “extort property or other consideration from another” and where “such property or other consideration were actually obtained.”⁴⁸ Compare the California statute with § 33.023 of the Texas Penal Code. In Texas it is a crime if a person “introduces ransomware onto a computer, computer network, or computer system through deception and without a legitimate business purpose.”⁴⁹ Notice the difference between the two statutes. Whereas in Texas it is generally sufficient to merely “introduce” the ransomware malware to a device, in California the requirements are far more stringent, requiring both an “intent to

47. See Kate Birch, *US and Canada Among Countries Most Attacked by Ransomware*, BUS. CHIEF (Nov. 15, 2021), <https://businesschief.com/technology-and-ai/us-and-canada-among-countries-most-attacked-ransomware> [<https://perma.cc/UC2U-RG2D>] (archived Aug. 24, 2022) (“Research by NordLocker has found the United States is the leading country hit by ransomware attacks in 2020 and 2021, with Canada coming third, behind the UK. The researchers looked at 1,200 companies targeted by 10 of the leading ransomware gangs.”).

48. CAL. PENAL CODE § 523. The Law defines “ransomware” as “a computer contaminant . . . or lock placed or introduced without authorization into a computer, computer system, or computer network that restricts access by an authorized person to the computer, computer system, computer network, or any data therein under circumstances in which the person responsible for the placement or introduction of the ransomware demands payment of money or other consideration to remove the computer contaminant, restore access to the computer, computer system, computer network, or data, or otherwise remediate the impact of the computer contaminant or lock.” *Id.*

49. TEX. CRIM. STAT. ANN. § 33.023.

extort” and actual acquisition of “property or other consideration” because of the extortion. These differences are significant as they generate real gaps in the way the crimes are defined and could be ultimately enforced across states.⁵⁰

Moreover, all fifty states have data breach notification laws that require the communication of data breach events to relevant state supervisory authorities, and in certain cases to impacted consumers. Reporting requirements, however, differ at the state level. The specific terminology around what constitutes a triggering event could result in ransomware attacks being excluded or included in the definition of a data breach. This is especially true where the ransomware attack did not involve the exfiltration of data or other forms of unauthorized acquisition or access (recall that in traditional data encryption cases, the hacker does not actually access or acquire the files, which remain on the original computer; the hacker merely locks those files with an encryption key).⁵¹

States are also the primary regulators of insurance law. So far, only one state insurance regulator—New York—has attempted to regulate cyber insurers on ransomware issues. On February 4, 2021, the New York Department of Financial Services, led by Superintendent Linda Lacewell, introduced the first state-wide cyber insurance regulation in the United States.⁵² The circular had only one specific requirement: that policyholders notify law enforcement for ransomware attacks.⁵³ As I have written elsewhere, however,

50. For other parallel legislation, see W. VA. CODE §§ 61-3C-3 to 61-3C-4; WYO. STAT. ANN. §§ 6-3-506, 6-3-507.

51. Note, however, that at least in the context of Health Insurance Portability and Accountability Act (HIPAA) the U.S. Department Health & Human Services Office for Civil Rights (“HHS OCR”) issued a guidance in 2016. “Specifically, HHS OCR explained that when electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information).” Alan Brill, David White & Aravind Swaminathan, *Does a Ransomware Attack Constitute a Data Breach? Increasingly, It May*, KROLL (Jan. 19, 2021), <https://www.kroll.com/en/insights/publications/cyber/ransomware-attack-constitute-data-breach> [https://perma.cc/BCH9-92PP] (archived Aug. 18, 2022).

52. See Letter from Linda A. Lacewell, Superintendent, N.Y. State: Dep’t Fin. Servs., to all Authorized Property/Casualty Insurers (Feb. 4, 2021), https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02 [https://perma.cc/6VLW-4K76] (archived Aug. 18, 2022).

53. For a view that questions the efficacy of cyber insurance regulation of ransomware notifications and indemnification, see Erin Ayres, *Banning Ransom Payments a ‘Blunt, Potentially Ineffective’ Tool: Geneva Association*, FPN ADVISEN (July 25, 2022), https://www.advisen.com/tools/fpnproc/fpns/articles_new_35/P/439958803.html?rid=439958803&list_id=35 [https://perma.cc/CG38-E4NL] (archived Aug. 18, 2022) (quoting the Geneva Association, the international association for the study of insurance economics: “An outright ban on the payment of ransoms or their reimbursement by re/insurers could backfire by driving transactions underground and encouraging ransomware attackers to engage in new, more malicious forms of extortion . . . The

one state regulator cannot tackle a collective action problem like this alone. The race to the bottom will continue if, outside the state of New York, a failure to notify will continue to be the norm. This is a matter better left to federal regulation, not state. The circular is also silent as to the entity to be notified or scope of notification. The reality is that the state is unable to actually enforce disclosure to federal law enforcement, over which it has no authority, nor can it be certain that the notification will be picked up and effectively handled once transmitted. A notification policy is only as good as the enforcement action that flows from it. As for local and state law enforcement, they are certainly in no position to manage the threat of global cybercrime and cyberwarfare, thereby highlighting the futility of notifying them.⁵⁴

Finally, States are also split in the way that they regulate public responses to ransomware attacks. North Carolina became the first State to pass legislation banning the payment of ransom by public entities, like state agencies, counties, and municipalities.⁵⁵ North Carolina further prohibited the act of negotiating with the hackers.⁵⁶ Florida passed similar legislation outlawing ransom payments.⁵⁷ But whereas North Carolina includes public school districts and universities in its list of public entities that are prohibited from paying ransom, Florida's law does not.⁵⁸ Similarly, and unlike North Carolina, Florida's law does not prohibit communications with hackers.⁵⁹ As some practitioners have noted,

[m]ore laws of this kind may be on the horizon as Pennsylvania and New York are considering similar mandates. Pennsylvania's proposed legislation would impose a tight time frame for agencies to report the ransomware attack to the appropriate state officials within two hours and it would ban the use of taxpayer money for ransomware payments, with the exception of certain circumstances where payment is authorized by the governor. New York's legislation, if enacted, would prohibit ransomware payments by not only public agencies, but also private companies.⁶⁰

State ransomware criminalization laws, data breach notification laws, cyber insurance regulations, and ransomware payment

absence of cyber insurance cover for extortion payments not only penalizes the insured, but also does nothing to address the growth of [Ransomware-as-a-Service], which has fueled ransomware attacks.”).

54. Asaf Lubin, *Insuring Evolving Technology*, 28(1) CONN. INS. L.J. 131, 161 (2021).

55. See Spencer Pollock & Kelly Campbell, *North Carolina Bans State Entities from Negotiating with Hackers - and Other States May Follow*, MCDONALD HOPKINS (June 9, 2022), <https://mcdonaldhopkins.com/Insights/June-2022/NC-bans-negotiating-with-hackers> [<https://perma.cc/S5AK-AYHY>] (archived Aug. 18, 2022).

56. See *id.*

57. See State Cybersecurity Act, FLA. STAT. § 282.318 (amended 2022).

58. See Elise Elam & Benjamin Wanger, *Florida Follows North Carolina in Prohibiting State Agencies from Paying Ransom*, BAKER HOSTETLER (July 19, 2022), <https://www.bakerdatacounsel.com/cybersecurity/florida-follows-north-carolina-in-prohibiting-state-agencies-from-paying-ransoms/> [<https://perma.cc/9C75-QL7>] (archived Aug. 18, 2022).

59. See *id.*

60. Pollock & Campbell, *supra* note 55.

prohibitions all vary drastically. Given that cyber harms and internet crimes know no territorial bounds, this patchwork of conflicting state responses has weakened the ability of the federal government and of each state to effectively address threats and mitigate harms.

b. Ad Hoc and Indecisive Federal Enforcement

The federal government has repeatedly recommended that ransom should not be paid,⁶¹ and even warned of sanctions where payments are done with knowledge of likely interference with established sanctions set out by the Department of Treasury.⁶² Yet, so far, the government has not enforced sanctions against such payments, even where local and state public entities were the ones behind the payment.⁶³ The FBI, for example, has treated the decision to pay the ransom as a legitimate business decision, noting further that a ban on

61. See e.g., CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, PROTECTING SENSITIVE AND PERSONAL INFORMATION FROM RANSOMWARE-CAUSED DATA BREACHES, https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf (last visited Sept. 21, 2022) [<https://perma.cc/2DU3-DTP3>] (archived Aug. 18, 2022) (noting that CISA “strongly discourages paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or may fund illicit activities. Paying the ransom also does not guarantee that a victim’s files will be recovered.”); see also David Bisson, *Mayors Say They’ll No Longer Pay Ransoms Connected to Security Events*, TRIPWIRE (July 12, 2019), <https://www.tripwire.com/state-of-security/security-data-protection/mayors-say-theyll-no-longer-pay-ransoms-connected-to-security-events/> [<https://perma.cc/BV9S-BB53>] (archived Aug. 18, 2022) (demonstrating that local government officials have also taken the position to not make ransom payments). The official non-partisan organization of cities with populations of at least 30,000 people has committed not to pay ransom in the case of a ransomware event. *Id.*

62. See generally OFF. OF FOREIGN ASSETS CONTROL (OFAC), U.S. DEPT OF TREASURY, UPDATED ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS (Sept. 21, 2021), <https://www.dwt.com/media/files/blogs/privacy-and-security-blog/2021/10/ofac-ransomware-sanctions-advisory.pdf> [<https://perma.cc/P2DD-Z4W6>] (archived Aug. 18, 2022). For an analysis of the limited impact that OFAC’s Guidance has had on deterring payments, see Kyle D. Logue & Adam B. Shniderman, *The Case for Banning (and Mandating) Ransomware Insurance*, 28(1) CONN. INS. L.J. 247 (2022); see also Michael T. Borgia & Dsu-Wei Yuen, *OFAC Makes Waves in Fight Against Ransomware, but Practical Effects Unclear*, DAVIS WRIGHT TREMAINE LLP (Oct. 1, 2021), <https://www.dwt.com/blogs/privacy--security-law-blog/2021/10/ofac-updated-ransomware-advisory> [<https://perma.cc/R6D4-SSN7>] (archived Aug. 18, 2022).

63. See Logue & Shniderman, *supra* note 62, at 300–01. The authors describe OFAC’s ban on payments as a “limited or contingent ban” that is “to date largely unenforced.” The authors cite OFAC’s “discretion in deciding whom to seek penalties against . . . [and] in deciding whether there has been a violation at all,” as one of the reasons for the limited effects of the ban. *Id.*

payments could have dramatic consequences.⁶⁴ As one FBI official noted in a statement to the US House Judiciary Committee, “if a company chooses to pay and they have now broken the law, then a cyber adversary has the ability to hold them accountable in the public’s eye and threaten them even more with a higher extortion.”⁶⁵

This sends mixed signals to the public and harms the ability to reduce the total amount of payments paid.⁶⁶ Moreover, due to the scale of harm, government is only able to respond to a fraction of actual cases, disincentivizing the public from communicating with law enforcement altogether.⁶⁷

This is not to suggest that there haven’t been successes. The new Department of Justice (DOJ) Digital Extortion task force has taken some noticeable public action. For example, in June 2021, the DOJ seized \$2.3 million in cryptocurrency paid to the ransomware extortionists Darkside, and, in November 2021, the DOJ seized an additional \$6 million in ransom payments to a pair of Russian and Ukrainian nationals who were behind the REvil ransomware.⁶⁸ Some praised what they called “coordinated anti-ransomware” by the federal government, which has in the latter part of 2021 produced evidence of “ransom payments clawed back, decryption keys obtained,

64. See Erin Ayers, *Banning Ransom Payments Would Worsen Extortion: FBI Official*, FPN ADVISEN (Apr. 4, 2022), https://www.advisen.com/tools/fpnproc/fpns/articles_new_35/P/427646848.html?rid=427646848&list_id=35 [https://perma.cc/63UV-PEZ2] (archived Aug. 18, 2022).

65. *Id.*

66. Most recently in the wake of the Colonial Pipeline ransomware attack, Anne Neuberger, the Deputy National Security Advisor for Cyber & Emerging Technologies, recognized that victims of ransomware “often face a very difficult situation, and they have to just balance the cost benefit when they have no choice with regards to paying a ransom.” It therefore did not condemn the Colonial Pipeline decision to pay \$5 million ransom one day after being hit with the attack. See Press Briefing by Jen Psaki, Press Secretary, Dr. Elizabeth Sherwood-Randall, Homeland Security Advisor and Deputy National Security Advisor & Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technologies, WHITE HOUSE (May 10, 2021), <https://www.whitehouse.gov/briefing-room/press-briefings/2021/05/10/press-briefing-by-press-secretary-jen-psaki-homeland-security-advisor-and-deputy-national-security-advisor-dr-elizabeth-sherwood-randall-and-deputy-national-security-advisor-for-cyber-and-emerging/> [https://perma.cc/W2AH-35PU] (archived Aug. 18, 2022).

67. See SIMON HANDLER, EMMA SCHROEDER, FRANCES SCHROEDER & TREY HERR, ATL. COUNCIL, COUNTERING RANSOMWARE: LESSONS FROM AIRCRAFT HIJACKING 10 (Aug. 26, 2021), <https://www.atlanticcouncil.org/wp-content/uploads/2021/08/IB-RANSOMWARE-3.pdf> [https://perma.cc/C6AU-6TW7] (archived Aug. 18, 2022) (“Ransomware payments cannot be considered in the binary—to ban or not to ban—because that action alone is both insufficient and potentially harmful. What is needed is to change the incentive structure of those targeted by ransomware, giving them more realistic alternatives.”).

68. See Rob Legare, Nicole Sganga & Jeff Pegues, *U.S. Seizes Over \$6 Million from Ransomware Attacks*, CBS NEWS (Nov. 8, 2021), <https://www.cbsnews.com/news/ransomware-attacks-united-states-6-million/> [https://perma.cc/8QEX-T79B] (archived Aug. 18, 2022).

communications infiltrated, [and] successful multi-national law enforcement efforts.”⁶⁹

The federal government has also relied on extraditions as a tool to bring cyber criminals to justice for ransomware attacks and related money-laundering. Relying on charges of wire fraud, access device fraud, and computer fraud, the government has been successful in reaching foreign hackers.⁷⁰ Maksim Berezan, for example, was extradited to the United States from Latvia and pleaded guilty to such charges in April 2021, after committing ransomware attacks “causing over \$53 million in losses.”⁷¹

Yet despite these examples and the general optimism associated with it, many acknowledge that “the sheer volume of attacks means a handful of prosecutions is unlikely to make a difference” as “the scheme is still too lucrative for criminals to give up.”⁷² Indeed, as one cybersecurity researcher noted, ransomware gangs “learn from others’ mistakes and improve their [operational security]” since ultimately, even as government works to shut them down, “they are here to stay.”⁷³

Against this backdrop of uncertain federal action and growing ransomware threats, private entities have begun to play a far more expansive role. Cybersecurity firms now offer ransomware negotiation services, and cyber commercial insurers connect victims to those firms as well as to data restoration and to PR companies, with the goal of reducing the total cost of each attack.⁷⁴ In other words, instead of

69. *Id.*

70. See, e.g., Conspiracy to Commit Access Device Fraud and Computer Intrusions, 18 U.S.C. § 371; Access Device Fraud, 18 U.S.C. § 1029; Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Wire Fraud Affecting Financial Institutions, 18 U.S.C. § 1343; Conspiracy to Commit Wire Fraud Affecting Financial Institutions, 18 U.S.C. § 1349.

71. *Cybercriminal Connected to Multimillion Dollar Ransomware Attacks Sentenced for Online Fraud Schemes*, U.S. DEP’T OF JUST. (Mar. 25, 2022), <https://www.justice.gov/usao-edva/pr/cybercriminal-connected-multimillion-dollar-ransomware-attacks-sentenced-online-fraud> [<https://perma.cc/BU9N-8PBS>] (archived Oct. 10, 2022); For another example, consider *Alleged Russian Cryptocurrency Money Launderer Extradited to United States*, U.S. DEP’T OF JUST. (Aug. 5, 2022), <https://www.justice.gov/opa/pr/alleged-russian-cryptocurrency-money-launderer-extradited-united-states> [<https://perma.cc/C6LW-BPKZ>] (archived Oct. 10, 2022) (describing a “defendant extradited from Greece to face charges stemming from the operation of BTC-e, an illicit bitcoin exchange alleged to have received deposits valued at over \$4 billion.” The BTC-e bitcoin exchange was utilized in many ransomware attacks).

72. *Id.*

73. *Id.*

74. See generally Zoe Kleinman, *Insurers Defend Covering Ransomware Payments*, BBC (Jan. 27, 2021), <https://www.bbc.com/news/technology-55811165> [<https://perma.cc/N5SJ-FYUM>] (archived Aug. 18, 2022) (explaining that insurers are now covering ransomware payments); Rachel Monroe, *How to Negotiate with Ransomware Hackers*, NEW YORKER (Mar. 31, 2021), <https://www.newyorker.com/magazine/2021/06/07/how-to-negotiate-with-ransomware-hackers> [<https://perma.cc/HZ6W-3L>]

working with law enforcement, the ineffectiveness of responses at the state and federal levels has generated new private markets for ransomware mitigation. These markets thrive on keeping the ransomware threat alive. They are not interested in its complete eradication, nor does their business model endorse a close partnership with state and federal agencies.

2. International Law

At the international level, primary principles and doctrines of international law—such as the rules concerning sovereignty, non-intervention, and the prohibition on the use of force—do not introduce meaningful prohibitions on ransomware attacks. This is because, under international law, there are high thresholds for a violation of any of these rules, and most criminal ransomware activities fall short of meeting those thresholds.

Most ransomware attacks do not constitute uses of force as defined under Article 2(4) of the United Nations Charter. To constitute a use of force, a cyberattack must, by its “scale and effects,” be comparable to a non-cyber kinetic use of force.⁷⁵ In other words, a cyberattack needs to parallel, in its scope and consequences, the kind of harms that may be generated by physical uses of force. Yet, most ransomware attacks only generate economic harms and thereby produce limited effects.

Similarly, most ransomware attacks do not violate the customary prohibition on intervention. The International Court of Justice *Nicaragua* decision defined an unlawful intervention as one that bears on “matters in which each State is permitted . . . to decide freely,”⁷⁶ such as “the choice of a political, economic, social, and cultural system, and the formulation of foreign policy.”⁷⁷ This first element is often referred to as the *domaine réservé* requirement (the “reserved domain” of core areas of state activity). Second, *Nicaragua* confirms that a state must be coerced to take the otherwise undesired choice.⁷⁸ Only coerced interventions are prohibited under the doctrine.

Ransomware attacks rarely constitute coercive intrusions into the *domaine réservé* of the state in which the target of the attack resides. Note that in the course of most ransomware operations, the targets are private individuals and companies, and no state is ever forced to act

JS] (archived Aug. 18, 2022). *But cf.* Carolyn Cohn, *Insurers Run from Ransomware Cover as Losses Mount*, REUTERS (Nov. 19, 2021), <https://www.reuters.com/markets/europe/insurers-run-ransomware-cover-losses-mount-2021-11-19/> [https://perma.cc/UH7G-AVAJ] (archived Aug. 18, 2022).

75. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 195 (June 27).

76. *Id.* ¶ 205.

77. *Id.*

78. *See id.*

“in an involuntary manner” or denied action it otherwise would have taken.⁷⁹ Even when the target is a public entity (say a police department or a public school), and where that entity is compelled to pay the ransom, such payment still falls short of a coercive intervention as the decision to pay is not one that may be said to fall within the *domaine réservé*. The ransomware will need to cause a disruption to political, social, or economic life with significant and direct consequences. Short of that, the intrusion on the state and the society is contained and limited and thereby does not rise to the level of an intervention.

As far as sovereignty is concerned, for ransomware to constitute an internationally wrongful act, it will first need to be attributable to a state with sufficient evidence (a challenge in and of itself).⁸⁰ After all, most ransomware gangs are criminal gangs and not organs of the state. The nexus between these gangs and the countries in which they operate is often ambiguous and hardly meets the strict tests of “direction and control” or “endorsement and acknowledgement” to result in effective attribution.⁸¹

Even more troubling, states fail to agree on the exact scope of application of sovereign equality in cyberspace, and, as such, the doctrine is unlikely to offer a meaningful constraint to ransomware currently. As summarized by Lieutenant Colonel Visger,

[b]y electing to treat sovereignty as a principle rather than as a substantive rule, the U.K. maintains that violations of sovereignty do not, on their own, constitute violations of international law. This position touched off the well-known debate surrounding sovereignty, with most states rejecting the U.K.’s position and

79. NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 317 (2d ed. 2017) [hereinafter TALLINN MANUAL 2.0].

80. See generally Kristen Eichensehr, *The Law & Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520 (2020); see also JOHN SAKELLARIADIS, ATL. COUNCIL, ISSUE BRIEF: BEHIND THE RISE OF RANSOMWARE 8 (2022), <https://www.atlanticcouncil.org/wp-sedcontent/uploads/2022/08/Behind-the-Rise-of-Ransomware.pdf> [https://perma.cc/CM6D-R5G2] (archived Aug. 10, 2022) (“[T]he fluidity, decentralization, and dynamism of the digital extortion market complicate the process of identifying individual ransomware actors. The relationships that characterize each ransomware group fluctuate constantly, with individuals moving between ransomware gangs, gangs purchasing tools and services from other criminals, and various groups contributing to different elements of an attack. The resulting complexity means that ‘it is often difficult to identify conclusively the actors behind a ransomware incident,’ as cybersecurity authorities in the United States, Australia, and the United Kingdom recently observed.”).

81. See G.A. Res. 56/83, ILC Articles on the Responsibility of States for Internationally Wrongful Acts, arts. 2, 8, 11 (Dec. 12, 2001).

concluding that a violation of sovereignty in fact violates a state's international law obligations.⁸²

Even if sovereignty was determined to be a standalone rule that may be violated, whether ransomware is a good candidate for such a violation is subject to skepticism. Are the actions of encrypting and demanding ransom, when conducted remotely over the internet, constitutive of a breach of territorial sovereignty? Do these acts interfere with or usurp inherently governmental functions? Do they cause physical damage, injury, or loss of functionality of the kind that could be said to trigger a sovereignty violation?⁸³ These are all hard questions of interpretation and application that lack international consensus.

Overall, the international legal rules governing cyberspace are “nascent and evolving.”⁸⁴ So far, states have not been willing to forego their own “freedom of action through the adoption or advancement of specific international law rules” that could constrain ransomware activity.⁸⁵ States prefer to operate in a seemingly lawless space for cyber activity, where every offensive and defensive action is presumed lawful, even if the consequence of that is the inability to regulate the use of these tools by adversaries to harm.

Even to the extent that the prohibition on the use of force, the prohibition on intervention, or the rules on sovereignty may be said to apply to a small group of particularly harmful and dramatic ransomware attacks, that would not be enough to address the overall issue. The majority of ransomware will remain outside of the scope of international regulation.

The same can also be said for certain tailored norms to regulate particularly heinous ransomware attacks. For example, some have proposed that a more limited rule may be said to evolve around banning ransomware attacks against critical infrastructure. The UN Group of Governmental Experts (UNGGE) adopted the norm that “[a] State should not conduct or knowingly support [information and communications technology] activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to

82. Mark Visger, *The International Law Sovereignty Debate and Development of International Norms on Peacetime Cyber Operations*, LAWFARE (July 12, 2022), <https://www.lawfareblog.com/international-law-sovereignty-debate-and-development-international-norms-peacetime-cyber-operations> [https://perma.cc/NMT7-6D5Q] (archived Aug. 10, 2022).

83. These questions are based on the Tallinn Manual's proposed tests for a sovereignty violation. See TALLINN MANUAL 2.0, *supra* note 79, at 20–21.

84. Gary Corn, *International Law's Role in Combating Ransomware?*, JUST SEC. (Aug. 23, 2021), <https://www.justsecurity.org/77845/international-laws-role-in-combating-ransomware/> [https://perma.cc/5DBZ-Y5R5] (archived Aug. 10, 2022).

85. *Id.*

provide services to the public.”⁸⁶ When President Biden met with President Putin in Geneva in June 2021, he gave Putin a list of sixteen critical infrastructure entities that were “off limits” to Russian cyberattacks.⁸⁷ In so doing, the administration certainly echoed the UNGGE report. At the same time, however, the policy does not constitute a complete ban of ransomware. By saying that certain ransomware attacks were “off limits,” the reverse would also be true, that the other ransomware attacks are “within bounds” and tolerable. That is a grotesque reality and one that only serves to further cement the practice of ransomware across most industries and against most victims.

A similar approach was taken by the Oxford Statement on the Regulation of Ransomware Operations.⁸⁸ The statement, produced by international legal experts under the auspices of the Oxford Institute for Ethics, Law & Armed Conflict, notes that “there is no space for ransomware in a healthy, peaceful, and prosperous international community.”⁸⁹ At the same time, the statement stops short of outlawing ransomware *ipso facto* as *malum in se* (evil in itself by that very fact). Instead, much like the Biden administration, the statement prohibits only those ransomware attacks that “result in violations of human rights,” “amount to a prohibited threat or use of force,” “violate the principles of sovereignty or non-intervention,” or “are contrary to the rights of other States.”⁹⁰ In other words, it is not the act of ransomware that by itself results in an illegality; instead the wrongfulness of the ransomware is determined by its nature, scale, and consequences on a case-by-case basis (taking into account various general principles of international law).⁹¹

In conclusion, even the most expansive interpretations of existing international law generate a patchwork of norms that, at best, could

86. Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, transmitted by Letter dated 26 June 2015 from the Secretary-General to the General Assembly, 8, U.N. Doc. A/70/174 (July 22, 2015).

87. Morgan Phillips, *Biden Gave Putin List of 16 Critical Infrastructure Entities ‘Off Limits’ to Cyberattacks*, FOX BUS. (June 16, 2021), <https://www.foxbusiness.com/politics/biden-putin-critical-infrastructure-entities-off-limits-cyberattacks> [https://perma.cc/F3BY-LQE7] (archived Aug. 12, 2022).

88. Full disclosure, the author was involved in the drafting of the statement and ultimately signed it once published, though disagreed with the drafters on its language.

89. Dapo Akande, Antonio Coco, Talita de Souza Dias, Duncan B. Hollis, James C. O’Brien & Tsvetelina van Benthem, *Oxford Statement on International Law Protections in Cyberspace: The Regulation of Ransomware Operations*, JUST SEC. (Oct. 4, 2021), <https://www.justsecurity.org/78457/oxford-statement-on-international-law-protections-in-cyberspace-the-regulation-of-ransomware-operations/> [https://perma.cc/ZUJ7-UGXH] (archived Aug. 12, 2022).

90. *Id.*

91. *See id.* Ultimately, the Oxford Statement puts forward merely a “vision” and calls on States to “fully commit” to that vision. States have yet to have done so publicly, leaving international law on ransomware in a vague and peculiar position.

be said to constrain a handful of severe ransomware attacks while leaving the rest untouched and unconstrained.

C. *The Causes of Ransomware Underenforcement*

This subpart will explain the root causes for ransomware underenforcement under both domestic and international law. This subpart builds on Peter Swire's excellent theoretical mapping in his 2009 article "No Cop on the Beat."⁹² For the purposes of this subpart, I define underenforcement as a situation involving "a weak state response to lawbreaking as well as to victimization."⁹³ I conclude that there are five primary causes that generate an underenforcement "wicked problem" for ransomware:⁹⁴ (1) information asymmetries, (2) clashing jurisdictions, (3) the tragedy of the commons, (4) managerial deficits, and (5) forensic and diplomatic challenges.

To provide context for each of the five challenges this paper will rely on a typical ransomware scenario: Ransomware Gang R1 is located in Country R and conducts operations against local business in countries V and H. Victims V1, V2, V3 and H1, H2, H3 all suffer significant business interruption and loss of revenue. V1 and H1 both have a cyber insurance policy provided by VI and HI respectively. The law enforcement agencies in V and H (VLE and HLE) are charged with the mandate of preventing and mitigating cybercrime.

1. Information Asymmetries

There are currently no obligations to share information about ransomware under domestic law across multiple information sharing lines. Victims are not required to share information with one another either domestically (V1 to V2) or internationally (V1 to H1); V1 is not required to share information with V2 (let alone H1). Similarly, victims have no obligation to share information with law enforcement either domestically (V1 to VLE) or internationally (V1 to HLE).⁹⁵ If the

92. See generally Peter P. Swire, *No Cop on the Beat: Underenforcement in E-Commerce and Cybercrime*, 7 J. TELECOMM. & HIGH TECH. L. 107 (2009) (discussing the difficulty of determining "definite and objective answers" to and descriptions of social and policy problems, namely the enforcement of "e-commerce, cybercrime and Internet harms").

93. Alexandra Natapoff, *Underenforcement*, 75 FORDHAM L. REV. 1715, 1717 (2006).

94. See Horst W. J. Rittel & Melvin M. Webber, *Dilemmas in a General Theory of Planning*, 4 POL'Y SCIS. 155, 160–61 (1973) (describing the concept of "wicked problems." These are public policy problems that, unlike problems in math or chess, avoid straightforward articulation and deny simple or final solutions.).

95. A recent exception is the "Strengthening American Cybersecurity Act of 2022" which was passed in March 2022. S. 3600, 117th. Cong. (2022). The new legislation requires organizations deemed to operate critical infrastructure "must report

insurance policy is triggered, insurers are similarly not required to share information with other insurers again (say between VI and HI), nor with any law enforcement agency for that matter.⁹⁶

As Peter Swire notes in the context of cyber harms, when “the enforcement agency receives a complaint, there is no basis for knowing whether the perpetrator has harmed one victim (the local complainant) or numerous victims (who live predominantly in other jurisdictions).”⁹⁷ Moreover, the lack of reporting obligations and information sharing means that the broader national security community, including law enforcement agencies, is “unable to exploit the full range of capabilities and expertise” in their counter ransomware efforts.⁹⁸

2. Clashing Jurisdiction⁹⁹

Our perpetrators in the scenario are a gang of hackers located in country R far away from the victims (who are located in V and H). This generates geopolitical considerations that enhance the enforcement gap. As Bátorla and Harašta write,

[r]ansomware attacks were predominantly aimed at North American and European targets. Multiple sources described most ransomware attacks as originating from cybercriminals in Russia and other commonwealth of Independent States (CIS) countries – 15 of the 25 most important ransomware groups in mid-2021 were believed to be based there . . . Evidence suggests that these countries were unwilling to intervene as long as threat actors followed

ransomware payments within 24 hours” to CISA and must report any other cyber-attack “within 72 hours.” Graham Cluley, *US Legislation Brings Mandatory Cyberattack and Ransomware Reporting One Step Closer*, TRIPWIRE (Mar. 3, 2022), <https://www.tripwire.com/state-of-security/government/us-legislation-brings-mandatory-cyberattack-and-ransomware-reporting-one-step-closer/> [https://perma.cc/4JTF-WV5U] (archived Aug. 12, 2022). Notice, however, that this reaffirms the structure discussed above of sectoral protections for critical infrastructure, while no protections or obligations beyond critical infrastructure. For further analysis, see *id.* Another exception includes the above discussed state regulation of public responses to ransomware. Indeed North Carolina and Florida, both demand notification to state authorities and/or law enforcement whenever a ransomware attack takes place against state public entities. See *supra* notes 55–59 and accompanying text.

96. Recall the discussion above about the New York State Cyber Insurance regulation as one possible exception. See *supra* note 52 and accompanying text.

97. Swire, *supra* note 92, at 111.

98. S. REP. NO. 107-351, at 77 (2002) (explaining that, as the Senate Select Committee on Intelligence noted, dealing with transnational threats “requires close coordination and information sharing among and within the Intelligence Community agencies”).

99. Parts of this Section repeat analysis that I have argued elsewhere in Asaf Lubin, *The Prohibition on Extraterritorial Enforcement Jurisdiction in the Datasphere*, in *HANDBOOK ON EXTRATERRITORIALITY IN INTERNATIONAL LAW 1* (Austen L. Parrish & Cedric Ryngaert eds., forthcoming 2022).

basic precautions regarding local targets or helped state intelligence and [Law Enforcement Agencies].¹⁰⁰

When a country provides shelter to ransomware gangs and refuses to take enforcement action against them, that country abuses the sovereign privileges it enjoys. In other words, the act of sheltering is an act of extending jurisdictional protections to shield criminals from enforcement actions taken by victim states.¹⁰¹ International law is agnostic to the way sovereigns use (and misuse) these privileges. As was articulated by the Permanent Court of International Justice in the *Lotus* case in 1927: “[T]he first and foremost restriction imposed by international law upon a State is that—failing the existence of a permissive rule to the contrary—it may not exercise its power in any form in the territory of another State.”¹⁰²

Applying the *Lotus* case, the “most solid view” of international law is that any non-consensual access to data by a law enforcement agency that is “stored on a server located in the territory of another state constitutes a breach of the territorial integrity of that state.”¹⁰³ This view of the law has been endorsed by courts,¹⁰⁴ governments,¹⁰⁵

100. Michael Bátorla & Jakub Harašta, *Releasing the Hounds? Disruption of the Ransomware Ecosystem Through Offensive Cyber Operations*, in 14TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT: KEEP MOVING 93, 99 (2022) (listing CIS countries as including Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan).

101. See SAKELLARIADIS, *supra* note 80, at 9 (“Russian noncompliance with transnational cybercrime investigations exacerbates the natural hurdles involved in transnational law enforcement. For more than a decade, major cybercriminal networks have operated with impunity out of Russia. Mounting evidence suggests that many of these criminals purchase their immunity through cooperation with Russian intelligence and law enforcement agencies.”).

102. S.S. *Lotus* (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 18 (emphasis added).

103. Bert-Jaap Koops & Morag Goodwin, *Cyberspace, the Cloud and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law* 61 (Tilburg L. Sch. Legal Stud. Rsch. Paper Series, Working Paper No. 05/2016, 2014). In fact, the authors cite to a US attorneys manual to demonstrate that even more innocuous acts of remote evidence-gathering, like making a phone call or sending a letter, could be “considered a breach of sovereignty.” *Id.*

104. See, e.g., X, Re (2009), 2009 F.C. 1058, para. 40 (Can. Fed. Ct.); Weber & Saravia v. Germany, App. No. 54934/00 Eur. Ct. H.R. ¶¶ 1, 88 (2006).

105. A 2013 study by the UN Office of Drugs and Crime summarized the opinions of forty-seven responding states on a range of cybercrime issues. Two-thirds of the responders concluded that it would be “not permissible” for foreign law enforcement to “access computer systems or data” without relying on formal mechanisms for affirming consent, like an MLA process. Those countries explicitly cited “the principle of sovereignty” to justify their position. See U.N. OFF. DRUGS & CRIME, COMPREHENSIVE STUDY ON CYBERCRIME 220 (Feb. 2013) https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [<https://perma.cc/JA2E-CUZY>] (archived Aug. 14, 2022).

scholars,¹⁰⁶ and certain treaty regimes.¹⁰⁷ The logic behind this interpretation is quite clear: “It is universally recognized, as a corollary of state sovereignty, that officials of one state may not exercise their functions in the territory of another state without the latter’s consent.”¹⁰⁸

As a result of this, countries are constrained under doctrinal, positivist, and formalist views of international law from engaging in unilateral non-consensual cross-border cyber enforcement operations (including certain operations to seize cryptocurrency or unmask the location and identities of the ransomware gang members).¹⁰⁹ This includes the use of offensive cyber operations to disrupt the ransomware ecosystem (e.g., hacking back to servers and devices, collecting intelligence, and interfering with certain ransomware networks). At least one group of scholars believes that these operations have real-life impacts as they hit the bottom line of the ransomware groups by “imposing infrastructure recovery, internal security costs, loss of reputation, and even increased stress on members, staff dismissals, and groups disbanding altogether.”¹¹⁰

As all extraterritorial cyber enforcement actions are deemed illegal and a violation of international law under existing doctrinal understanding, then victim states are simply left paralyzed. The

106. See, e.g., Robert J. Currie, *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the “Next Frontier”?*, 54 CAN. Y.B. INT’L L. 1, 51 (2016) (concluding that, for the time being, states are still committed to a “Westphalian-bound model” that prohibits extraterritorial enforcement jurisdiction in cyberspace); Joachim Zekoll, *Jurisdiction in Cyberspace*, in BEYOND TERRITORIALITY: TRANSNATIONAL LEGAL AUTHORITY IN AN AGE OF GLOBALIZATION 341, 369 (Gunther Handl et al. eds., 2012) (“Disputes arising out of Internet activities are, for the most part, governed by traditional, state-based jurisdictional forces.”); Kevin Jon Heller, *In Defense of Pure Sovereignty in Cyberspace*, 97 INT’L L. STUD. 1432, 1464 (2021) (“[L]ow-intensity law-enforcement operations violate sovereignty simply because they involve penetrating a computer system located on the territory of another State.”); Stephen Allen, *Enforcing Criminal Jurisdiction in the Clouds and International Law’s Enduring Commitment to Territoriality*, in THE OXFORD HANDBOOK OF JURISDICTION IN INTERNATIONAL LAW 381, 409 (Stephen Allen et al. eds., 2019) (noting that “unilateral retrieval of data located within another state’s territory” is in “contravention of international law,” and further suggesting that any attempt to “bypass the territorial conception of enforcement jurisdiction by reference to exceptional grounds” is “unsustainable”).

107. The leading cybercrime treaty, the Council of Europe Convention on Cybercrime (or Budapest Convention) prohibits non-consensual transborder access to computer data, except in very limited scenarios. See Convention on Cybercrime art. 32, Nov. 23, 2001, 185 E.T.S. (entered into force July 1, 2004) [hereinafter Budapest Convention]. Note, however, that Article 39(3) confirms that the Convention does not affect other rights or restrictions, thereby opening the door for parallel evolution of customary practice around extraterritorial enforcement in cyberspace. See *id.* art. 39(3).

108. RESTATEMENT (THIRD) OF FOREIGN RELS. L. OF THE U.S. § 432, cmt. b (AM. L. INST. 1987) (suggesting further that the offended state may be entitled to seek certain reparation).

109. See Heller, *supra* note 103, at 1468 (“[A]ny remote penetration of a computer system, even penetration that does not cause any harm, violates the territorial sovereignty of the State in which the computer system is located.”).

110. Bátorla & Harašta, *supra* note 100, at 114.

harboring state may continue to harbor with impunity, and societies are forced to burden the cost of continued crime.¹¹¹

3. The Tragedy of the Commons

In social sciences Garratt Hardin's "tragedy of the commons" refers to a situation where individual users acting independently from one another operate solely on the basis of their personal interest against the common good. As was already suggested, given the magnitude of the ransomware problem, no one local entity can take this challenge alone. With limited prosecutorial resources, and where most victims and perpetrators are outside one's own jurisdiction, it is easy for enforcement agencies to kick the can down the road and drag their feet, hoping someone else will address the problem.¹¹² The shared resource of cyberspace is thus progressively polluted with hackers engaging in ransomware, with no one willing to invest in bringing an end to this menace. Peter Swire has demonstrated how the "someone else's problem" issue manifests in cyber enforcement cases to generate a commons problem:

Prosecuting the distant perpetrator will also be less of a priority as a matter of public choice—the enforcer will presumably get more credit locally when all of the victims are local, rather than bringing a case against a perpetrator who mostly harms individuals outside of the jurisdiction. Where enforcement is spread across many local jurisdictions, we thus would expect a classic commons effect: Rational local enforcers will focus on local effects, leading to underenforcement for the system as a whole.¹¹³

4. Managerial Deficits

Most law enforcement agencies lack the necessary personnel, administrative, and technical resources needed to respond to the ransomware challenge. I call this a "managerial deficit."

The last few years in ransomware operations saw the development of a business model centered around "ransomware-as-a-service"

111. *See id.* at 99.

112. *See* Cameron Bertron, *Answering the Call: Improving Local Police Response to Ransomware*, ALL FOR SECURING DEMOCRACY (Jan. 14, 2022), <https://securingdemocracy.gmfus.org/answering-the-call-improving-local-police-response-to-ransomware/> [<https://perma.cc/VE75-TJJB>] (archived Aug. 16, 2022) (describing a study in which researchers "called local police in the most populous city in all 50 states" asking for information about how to respond to a ransomware incident. The research indicated that "most local agencies do not have a clear or codified response strategy to ransomware . . . Overall, the responses seemed improvised and erratic. These results point to a lack of clarity and communication at higher levels of law enforcement as to who deals with ransomware and cybercrime more broadly. Responses are bound to remain inconsistent in the absence of direct guidelines for operators and officers. Without a clear chain of command for ransomware cases, both local law enforcement and victims are in the dark.").

113. Swire, *supra* note 92, at 113.

(RaaS).¹¹⁴ RaaS is an established industry within the ransomware business, in which operators “will lease out or offer subscriptions to their malware creations to others for a price—whether this is a per month deal or a cut of any successful extortion payments.”¹¹⁵ RaaS allows for increasing the scale of crime. Hackers do not need to develop their own criminal platforms anymore. They can merely purchase minutes on existing RaaS platforms to target hundreds of victims at once, knowing that at least some will pay.¹¹⁶ This is combined with underground forums on the DarkNet. These forums help “lower the entry bar” and provide “social and market infrastructure for cybercrime communities, including advertising, sales of initial accesses, recruitment and exchange of information, intrusion tools, and expertise.”¹¹⁷ Unlike the use of private messaging apps, these forums allow for “scale, accessibility, inherent trust, and reputation mechanisms, such as limited or invite-only access, escrow services, ‘karma’ systems based on activity (e.g., number of posts, transactions, cryptocurrencies deposited) or user recommendations.”¹¹⁸

Considering the lucrative nature of RaaS and the difficulty of tracking down and prosecuting operators, it should come as no surprise that law enforcement is facing a scalability problem. VLE and HLE, in our hypothetical story, do not have the necessary resources to simultaneously address hundreds of crimes all happening at once. So, while crime has scaled up, responses to it have not.¹¹⁹ As a result, often victims call law enforcement and get only limited and partial assistance to their problems.¹²⁰ They are therefore not incentivized to

114. CONG. RSCH. SERV., RANSOMWARE AND FEDERAL LAW: CYBERCRIME AND CYBERSECURITY 5 (2021), <https://crsreports.congress.gov/product/pdf/R/R46932> [<https://perma.cc/5TP5-T3DU>] (archived Aug. 16, 2022).

115. Charlie Osborne, *Ransomware in 2022: We're All Screwed*, ZDNET (Dec. 22, 2021), <https://www.zdnet.com/article/ransomware-in-2022-were-all-screwed/> [<https://perma.cc/2ZX3-P8HT>] (archived Aug. 16, 2022).

116. See SAKELLARIADIS, *supra* note 80, at 6 (“Increasing specialization across different stages of the ransomware life cycle also is evident in the growth of the ransomware-as-a-service model (RaaS). In a RaaS structure, a core group of criminals manage a ransomware payload, while outsourcing ransomware deployment to so-called ‘affiliates.’ The model has the dual benefit of allowing ransomware groups to scale their operation and to off-load risk, with affiliates now drawing increasing attention from law enforcement. According to an interview given by a member of the REvil ransomware gang, the group at one point had sixty affiliates carrying out attacks on its behalf. As of October 2021, eight of the ten leading ransomware groups employed an affiliate model to carry out attacks.”).

117. Bátorla & Harašta, *supra* note 100, at 98.

118. *Id.*

119. See *supra* note 109 and accompanying text.

120. *Id.* In fact, as part of the study multiple police departments “were unsure of their answer or googled what the police response should be” when confronted with a phone call asking for advice in the wake of a ransomware incident. An additional group of law enforcement first responders didn’t even know what ransomware was. One agent went as far as to suggest that “ransomware was not a matter for law enforcement.” *Id.*

communicate with law enforcement in the future—enhancing the informational asymmetry even further.

5. Forensic and Diplomatic Challenges

Challenges in evidence gathering, attribution issues, and the varying degrees of technological sophistication and literacy possessed by law enforcement have also complicated the ability to respond to this crime effectively. The duality of this threat—having the appearance of a national security problem (that can only be addressed by national security authorities and frameworks) but having local impacts as a domestic crime—is what makes this a unique threat.

This is not the first time that the United States faces a threat that blurs the line between national security and domestic crime. Consider, for example, the long period during the 1980s of kidnappings of CEOs of American companies in Latin-America. Ed Meese, then the Attorney General of the United States, was considering a ban on kidnapping and ransom insurance as some argued that the “presence of insurance actually increases the probability of kidnapping.”¹²¹ Ultimately, Meese decided not to ban the program, as he worried that a ban would disincentivize “contact with law enforcement.”¹²² This is because indemnification under the policies depended on notification to the FBI. In fact, insurers turned to the FBI to negotiate with the kidnappers and diplomatically work with the relevant foreign countries to ensure the safe release of the kidnapped.¹²³ In other words, the forensic and diplomatic challenges meant that victims and insurers were encouraged to work with law enforcement to resolve these crises.

The ransomware problem is one that no longer mandates that victims and their insurers go through the government. Whereas physical kidnappings mandated inter-governmental coordination to assist in the release and recovery efforts, when everything is digital, and all that is kidnapped is data, there is no physical element that necessitates the role of government for crisis management. Into this fray enter private security start-ups led by former US intelligence and cyber professionals, who bring with them the same national security expertise that was once within the complete monopoly of the government.¹²⁴ The result is that insurance policies no longer demand

121. Gideon Parchomovsky & Peter Siegelman, *The Paradox of Insurance*, FAC. SCHOLARSHIP AT PENN CAREY L. 1, 5 (2020), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3160&context=faculty_scholarship [https://perma.cc/C9V5-L92P] (archived Aug. 16, 2022).

122. Richard J. Aldrich & Lewis Herrington, *Secrets, Hostages and Ransoms: British Kidnap Policy in Historical Perspective*, 44(4) REV. INT'L STUD. 738, 756 (2018).

123. *See id.*

124. *See* Richard Byrne Reilly, *Born in the NSA!*, VENTURE BEAT (May 1, 2014), <https://venturebeat.com/2014/05/01/born-in-the-nsa-former-spies-are-starting->

notification to law enforcement or collaboration with the government, further exacerbating the informational asymmetries discussed above. VI and VII can work together at the exclusion of the government and thereby at the exclusion of public policy.

These five challenges all demonstrate the need to develop international and transnational responses to ransomware. Such responses could more effectively address the scalability problems, commons and jurisdictional concerns, and informational gaps identified. The next Part will begin to sketch possible models for such intranational regulation.

III. REDEFINING THE CRIME OF RANSOMWARE

A. *Ransomware and the Outlawry of Hostis Humani Generis*

In the lead-up to Russia's war of aggression against Ukraine, President Biden had a rhetorical gaffe, when he tried to distinguish between a "minor incursion" by Russia into Ukraine and "more severe incursions."¹²⁵ Part of what triggered the international community's dismay of Biden's statement was the fact that aggression is an internationally recognized crime. Under UNGA Resolution 3314, "[a] war of aggression is a crime against international peace"¹²⁶ and "no territorial acquisition or special advantage resulting from aggression is or shall be recognized as lawful."¹²⁷ The consequence of that is that "[n]o consideration of whatever nature, whether political, economic, military or otherwise, may serve as a justification for aggression."¹²⁸

Aggression is *malum in se* (evil by itself). It is defined by a baseline of illegality. It is not the only crime of its kind. There are other international delinquencies which have been outlawed by the international community due to their unique nature. We may be able to speak of three generations of such crimes:

Generation 1: piracy on the high seas and the slave trade

Generation 2: hostage taking and aerial hijacking

Generation 3: organized transnational crime and terrorism

companies-all-over/ [https://perma.cc/YH3D-BNAG] (archived Aug. 16, 2022) (citing a former NSA operative who suggested that between "40 to 50 percent of U.S. security IT startups are launched by former NSA staffers").

125. See Tracy Wilkinson, *Biden's 'Minor Incursion' Comment Roils Diplomatic Efforts to Halt Russian Invasion of Ukraine*, L.A. TIMES (Jan. 20, 2022), <https://www.latimes.com/politics/story/2022-01-20/bidens-minor-incursion-comment-roils-diplomatic-efforts-to-halt-russian-invasion-of-ukraine> [https://perma.cc/C2H6-JTZN] (archived Aug. 16, 2022).

126. G.A. Res. 3314 (XXIX), Definition of Aggression, art. 5(2) (Dec. 14, 1974).

127. *Id.* art. 5(3).

128. *Id.* art. 5(1).

Maritime piracy, hostage taking, aerial hijacking, organized transnational crime, terrorism, and now ransomware share a number of core features: (1) all are threats to the intranational movement of goods, services, and persons; (2) all depend on domestic legal systems to prosecute offenders; (3) all have transnational components that expand beyond the purely domestic environment of one state and complicate reliance on national prosecutions; (4) all involve offences against core human and universal values of freedom; (5) all involve relatively low costs to perpetuate the assaults; and (6) all generate massive victimization on scale due to the indiscriminate nature of the attacks, thereby shocking the conscience of the international community.¹²⁹

It is in this sense that the international criminalization of ransomware can naturally derive its legitimacy and internal logic from the three generations that preceded it and become a sort of fourth digital generation of the international criminalization and outlawry of these “enemies of mankind” (*hostis humani generis*).¹³⁰ In fact, it would seem to be true that in all the previous generations that came before it, “the concerted action taken by the global community to suppress these crimes” demonstrated the very power and reach of the “international legal order.”¹³¹ By traveling through time, one can anchor ransomware prevention strategies to other previously tried and recognized frameworks. Learning from the past and contemporary history of the various generations of *hostis humani generis* crimes and their outlawry is crucial for regulators. It allows us to gain new understandings and insights about an emerging crime based on parallel antecedents.

129. See NANCY DOUGLAS JOYNER, AERIAL HIJACKING AS AN INTERNATIONAL CRIME 263 (1974); see also Evan F. Horsley, *State-Sponsored Ransomware Through the Lens of Maritime Piracy*, 47 GA. J. INT'L & COMP. L. 669, 681 (2019) (“In many ways ransomware attacks are to the internet what pirates traditionally were to the seas . . . The world as a whole has an abundance of experience dealing with maritime piracy. The understanding that thousands of years of marine pillaging has given us, both in the form of our more traditional understandings and in the form of our modern-day approach, should guide us as we begin tackling the domain of cyberspace.”); HANDLER, SCHROEDER & HERR, *supra* note 67, at 10 (“Ransomware is not a new phenomenon. As with hijackings, addressing the root causes of ransomware requires a multifaceted approach, mixing active and passive measures to block the realization of value by criminal groups and deny groups their safe havens.”).

130. See *U.S. v. Yunis*, 924 F.2d 1086, 1091 (D.C. Cir. 1991) (citing the RESTATEMENT (THIRD) OF FOREIGN RELS. L. OF THE U.S. §§ 404, 423 (AM. L. INST. 1987)) (“Under the universal principle, states may prescribe and prosecute ‘certain offenses recognized by the community of nations as of universal concern, such as piracy, slave trade, attacks on or hijacking of aircraft, genocide, war crimes, and perhaps certain acts of terrorism,’ even absent any special connection between the state and the offense.”).

131. JOYNER, *supra* note 129, at 266.

B. *Outlawing by Extension and Analogy or by Treaty Design?*

Past scholarship is rich with examples demonstrating the connections between the different generations of crimes. The literature is filled with books that examine, for example, the nexus between aircraft hijacking and piracy,¹³² terrorism and piracy,¹³³ or terrorism and organized crime.¹³⁴ Reviewing this scholarship, and the relevant treatises and customs associated with those crimes, a set of requirements emerges. These “principles of outlawry” are common across all the generations of crime and must form part of any future outlawry of ransomware:¹³⁵

- (1) **Proclamation Principle:** the international character of the crime is proclaimed and justified, thereby elevating it to the status of an international crime.¹³⁶
- (2) **Criminalization Principle:** states are obligated to adopt clear legislation and other enforcement measures that impose under their domestic laws “heavy and effective penalties” against perpetrators and increase deterrence.¹³⁷
- (3) **Universal Jurisdiction Principle:** affirming the right of each state to apprehend the offender wherever they may be found and prosecute and punish them for the offence, irrespective of the place where the offence is committed or felt.
- (4) **Prosecute or Extradite Principle:** states are obligated to prosecute or extradite (*aut dedere, aut judicare*) offenders if they are found in their territory.
- (5) **Cooperation Principle:** states are obligated to cooperate and provide judicial assistance in all criminal matters relating to the offence.

In order to internationally criminalize ransomware, rule prescribers will need to engage in a process during which these

132. See, e.g., S.K. AGRAWALA, AIRCRAFT HIJACKING AND INTERNATIONAL LAW 73–74 (1973); JOYNER, *supra* note 129.

133. See generally, e.g., DOUGLAS R. BURGESS, THE WORLD FOR RANSOM: PIRACY IS TERRORISM, TERRORISM IS PIRACY (2010).

134. See generally, e.g., THE NEXUS BETWEEN ORGANIZED CRIME AND TERRORISM: TYPES AND RESPONSES (Letizia Paoli et al. eds., 2022).

135. See generally AGRAWALA, *supra* note 132, at 73–74; JOHN F. MURPHY, PUNISHING INTERNATIONALLY TERRORISTS: THE LEGAL FRAMEWORK FOR POLICY INITIATIVES (1985).

136. See AGRAWALA, *supra* note 132, at 74 (“[H]ijacking constitutes a crime against humanity as such hijackers are enemies of mankind, *hostis humani generis*. This crime constitutes an offence against a juridical value, human and universal, which characterizes the crime, *Juris gentium*, above any individual interest. And the fundamental characteristic of every offence *Juris gentium* is the obligatory punishment by all states, wherever the offence is committed.”).

137. See *id.* at 73.

principles will be adopted and recognized for the crime of ransomware. This process can occur in one of two ways: through a specialized regime (drafting and adopting a new international instrument for ransomware) or through an inductive process that builds on the existing instruments. Given the number of international treaties covering all the previous generational crimes, it may be possible to apply some of them by analogy and by extension to different categories of ransomware. This subpart explores each of these options.

1. New International Instrument

The 1960s and 1970s were a period of growth in the development of new treaties. In fact, in the days leading up to the adoption of the aerial hijacking conventions, drafters of those treaties strongly believed that the issue could not be sufficiently addressed through the formation of custom. They considered custom to be “too slow and burdensome for global security needs.”¹³⁸ It is for this reason that treaty-based instruments were favored. The conventions were seen as the speediest and most tailored mechanism to advance the rule of law and deter and defend against hostage taking in the air.

The world has sure changed since then, both in terms of the internal domestic politics within the United States and the broader strategic competition environment on the world stage. It is now considered practically impossible to imagine any international instrument developing, certainly not on a subject as sensitive as cybercrime, and certainly not at a time where Russia’s invasion of Ukraine has reinvigorated Cold War political antics.

Nonetheless, it is also true that on 27 December 2019, the UN General Assembly adopted Resolution 74/247 on “Countering the use of information and communications technologies for criminal purposes,” which set in motion a process to draft a global comprehensive cybercrime treaty.¹³⁹ On 26 May 2021, the UN General Assembly adopted Resolution 75/282, mandating the production of a complete draft and its delivery to the General Assembly in time for its seventy-eighth session (beginning in September 2023 and concluding in September 2024).¹⁴⁰

The planned convention is already facing opposition. Over forty digital rights organizations and experts warned that a proposed

138. JOYNER, *supra* note 129, at 264.

139. See G.A. Res. 74/247 (Dec. 27, 2019).

140. See G.A. Res. 75/282 (May 26, 2021). According to this resolution, the draft convention shall consider existing international instruments and efforts at the national, regional, and international levels on combating the use of information and communications technologies for criminal purposes. This includes the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime. See *id.*

convention poses a threat to human rights.¹⁴¹ The European data protection supervisor expressed concern that, if not specifically addressed, there is a “substantial risk that the final text of the Convention could lead to a weakening of the fundamental rights and freedoms of natural persons provided for by EU law, in particular their rights to data protection and privacy.”¹⁴² Others cited Russia’s leadership in promoting this treaty as proof of its improbability. These commentators suggest that it is “hard to see how Russia could engage in negotiations for a legally-binding cybercrime treaty in good faith. It’s harder still to see how it can negotiate at the United Nations for a treaty based on upholding state sovereignty while simultaneously invading a sovereign nation state”¹⁴³ (alluding to Russian invasion into and annexation of parts of Ukraine in 2022).

Even if the convention never materializes, the process of its development could serve a function of its own. The deliberations around the scope and text of the new treaty could become a diplomatic epicenter for conversations about norms of the kind this Article advocates for. Moreover, even if a comprehensive and universal regime is not in reach, a club model could offer an interim solution whereby the United States and the likeminded take the first step of introducing the intranational crime of ransomware, with the hope that the regime would ultimately be adopted by a sufficiently robust number of states.

2. Analogy and Extension

As was already alluded to, ransomware overlaps at least partially with several other crimes that are subject to treaty-based regulation. These include (1) the 1979 International Convention against the Taking of Hostages, (2) the 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, (3) the 1997 International Convention for the Suppression of Terrorist Bombings,

141. See Katitza Rodriguez & George Wong, *Letter to the United Nations to Include Human Rights Safeguards in Proposed Cybercrime Treaty*, ELEC. FRONTIER FOUND. (Feb. 27, 2022), <https://www EFF.org/deeplinks/2022/02/letter-united-nations-include-human-rights-safeguards-proposed-cybercrime-treaty> [https://perma.cc/S9LS-E8XM] (archived Aug. 24, 2022).

142. EUR. DATA PROTECTION SUPERVISOR, OPINION 9/2022 ON THE RECOMMENDATION FOR A COUNCIL DECISION AUTHORISING THE NEGOTIATIONS FOR A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES ¶ 12 (May 18, 2022), https://edps.europa.eu/system/files/2022-05/2022-05-18-opinion_on_international_convention_en.pdf [https://perma.cc/6ZZE-8MMZ] (archived Sept. 2, 2022).

143. Jeff Burt, *UN Mulls Russia’s Pitch for Cybercrime Treaty*, THE REG. (Mar. 7, 2022), <https://www.theregister.com/2022/03/07/russia-un-cybercrime-treaty/> [https://perma.cc/C8VB-M3UZ] (archived Aug. 24, 2022) (quoting Mercedes Page, Founder and CEO of Young Australians in International Affairs).

(4) the 1999 International Convention for the Suppression of the Financing of Terrorism, (5) the 2000 United Nations Convention against Transnational Organized Crime, (6) the 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing Convention), and (7) the 2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft.¹⁴⁴

Applying these treaties to ransomware could open the door to substantive enforcement opportunities. By selecting relevant provisions for strategic application,¹⁴⁵ new obligations may emerge to both constrain sheltering states and empower victim states. Options for litigation may also be generated. While providing a full exploration of each of the above listed treaties and frameworks is outside the scope of this Article, I will anecdotally examine a few to offer insight into the Article's proposed suggestion.

The International Convention Against the Taking of Hostages defines the act of "hostage taking" in Article 1. It reads,

[a]ny person who seizes or detains and threatens to kill, to injure or to continue to detain another person (hereinafter: referred to as the "hostage") in order to compel a third party, namely, a State, an international intergovernmental organization, a natural or juridical person, or a group of persons, to do or abstain from doing any act as an explicit or implicit condition for the release of the hostage commits the offence of taking of hostages ("hostage-taking") within the meaning of this Convention.¹⁴⁶

Note that the "Article makes no reference to the manner of seizure or detention,"¹⁴⁷ and that many instrumentalities short of the use of force that helps sustain the seizure or detention could "suffice to bring

144. International Convention Against the Taking of Hostages, Dec. 17, 1979, 1316 U.N.T.S. 205; Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Mar. 10, 1988, 1678 U.N.T.S. 222; International Convention for the Suppression of Terrorist Bombings, Dec. 15, 1997, 2149 U.N.T.S. 256; International Convention for the Suppression of the Financing of Terrorism, Dec. 9, 1999, 2178 U.N.T.S. 197; United Nations Convention Against Transnational Organized Crime, Nov. 15, 2000, 2225 U.N.T.S. 209; Convention for the Suppression of Unlawful Acts Relating to International Civil Aviation, Sept. 10, 2010, 50 I.L.M. 141; Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft, INT'L MARITIME ORG. (Oct. 14, 2005), <https://www.imo.org/en/About/Conventions/Pages/SUA-Treaties.aspx> [<https://perma.cc/2Y95-VPZT>] (archived Aug. 24, 2022).

145. See MICHAEL HEAD, CRIMES AGAINST THE STATE: FROM TREASON TO TERRORISM 275 (2011).

146. International Convention Against the Taking of Hostages, *supra* note 144, art. 1. As a matter of future law there is certainly a possibility for liberal-rule appliers to consider whether the capture of data should be seen as having similar characteristics as the detention of one's person. After all, some argue that our digital self is now an extension of our physical self. See, e.g., Russell W. Belk, *Extended Self in a Digital World*, 40(3) J. CONSUMER RSCH. 477 (2013).

147. JOSEPH LAMBERT, TERRORISM AND HOSTAGES IN INTERNATIONAL LAW: A COMMENTARY ON THE HOSTAGES CONVENTION 80 (1990).

the conduct within the scope of this Convention.”¹⁴⁸ If we return to our basic scenario, we can examine this test case by adjusting the facts ever so slightly. What if the attacked V1 was a hospital, and what if R’s ransomware attack locked a certain patient in the operating room, with the physicians outside of the room, unable to assist her. At this point, a ransomware could result in further delays in surgeries and ultimately can even lead to death.¹⁴⁹ Also consider the ransomware on Colonial Pipeline which resulted in significant gas shortages and multiple states issuing emergency proclamations.¹⁵⁰ What if hackers knew of the likely gas shortages and aimed their attack at restricting the movement of certain individuals. Or what if hackers targeted a plane, instead of a gas pipeline, forcing it to stay on the tarmac for hours with the passengers on board. The wording of Article 1 may extend to cover some resulting outcomes occurring from all of these scenarios. After all, clever litigators may try to argue that each scenario demonstrates a broader form of “detention” as used in Article 1.

Such an interpretation could have dramatic consequences because, under Article 16 of the International Convention Against the Taking of Hostages, disputes about the convention may be referred to the International Court of Justice (and as both the United States and Russia are parties to this treaty with no reservations, this could theoretically lead to a potential case in the future).

By way of a second analogy, compare the customary prohibition on terrorism with the crime of ransomware. “Terrorism” is defined as encompassing three key elements:

- (i) the perpetration of a criminal act (such as murder, kidnapping, hostage-taking, arson, and so on), or threatening such an act;
- (ii) the intent to spread fear among the population (which would generally entail the creation of public danger) or directly or indirectly coerce a national or international authority to take some action, or to refrain from taking it; and

148. *Id.* at 81.

149. See William Ralston, *The Untold Story of a Cyberattack, A Hospital and A Dying Woman*, WIRED (Nov. 11, 2020), <https://www.wired.co.uk/article/ransomware-hospital-death-germany> [<https://perma.cc/F3ZX-CEDN>] (archived Aug. 24, 2022); Kevin Collier, *Baby Died Because of Ransomware Attack on Hospital, Suit Says*, NBC NEWS (Sept. 30, 2021), <https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465> [<https://perma.cc/J9R2-KV83>] (archived Aug. 24, 2022).

150. See Sean Michael Kerner, *Colonial Pipeline hack explained: Everything you need to know*, TECHTARGET (Apr. 26, 2022), <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know> [<https://perma.cc/7WEB-ZJ82>] (archived Aug. 24, 2022).

(iii) when the act involves a transnational element.¹⁵¹

Under this definition, certain types of ransomware attacks may be considered a form of terrorism. Consider organized group R1 operating with some political motivations or ties to the intelligence apparatus of country R. If the attack is targeting a public utility (like a bank or railway company) with the knowledge that its business interruption will trigger fear amongst the population, there is certainly the possibility of defining the act as terrorism.

A final analogy could be found in the wording of the UN Convention Against Transnational Organized Crime. Article 2(a) defines an “organized criminal group” as

- (1) a group of three or more persons that was not randomly formed;
- (2) existing for a period of time;
- (3) acting in concert with the aim of committing at least one crime punishable by at least four years' incarceration;
- (4) in order to obtain, directly or indirectly, a financial or other material benefit.¹⁵²

This definition perhaps fits the best, as nearly all ransomware attacks are launched by gangs who will easily qualify as meeting these requirements.

A specialized international regime to regulate the crime of ransomware remains the best solution for ransomware's underenforcement problem. Nonetheless, given current political instability, it is very unlikely that a treaty on ransomware will be drafted and adopted in the near future. The three examples above hopefully show that there are other solutions to regulating ransomware, including by analogizing and extending the application of existing treaty and customary frameworks.

IV. BUILDING THE RANSOMWARE ENFORCEMENT TOOLKIT

This final Part of the Article will examine the implications of recognizing ransomware as an international crime. It will specifically

151. Prosecutor v. Ayyash, STL-11-01/1, Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, ¶ 85 (Feb. 16, 2011). It should be noted that there remains “to this day” a fierce debate about whether the definition of the crime of terrorism has reached a customary-agreed definition, the Ayyash decision notwithstanding. See Corman Kenny, *Prosecuting Crimes of International Concern: Islamic State at the ICC?*, 33 *UTRECHT J. INT'L & EUR. L.* 120, 131 (2017).

152. United Nations Convention Against Transnational Organized Crime, *supra* note 144, art. 2(a).

look at three areas of development that could assist in closing the ransomware underenforcement gap by directly addressing some of the root causes of ransomware, as mapped out in Part I. In particular, I will consider the following likely implications: (1) expanding policies for naming and shaming harboring states, (2) authorizing extraterritorial cyber enforcement and prosecution, and (3) advancing strategies for strengthening cybersecurity at home.

A. *Naming and Shaming Harboring States*

The problem faced by existing international bodies tasked with regulating cyberspace, like the UNGGE and the UN Open Ended Working Group, is that they have so far failed to generate a large enough consensus for their conclusions. Namely, these deliberations have failed to result in agreement on the specifics surrounding the application of each of the norms for responsible behavior in cyberspace.¹⁵³ Given that the crime of ransomware is likely to focus only on individuals and private gangs, it perhaps, if negotiated effectively, could be a low-hanging fruit for negotiating governments. This is because any criminalization is unlikely to prove an impediment to national cyber-related activities.¹⁵⁴

Furthermore, changing the terminology around ransomware from a domestic crime to an international delinquency—said in one breath alongside piracy, terrorism, and slavery—would have an expressive function.¹⁵⁵ It would raise the stakes in diplomatic negotiations and will help secure broader agreement between allies on the need for deterrence and enforcement strategies against states that turn a blind eye to ransomware.

Moreover, it will serve the function of “condemnation” within the broader cyber accusation theory as developed by Martha Finnemore

153. See generally Arindrajit Basu, Irene Poetranto & Justin Lau, *The UN Struggles to Make Progress on Securing Cyberspace*, CARNEGIE ENDOWMENT FOR INT'L PEACE (May 19, 2021), <https://carnegieendowment.org/2021/05/19/un-struggles-to-make-progress-on-securing-cyberspace-pub-84491> [https://perma.cc/K564-D8WA] (archived Aug. 24, 2022).

154. Cf. CHRISTOPHER J. D'URSO, NOWHERE TO HIDE: INVESTIGATING THE USE OF UNILATERAL ALTERNATIVES TO EXTRADITION IN UNITED STATES PROSECUTIONS OF TRANSNATIONAL CYBERCRIME 285 (2021) (unpublished Ph.D. dissertation, University of Oxford) (on file with author) (suggesting that “cybercrime is not likely to progress toward cooperation as occurred in the case of both terrorism and drug trafficking. With those offenses, host countries recognized the substantial domestic harms that the illicit conduct caused and were often eager to assist in handing over the perpetrators. Yet, cybercriminals know not to target their fellow citizens, engendering little, if any, domestic harms. This is precisely why certain states have turned to sponsoring such conduct rather than combatting it.”).

155. See generally Alex Geisinger & Michael Ashley Stein, *A Theory of Expressive International Law*, 60 VAND. L. REV. 77 (2007) (discussing the literature around the role of normative pressure in influencing rational actors to alter their behavior).

and Duncan Hollis.¹⁵⁶ In other words, it will bring shape and teeth to the “expression of disapproval” upon a state’s attribution of a ransomware operations to a harboring state.¹⁵⁷ The stronger the condemnation—especially where international crimes come into play—the more likely it is that the accused will change its behavior.¹⁵⁸ Moreover, the condemnation helps articulate “good” and “bad” behavior and thereby supports the formation of new norms and legal rules.¹⁵⁹

B. *Extraterritorial Enforcement and Prosecution*¹⁶⁰

As explained before, one of the biggest challenges posed by the threat of ransomware is the inability of states to enforce their criminal laws against hacker groups due to jurisdictional limitations generated by the act of harboring.¹⁶¹ By housing ransomware servers and networks in their territory, these harboring states shield the hackers from enforcement action. They know that victim states are unlikely to intrude on their territorial sovereignty and are therefore reassured that that sovereignty will offer sufficient protection to the criminals, many of whom are their nationals.

How might we be able to address this form of abuse? How might we be able to preserve the traditional prohibition on extraterritorial enforcement while still working around that prohibition to allow victim states to engage in effective criminal investigations and disruptive enforcement activities? One solution comes from exploring the work of Cedric Ryngaert. Ryngaert proposed the idea of a “positive sovereignty principle” which he described in the following way: “States are allowed to apply their laws to a foreign situation, to the extent the State that has the stronger nexus to the situation fails to adequately deal with, in manner that is, on aggregate, harmful to, the regulatory interests of the international community.”¹⁶² When a country like Iran, North Korea, or Russia provides safe harbor to hackers—sometimes even indirectly employing them¹⁶³—those countries should be denied the

156. See generally Martha Finnemore & Duncan B. Hollis, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, 31(3) EUR. J. INT’L L. 969 (2020).

157. *Id.* at 989.

158. *See id.* at 992.

159. *Id.* at 993.

160. Parts of this Section repeat analysis I have argued elsewhere in Lubin, *supra* note 99.

161. *See supra* notes 99–111 and accompanying text.

162. *See* CEDRIC RYNGAERT, JURISDICTION IN INTERNATIONAL LAW 190 (2d ed. 2015).

163. *See* Frank Bajak, *How the Kremlin Provides a Safe Harbor for Ransomware*, ASSOCIATED PRESS (Apr. 16, 2021), <https://apnews.com/article/business-technology-general-news-government-and-politicsc9dab7eb3841be45dff2d93ed3102999> [<https://perma.cc/74C4-5DRF>] (archived Aug. 24, 2022).

ability to abuse their sovereignty in this way. If ransomware is recognized as an international crime, then relying on sovereignty to further sustain it would become “harmful to the regulatory interests of the international community” precisely in the way that Ryngaert suggested. That would mean that states would finally have the right to investigate violations of their criminal laws and enforce their judgements extraterritorially without fear of a conflict with the laws of the harboring state.¹⁶⁴

Thinking beyond the issue of cyber investigation and enforcement, international criminalization of ransomware could serve other important functions. Recall that “inconsistencies in approaches, definitions, and sanctions can hinder international cooperation, particularly when it comes to assistance.”¹⁶⁵ Setting a universally agreed upon definition of the crime of ransomware, capable of adoption into domestic legislation, could introduce greater harmonization of substantive criminal laws, at least amongst like-minded countries. Moreover, obligations to cooperate and to extradite or prosecute could further support the efforts of individual states to bring perpetrators of ransomware offences to justice.

C. *Enhancing Cybersecurity at Home*

Historical analysis demonstrates the value of internationally criminalizing certain global crimes, such as piracy, aerial hijacking, and terrorism. In each of the three cases, the generation of international treaties and regimes led to greater centralization and harmonization of rules, and the formulation of new security protocols and best practices for prevention and mitigation of harm. They also helped reshape the public/private partnership and discourse as well as create new transnational agencies and partnerships which in turn created even further opportunities for standard-setting. Take aerial hijacking as a great example. At first, the problem was seen as one subject to the self-help measures taken by each of the individual

164. D’Urso argues that unilateral investigation and enforcement against cybercrime is “here to stay.” He, however, focuses his analysis on the efficacy and availability of luring operations. These are undercover operations aimed at encouraging cyber criminals to leave their country of residence (the harboring state) under false pretenses, so to be able to effectuate arrests and trials. He concludes by developing an interesting framework for responsibly and prudently deploying such lure operations in cybercrime cases. See D’URSO, *supra* note 154, at 218–80. While such operations could be fruitful in the fight against ransomware, the intelligence necessary to locate and identify ransomware gang members (as well as stop their operations in real time) will depend on cyber means of investigation. To employ such means states will still need to respond to any challenges imposed by the application of the prohibition on extraterritorial enforcement in cyberspace. As such the analysis offered in this paper remains relevant even in the context of D’Urso’s proposal.

165. JODY R. WESTBY, INTERNATIONAL GUIDE TO COMBATING CYBERCRIME 62 (2003).

airlines.¹⁶⁶ In fact, there were even academics who suggested that the pursuit of international legal instruments was a “serious miscalculation”¹⁶⁷ and that hijackings should be addressed as a “technical problem” rather than a “legal one.”¹⁶⁸ Those who believed this view argued that it was the role of flight technicians and professional airlines to address the problem of hijackings, and not the responsibility of government lawyers and foreign diplomats.¹⁶⁹

But the proceedings and scholarship that culminated with the adoption of the international conventions on skyjacking produced a significant realization for the participating countries. It affirmed that the old way of dealing with the problem, the one centered around the role of private entities, was in fact “sporadic, fragmented and short-term, determined by the whims, enthusiasms, apathies, and day-to-day policies of individual airlines and airport authorities.”¹⁷⁰ In the previous world order, “safety [was] an illusion.”¹⁷¹

This ultimately led to what passengers now take for granted a set of standardized international precautions taken in the design of aircrafts, in running security checks at airports, and in the organization of flights from takeoff to landing. Personal searches and searches of luggage, metal-detectors, and sniffing dogs were put in place through a process which first began in the adoption of these international instruments.¹⁷²

National and international programs were formulated to subsidize and help train and support the adoption of better security measures at airports and onboard aircrafts.¹⁷³ As some researchers have noted, “[a] steady decline in hijackings was driven instead by a collective effort among victim states and the private sector, employing a cocktail of active and passive measures—all of which holds lessons for policymakers working to combat ransomware.”¹⁷⁴

The development of an international agenda for fighting and criminalizing ransomware will set in motion new fora and new public-

166. See PETER CLYNE, *AN ANATOMY OF SKYJACKING* 138 (1973) (noting that “[i]t was only very recently that self-help was seen to be inadequate for the needs of a modern state, and that the problem of keeping order and enforcing the law came to be accepted as a national responsibility”).

167. Charles F. Butler, *The Path to International Legislation Against Hijacking*, in *AERIAL PIRACY AND INTERNATIONAL LAW* 27, 34 (Edward McWhinney ed., 1971).

168. Michael Pourcelet, *Hijacking: The Limitations of the International Treaty Approach*, in *AERIAL PIRACY AND INTERNATIONAL LAW* 55, 58 (Edward McWhinney ed., 1971).

169. See *id.*

170. CLYNE, *supra* note 166, at 177.

171. *Id.*

172. See CLYNE, *supra* note 166, at 181–82. Clyne further demonstrates how new coalitions were formed to demands these new precautions be implemented. *Id.* at 174 (discussing the role of the British Airline’s Pilots Association in mandating the introduction of security measures at Heathrow airport).

173. See generally HANDLER, SCHROEDER & HERR, *supra* note 67.

174. See *id.* at 5.

private coalitions to advance global, uniform, and standardized preventive security measures, crisis management structures, and response policies.

Moreover, the international criminalization of ransomware could impact what commercial insurers and individual victims are willing to do by generating an ethical discourse that will latch onto any concrete laws and regulations. It could enhance the expectation of reporting to law enforcement and reduce the number of ransom payments, knowing that in paying the ransom one might be deemed complicit in a crime against mankind. In other words, the internationalization of the crime could serve as a counterbalance to the sense that some victims have that their individual interests should outweigh any communal or collective societal interest. By merely framing the crime as one akin to terrorism or piracy, individual victims could develop a completely different lens and internal compass through which to view what reasonable responses are once a ransomware attack materializes.¹⁷⁵ This could also lead to a healthier ransomware insurance market, a market which currently suffers from soaring premiums and resulting gaps in coverage.¹⁷⁶

V. CONCLUSION

This Article was produced as part of the *Vanderbilt Journal of Transnational Law's* Spring 2022 Symposium. The title of that symposium was "The Law of Cyberterrorism." Whereas "cyber terrorism research and policy has hit somewhat of a deadlock in recent years,"¹⁷⁷ I read the call for symposium papers in a more general way: as an invitation to dig into the interoperability between cyberattacks like ransomware and traditional terrorism. The more I delved into the research, the more I realized that the international crime of terrorism has a rich history that can be tied to previous generations of parallel crimes: a string of delinquencies going back to maritime piracy and skyjacking. As I continued my research, I concluded that ransomware

175. A similar process took place in the United Kingdom in the context of kidnapping and terrorism insurance. See Asaf Lubin, *Public Policy and the Insurability of Cyber Risk*, 5 J.L. & TECH. TEX. 45, 97–98 (2021).

176. See e.g. Cheryl Winokur Munk, *Buying Cyber Insurance Gets Trickier as Attacks Proliferate, Costs Rise*, WALL ST. J. (Aug. 8, 2022), <https://www.wsj.com/articles/buying-cyber-insurance-gets-trickier-as-attacks-proliferate-costs-rise-11659951000> [https://perma.cc/5LED-LF3N] (archived Oct. 10, 2022); Kane Wells, *Cyber insurance study suggests businesses lack ransomware insurance*, REINSURANCE NEWS (Aug. 22, 2022), <https://www.reinsurancene.ws/cyber-insurance-study-suggests-businesses-lack-ransomware-insurance/> [https://perma.cc/B53B-FUGJ] (archived Oct. 10, 2022).

177. See STEFAN SOESANTO, ELCANO ROYAL INST., CYBER TERRORISM. WHY IT EXISTS, WHY IT DOESN'T, AND WHY IT WILL 7 (2020), <https://media.realinstitutoelcano.org/wp-content/uploads/2021/11/ari47-2020-soesanto-cyber-terrorism-why-it-exists-why-it-doesnt-and-why-it-will.pdf> [https://perma.cc/V6SK-26T9] (archived Aug. 24, 2022).

forms another link in this cross-generational family of international crimes.

Of course, proposing a “fool-proof legal framework and creat[ing] an international regime for preventing and deterring” international crimes, like ransomware, is not easy.¹⁷⁸ As S.K. Agrawala teaches us, “[m]any factors, political and economic play their part, and the efforts of nations with divergent interests have to be coordinated.”¹⁷⁹ But building on the successes of the past and learning from history is perhaps our best bet. We therefore must explore historically contextualized regulatory solutions to the problem of ransomware.

Usually in their academic writing, law professors like to say that through their research they have discovered a paradigm-shifting new theoretical frame. I am arguing the exact opposite of that in this paper. In my research I have *not* found a new frame, but rather an old one. Just by way of an anecdotal example, consider the words of Douglas Burgess in his book “The World for Ransom”:

[I]f international terrorists are neither ordinary criminals nor enemy combatants, what are they? There is an answer. Old, dusty, anachronistic perhaps, but eminently workable and entirely accurate.

They are pirates.

This book will prove that a precedent for terrorism exists in piracy—that they are, in fact, the same crime. Once we have a precedent, we have a law: terrorists will borrow not only pirates’ unique status as enemies of human race . . . but also the equally unique measures accorded to states to hunt them down.¹⁸⁰

My Article is merely an expansion of Burgess’s controversial claim, extending his arguments deep into the digital age. For, you see, ransom gangs are transnational organized criminals; they are terrorists; they are hijackers; they are pirates. And like Burgess says, once the international community recognizes that, it will have a relevant law to apply—be it as a matter of extending existing treaty frameworks or by developing new regimes based on old insights. If one views the world through this lens, it is no longer surprising to read a newspaper story with the headline: “Exclusive: U.S. to Give Ransomware Hacks Similar Priority as Terrorism.”¹⁸¹ Of course the United States will, for the two crimes are one in the same.

178. See AGRAWALA, *supra* note 132, at 138.

179. *Id.*

180. BURGESS, *supra* note 133, at 22.

181. Christopher Bing, *Exclusive: U.S. to Give Ransomware Hacks Similar Priority as Terrorism*, REUTERS (June 4, 2021), <https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/> [https://perma.cc/R4D6-FAXY] (archived Aug. 24, 2022).