Dear Participants of the Ostrom Workshop Colloquium Series,

Thank you for taking the time to read this work-in-progress. The project is obviously still in early stages. The version you have in front of you includes an abstract, introduction, an outline, and a few of the main arguments that I plan to raise in each section. I plan to spend most of the spring working on this paper based on feedback from Colloquium participants, with the goal of completing my revisions before the end-of-May. The paper will be published with the Vanderbilt Journal of Transnational Law as part of a special symposium organized by the journal titled: “The Law of Cyberterrorism: State Responsibility, Organized Crime, and Election Interference.”

Best,

Asaf Lubin
lubina@iu.edu
THE LAW AND POLITICS OF RANSOMWARE

Asaf Lubin*

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 4,000 ransomware attacks a day worldwide, a figure which was already alarming. By 2020, however, “attacks leveled out at 20,000 to 30,000 per day in the U.S. alone.” That is a ransomware attack every 11 seconds, each of which cost victims on average 19-days of network downtime and a payout of over $230,000. In 2021, global costs associated with ransomware recovery will exceed $20 billion.

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

To address these challenges the paper makes the case for the internationalization of the crime 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 paper makes the claim that most ransomware attacks are already criminalized under existing international law. In fact, the paper draws on historical analysis to portray

---

* 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, and a. 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.
the criminalization of ransomware as a “fourth generation” in the outlawry of Hostis Humani Generis (enemies of mankind).

The paper demonstrates the various opportunities that could arise from treating ransomware gangs as ones subject to universal jurisdiction. The paper focuses on four such opportunities for closing the ransomware underenforcement gap: (1) Expanding policies for naming and shaming harboring states; (2) Authorizing extraterritorial cyber enforcement action; (3) Extending the jurisdictional reach of both domestic and international courts; (4) Enhancing ransomware reporting obligations and restrictions on payments while advancing strategies for strengthening cybersecurity at home.

INTRODUCTION ........................................................................................................4

I. THE PROBLEM OF RANSOMWARE ......................................................................8
   A. DEFINING RANSOMWARE .................................................................................8
   B. EXISTING REGULATION AND ITS LIMITS ..........................................................8
      1. Domestic Law .......................................................................................................8
      2. International Law .................................................................................................11
   C. THE CAUSES OF RANSOMWARE UNDERENFORCEMENT .............................11
      1. Information Asymmetries ..................................................................................12
      2. Law of Jurisdiction ............................................................................................12
      3. Tragedy of the Commons ..................................................................................12
      4. Managerial Deficits ...........................................................................................12
      5. Forensic Challenges ............................................................................................13
      6. Reversal of Public and Private Roles .................................................................13

II. REDEFINING THE CRIME OF RANSOMWARE .............................................14
   A. RANSOMWARE AS PIRACY ..............................................................................14
   B. RANSOMWARE AS HOSTAGE TAKING ...............................................................14
   C. RANSOMWARE AS TRANSNATIONAL CRIME .................................................14
   D. RANSOMWARE AS TERRORISM .......................................................................14

III. BUILDING THE RANSOMWARE ENFORCEMENT TOOLKIT .......................16
   A. NAMING AND SHAMING HARBOURING STATES .........................................17
   B. EXTRATERRITORIAL ENFORCEMENT ACTION ............................................17
   C. DOMESTIC AND INTERNATIONAL ADJUDICATION .....................................19
   D. REPORTING OBLIGATIONS, RESTRICTIONS ON PAYMENTS, AND CYBERSECURITY ....20

CONCLUSION ........................................................................................................20
INTRODUCTION

Lake City is located in northern Florida and has a population of roughly 12,000 residents. The city is rich with history and traditions, annually hosting a reenactment of the state’s largest Civil War battle, the Olustee Battle, as well the Alligator Warrior Festival, a three-day event celebrating Native American and immigrant cultures. One of the city’s most frequented tourist attractions is Webb’s Antique Mall, housing 400 booths in a 60,000 square feet air-conditioned building filled with historical and vintage treasures.

On 10 June 2019, this quaint town suffered a service-crippling ransomware attack. An employee of the town opened a malicious email with a compromised document that infected the city’s computers with a ransomware. Beginning at 7:30am “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.” With about 16 terabytes of information effectively locked, and online payment systems inoperable, the city was running blind. City employees were forced to go back to “paper receipts and hand-written building permits.”

Ransomware attacks are designated to deny access to a computer system or data, usually by encrypting it, until the victim pays extortion payments to the attacker. The ransomware used in Lake City’s attack, was the Ryuk...

4 Id.
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 Ransomware: What It Is and What to Do About It, DOJ (Jun., 2016), https://www.justice.gov/criminal-ccips/file/872766/download.
malware. According to the United Kingdom’s National Cyber Security Centre (NCSC), “Ryuk was first seen in August 2018 and has been responsible for multiple attacks globally.” 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.”

And just like clockwork, days after the initial infection, a ransom demand arrived. At first the city attempted to work with the FBI, and a consultancy firm (hired by its municipal risk pool insurer, Florida League of Cities) to restore systems. 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. Indeed, within two weeks from the incident, the city manager made a decision to fire the city’s IT director for failures relating to the incident.

Failing to restore network operability the city’s risk pool hired a negotiator who communicated with the hackers and brought their ransom demands down to 42 Bitcoins, roughly $460,000, of which the city only paid the $10,000 deductible with the League of Cities paying the rest. Ultimately,

---

9 Id.
10 See Robles, supra note 3. For an explanation of local government risk pools see John Rappaport, How Private Insurers Regulate Public Police, 130(6) HARV. L. REV. 1539, 1557-58 (2017) (“The nature, structure, and regulation of these pools vary from state to state, but the basic idea is consistent: a 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. Where an insurer issues an insurance policy to a policyholder in exchange for a premium, a pool writes a coverage memorandum to a member in exchange of a contribution. Underwriting, loss prevention, and claims management look similar in the two contexts. Putting formalities to one side, pools are essentially small mutual insurers.”).
11 See Villas-Boas, supra note 5.
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.\textsuperscript{13} 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.\textsuperscript{14}

Lake City is not alone. From A power distribution company in India,\textsuperscript{15} through the Royal Zoological Society of Scotland,\textsuperscript{16} to the court system of the Brazilian state of Rio Grande do Sul,\textsuperscript{17} ransomware is anywhere and everywhere. In the United States ransomware has become a real pandemic. In recent years we saw ransomware hitting a regional hospital in Indiana,\textsuperscript{18} a school district in Michigan,\textsuperscript{19} a courthouse in Texas,\textsuperscript{20} and a port in California.\textsuperscript{21} Even Lady Gaga is not immune.\textsuperscript{22}

The problem has become so big that John Oliver devoted a segment of Last Week Tonight to it, noting that the threat as gone from a “trickle to an

\textsuperscript{13} See Robles, supra note 3.
\textsuperscript{15} Pierluigi Paganini, Systems at a Power Company in India infected by a ransomware, SECURITY AFFAIRS (Mar. 30, 2018), https://securityaffairs.co/wordpress/70836/hacking/power-company-ransomware.html.
\textsuperscript{17} Garrett Thompson, Brazilian Courts Face Ransomware for Second Time in Recent Months, BINARY DEFENSE (May 3, 2021), https://www.binarydefense.com/threat_watch/brazilian-courts-face-ransomware-for-second-time-in-recent-months/.
absolute flood.’ He is not wrong. Ransomware is growing in both numbers and severity. In 2016, hackers perpetrated roughly 4,000 ransomware attacks a day worldwide, a figure which was already alarming. By 2020, however, “attacks leveled out at 20,000 to 30,000 per day in the U.S. alone.” That is a ransomware attack every 11 seconds, each of which cost victims on average 19-days of network downtime and a payout of over $230,000. In 2021, global costs associated with ransomware recovery exceeded $20 billion.

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

To address these challenges the paper makes the case for the internationalization of the crime 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 paper makes the claim that most ransomware attacks are already criminalized under existing international law. In fact, the paper 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 paper demonstrates the various opportunities that could arise from treating ransomware gangs as ones subject to universal jurisdiction. The paper focuses on four such opportunities for closing the ransomware underenforcement gap: (1) Expanding policies for naming and shaming harboring states; (2) Authorizing extraterritorial cyber enforcement action;

---

23 For the full segment see John Oliver, Ransomware: Lat Week Tonight on HBO (Aug. 16, 2021), https://www.youtube.com/watch?v=WqD-ATqw3js.


27 Id.

28 Id.
(3) Extending the jurisdictional reach of both domestic and international courts; (4) Enhancing ransomware reporting obligations and restrictions on payments while advancing strategies for strengthening cybersecurity at home.

I. THE PROBLEM OF RANSOMWARE

A. Defining Ransomware

[This section will define ransomware and provide a brief overview of the technological and political dimensions of the phenomenon. Generally, in ransomware attacks, the files on a device, server, or network are encrypted by malware rendering them inaccessible. Malicious actors then demand ransom in exchange for the needed decryption keys. In the case of the Colonial Pipeline and JBS Meat Market attacks, both attacks were attributed to Russian criminal gangs by the U.S. intelligence community and in both incidents the hackers were paid millions of dollars in ransom by the victims. The U.S. government blames Russia for harboring these criminals and President Biden confronted President Putin on this issue in Geneva during their summit on 16 June 2021.

Ransomware attacks are targeting every industry and walk of life, from law firms to hospitals to academic institutions to insurance companies to police departments. Ransomware is also attacking private individuals, not only big firms or public utilities. By targeting every aspect of our interconnected digital lives, 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 even at the expense of financing a criminal enterprise.

This section will also address recent trends in ransomware’s evolution including the concept of “ransomware-as-a-service” and rise of mobile ransomware attacks. Most importantly it will discuss a possible future terrifying evolution of ransomware, as exemplified in the Kaseya attack which combined ransomware with a zero-day attack (exploiting unknown and unpatched vulnerabilities) and a supply chain attack (cascading along the bottlenecks and chokeholds of our internet society.

B. Existing Regulation and its Limits

1. Domestic Law
This section will briefly touch on the existing patchwork of direct and indirect regulation within the United States to address ransomware. This includes the criminalization of possessing and distributing ransomware tools, the regulation of cyber insurers, and the sanctioning of certain types of ransomware payments.


**Federal Level:** 18 U.S.C. § 1030(a)(7), U.S. Department of Treasury’s Office of Foreign Asset Control (OFAC) Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (Oct. 2020). SEC also issued a Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 2018).²⁹ The Inter-Agency Tactical Guidance led by CISA (through StopRansomware.gov) and the new DOJ Ransomware Taskforce will also be discussed. Finally, I will explore two legislative efforts from Congress: the House “Ransomware and Financial Stability Act” and the Senate “Sanction and Stop Ransomware Act” (these two 2021 acts addressed certain reporting obligations and sanction certain ransomware payments).

This section will highlight four key points:

- **The hesitant and indecisive nature of the federal and state response to date:** While recommending no payment of ransomware,²⁰ so far the government has not enforced against

²⁹ Both the SEC and the Financial Industry Regulatory Authority (FINRA) have each published reports outlining regulatory examination priorities for 2021. The SEC’s report focused on companies improving responses to cyberattacks and identifying potential risks within their environment. FINRA’s report highlighted potential vulnerabilities and outlined recommended practices for member firms to implement in their compliance programs. Both organizations noted the sharp increase in remote operations due to the pandemic and the rise in cyberattacks which has led to amplified concern over the security of sensitive information.” Alex Koskey and Matt White, *Ransomware state of the union: regulations, trends and mitigation strategies*, REUTERS (Oct. 14, 2021), https://www.reuters.com/legal/legalindustry/ransomware-state-union-regulations-trends-mitigation-strategies-2021-10-14/.

³⁰ See e.g. CISA, *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 (noting that CISA “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
such payments, even where local and state public entities have paid the ransom. This sends mixed signals to the public and harms the ability to reduce the total amount of payments paid. 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.

- **Limited role of tort liability and FTC enforcement:** examining cases like *Keach v. BST & Co. CPAs, LLP* and *Grifo & Company* as well as *PLLC v. Cloud X Partners Holdings, LLC* this section will highlight how courts have rejected the introduction of new duties of care in the context of ransomware prevention and mitigation, thereby denying the evolution of common law negligence claims (which is problematic especially where a breach of contract argument is not available). In addition, I will try to show the limited role that the FTC has so far played in responding to ransomware (compared to its expensive role in other cybersecurity regulation and enforcement). I will therefore make the claim that federal agencies in the U.S. have focused most of their attention on “data breaches” in a way that has come at the expense of addressing ransomware (given that the crime does not fall into the traditional definition of a data breach as understood under most state data breach notification laws).

- **Limited criminal enforcement:** Despite some ad hoc successes—such as DOJ’s seizure in June 2021 of $2.3 million in cryptocurrency paid to the Ransomware Extortionists Darkside and of another seizure in November 2021 of $6 million in ransom payments to a pair of Russian and Ukrainian nationals who were behind the REvil ransomware—as a general rule there have been few indictments for ransomware crimes in the United States and even fewer convictions. Successful action to re-seize money files will be recovered.”); United States Conference of Mayors, *Opposing Payment To Ransomware Attack Perpetrators* (July 12, 2019), https://www.tripwire.com/state-of-security/security-data-protection/mayors-say-theyll-no-longer-pay-ransoms-connected-to-security-events/ (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).

31 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.
paid is at the moment best understood as a drop in the ocean.

- **The rising role of private actors**: Against this backdrop of ineffectiveness on the state and federal levels, the section will end with the rise of new markets for ransomware prevention and mitigation including private security companies that negotiate with the hackers, tech teams that handle the data restoration front, and commercial insurers that cover the cost of paying the ransom.

2. International Law

   [This section will briefly touch on the limits of primary principles of international law to address the problem of ransomware. In particular, this section will focus on the doctrines of sovereignty, due diligence, non-intervention, attribution, and countermeasures.\(^{32}\) It will conclude, as others have, by noting that the “space is nascent and evolving,”\(^{33}\) and that so far states have not been willing to forego their own “freedom of action through the adoption or advancement of specific international law rules”\(^{34}\) that could constrain ransomware activity. The Oxford Statement on the Regulation of Ransomware Operations, one that I was involved in the drafting of and gladly signed once published, doesn’t change much of these conclusions. While the statement reflects the strong positions of expert members within the invisible college as to existing international law, it ultimately acknowledges that it serves as a call to nations “to fully commit to this vision,”\(^{35}\) a vision that they clearly have not yet signed on to]

C. The Causes of Ransomware Underenforcement

Following up from the previous two sections, this section will explain the root causes for ransomware underenforcement under both domestic and international law. It builds on prior works, like that of Peter Swire in “No Cop on the Beat.”\(^{36}\) For the purposes of this section, I define

---

\(^{32}\) See *e.g.*, Kenneth Kraszewski, Scenario 14: Ransomware Campaign, CYBER LAW TOOLKIT (https://cyberlaw.cccdcoe.org/wiki/Scenario_14:_Ransomware_campaign).


\(^{34}\) *Id.*


\(^{36}\) See generally, Peter Swire, *No Cop on the Beat: Underenforcement in E-Commerce*
underenforcement as a situation involving “a weak state response to lawbreaking as well as to victimization.” 37 This section will briefly touch on six different causes:

1. Information Asymmetries

[Will highlight the fact that there are no obligations to share information under domestic law (between insurers, security firms, victims), and no incentives to report to law enforcement, resulting in severe informational gaps. I will try to connect this point to the informational gaps that persisted in the pre 9/11 era and were identified by congress to be one of the causes of the tragedy.]

2. Law of Jurisdiction

[In ransomware cases perpetrators are often operating from abroad in countries that provide them shelter and refuse to take enforcement action against them. As was articulated by the Permanent Court of International Justice (PCIJ) in the Lotus case: “the 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.” 38 The doctrine, as interpreted by pure sovereignists, therefore prohibits law enforcement from taking extraterritorial cyber enforcement action without the consent and cooperation of the ransomware harboring state, resulting in complete impunity.]

3. Tragedy of the Commons

[Given the magnitude of the problem, no one local individual 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.]

4. Managerial Deficits

[Ransomware is about scale. The hackers use “ransomware-as-service” to target hundreds of victims at once, knowing that at least some will pay.

---

38 See S.S. Lotus Case (Fr v Turk) (Judgment) [1927] PCIJ Rep Series A No 10, 19.
The problem is that law enforcement is not capable of simultaneously addressing hundreds of crimes all happening at once. So, while crime has scaled up, responses to it have not. As a result, often victims call law enforcement and get only limited and partial assistance to their problems. They are therefore not incentivized to communicate with law enforcement in the future – enhancing the informational asymmetry even further.

5. Forensic Challenges

[Challenges in evidence gathering, attribution issues, and the varied technological sophistication and literacy of 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 on an hourly basis through domestic crime—is what makes this a unique threat.]

6. Reversal of Public and Private Roles

[In the 1980s debates grew in the US about kidnapping and ransom insurance, following a series of high-profile kidnappings of CEOs of companies in Latin America. Then US Attorney General, Ed Meese, was considering a ban on insurance for kidnapping. The thinking was that “presence of insurance actually increases the probability of kidnapping.” Ultimately, his decision was to not ban such programs. The worry was that a ban on insurance would create “an inhibition to early contact with law enforcement.” This is because policyholders were required under their insurance policies to notify the FBI prior to indemnification. In fact, insurers relied on the FBI’s involvement, to negotiate with the kidnappers and diplomatically work with the countries in which those kidnappers were operating.

The problem we’re seeing with ransomware is that there is no longer a reason to go through the government. Physical kidnappings mandate inter-governmental coordination to assist in the release and recovery of the kidnapped. When everything is digital and no physical element is involved

---


in the process, the role of government in resolution of these sorts of ongoing crises decreases. Add to that, a recent rise in private security startups 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. The result is that insurance policies no longer demand notification to law enforcement or collaboration with the government, further exacerbating the informational asymmetries discussed above.]

II. REDEFINING THE CRIME OF RANSOMWARE

A. Ransomware as Piracy
B. Ransomware as Hostage Taking
C. Ransomware as Transnational Crime
D. Ransomware as Terrorism

[When President Biden met with President Putin in June 2021 in Geneva, the message that was sent was that “certain critical infrastructure should be off limits to attack. Period.”41 This included the 16 sectors designated as critical by the U.S. Homeland Security Department (which includes: telecommunications, healthcare, and energy). By claiming that certain types of ransomware were off-the-table the administration was also presumably reaffirming the idea that “other” types of ransomware were on the table. This is a troubling proposition (and echoes Biden’s most recent rhetorical blunder, distinguishing between a “minor incursion” by Russia into the Ukraine and more severe incursions42).

This section will try to make the case that most (if not all) ransomware attacks are malum in se (evil in itself). It will build the case for a baseline of illegality around ransomware attacks as a matter of international law. To make the case, the section will begin by describing three prior generations of the outlawry of certain kinds of international crimes:

Generation 1: Piracy on the high seas and the Slave Trade.


42 See Tracy Wilkinson, Biden’s ‘minor incursion’ comment roils diplomatic efforts to halt Russian invasion of Ukraine, LOS ANGELES TIMES (Jan. 20, 2022).
It is in this sense that the international criminalization of ransomware can naturally derive its legitimacy and logic from the three generations that preceded it and become a sort of fourth digital generation of the criminalization of “crimes against the state.”

The section will look at existing treaty bodies to explore the way current regimes already capture certain aspects of the crime of ransomware. As will be demonstrated there is significant overlap between the various authorities and definitions, which creates an opportunity for either selectively applying relevant provisions, or using them as a theoretical model for thinking through future regulation. In particular, the section will look at the 1979 Hostage Taking Convention, the 2000 Convention Against Transnational Crime, and the customary prohibition against the harbing of terrorists. Consider the following three examples that will be analyzed against actual ransomware case studies:

- “The International Convention Against the Taking of Hostages” defines the act of hostage taking in the following way: “Any 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.” (Article 1).
  - Without getting metaphysical (by asking whether we’ve reached the point where the detention of one’s data is like the detention of one’s person, given that our digital self is now an extension of our physical self), there are certain ransomware attacks that result in actual physical detention or significant constraint. Think about ransomware against hospitals, which result in delays in surgeries and ultimately can even lead to death. Also

\[\text{\textsuperscript{43}}\] For more on this see Michael Head, Crimes Against the State: From Treason to Terrorism 275 (2011).

consider the ransomware on Colonial Pipeline which resulted in significant gas shortages. One can certainly justify the inclusion of at least some ransomware in the category laid down by Article 1 of the Convention.

- The customary prohibition on terrorism, defines the crime 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; (iii) when the act involves a transnational element.”

  o Again, under this definition, ransomware attacks—especially those orchestrated by organized groups with potentially broader political agendas—neatly falls into the definition of terrorism.

- “The UN Convention Against Transnational Organized Crime” 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.” (Art. 2(a)).

  o Here too, most ransomware gangs will easily qualify and meet the definition.]

III. BUILDING THE RANSOMWARE ENFORCEMENT TOOLKIT

[This final section of the paper will examine the implications of recognizing ransomware as an international crime. It will specifically look at four areas of development that could assist in closing the ransomware underenforcement gap by directly addressing some of the root causes of ransomware discussed in section I.C. of this paper: (1) Expanding policies for naming and shaming harboring states; (2) Authorizing extraterritorial

---

cyber enforcement action; (3) Extending the jurisdictional reach of both domestic and international courts; (4) Enhancing ransomware reporting obligations and restrictions on payments while 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 OEWG is that they have failed to bring together consensus amongst member states around norms for responsible behavior in cyberspace. Given that it is unlikely that countries like Russia will sign-on to any new treaty regimes or resolutions that would prohibit or criminalize ransomware, the benefit of my proposal is that it builds on existing mechanisms. These mechanisms are both reflective of customary international law, and in certain circumstances even have harboring states as parties.

By changing the language around ransomware from one of domestic and petty crime, to one of international delinquency – said in one breath alongside piracy, terrorism, and torture – would have an expressive function. It would allow to raise the stakes in diplomatic talk and deterrence strategies against those states that facilitate or turn a blind eye to such attacks.]

B. Extraterritorial Enforcement Action

[the “most solid view” of international law is that any non-consensual access to data that is “stored on a server located in the territory of another state constitutes a breach of the territorial integrity of that state.”46 This view

---

46 Bert-Jaap Koops & Morag Goodwin, ‘Cyberspace, the Cloud and Cross-Border Criminal Investigation’, [2014] Tilburg Law School Legal Studies Research Paper Series, No. 05/2016, at 61 (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.”).
of the *lex lata* has been endorsed by courts, governments, scholars, and certain treaty regimes. The logic behind this interpretation is quite clear. As the American Law Institute’s Restatement (Third) of Foreign Relations confirms: “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.”

Relying on historical analogy, I will draw some lessons from certain episodes of extraterritorial enforcement action taken in the fight against pirate broadcasting (specifically Danish legislation and efforts to unilaterally seize

---

47 See *e.g.* X (Re), [2010] 1 FCR 460, 2009 FC 1058 (CaLII), para. 40; *Weber and Saravia v. Germany*, Decision, App. No. 54934/00, ECtHR, 29 June 2006, para. 88.

48 A 2013 study by the UN Office of Drugs and Crime summarized the opinions of 47 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 UNODC, Comprehensive Study on Cybercrime, (February 2013) <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> accessed 7 September 2021, 220 [hereinafter: UNODC Report].

49 See *e.g.* Robert J. Currie, *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the “Next Frontier?,* 54 CAN. YB INT’L. L. 63, 97 (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 THE AGE OF GLOBALIZATION* 341, 369 (Gunther Handl, Jochim Zekoll, & Peer Zumbansen eds., 2012) (noting that dispute 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, 1458 (2021)* (supporting a pure-sovereignist model according to which “low-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, Daniel Costelloe, Malgosia Fitzmaurice, Paul Gragl, & Edward Guntrp 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.”).

50 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 Council of Europe, Convention on Cybercrime, opened for signature 2001, E.T.S. No. 185, Art. 32 (entered into force 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).

51 Restatement (Third) of Foreign Relations Law of the United States § 432 cmt. b (suggesting further that the offended state may be entitled to seek certain reparation).
the Lucky Star, a ship registered in Guatemala and owned by a company incorporated in Lichtenstein that broadcasted from outside Danish territorial waters).

Note that in this section I don’t intend to take the position that all of cyberspace is subject to universal jurisdiction.\textsuperscript{52} Rather, I limit the analysis to the possibility for universal jurisdiction to ransomware (or even certain categories of heinous ransomware).\textsuperscript{53}

I further plan to build on the work of Cedric Ryngaert on “positive sovereignty principle,” which he describes 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.”\textsuperscript{54} Ransomware is one particular area where Ryngaert’s concept of positive sovereignty principle could be best applied.

What I hope to show in this section is the varied ways internationalizing the crime of ransomware could open the door for state action without the consent of the harboring state including unilateral cyber enforcement action]

C. Domestic and International Adjudication

[The treaties discussed above introduce certain built-in tools that could open the door for actual legal action against the perpetrators of ransomware crimes. For example, the International Convention Against the Taking of Hostages, to which Russia is a party, extends the International Court of Justice’s (ICJ) jurisdiction and gives an opportunity for victim states to explore this venue in seeking possible recourse.

Domestic courts would too benefit from a possible reliance on the above discussed international regimes. These regimes introduce a set of obligations that could help facilitate domestic prosecutions: (1) universal jurisdiction over the crimes in question; (2) obligations to “extradite or prosecute” on the harboring state; (3) obligation on the harboring state and third-parties to collaborate in the investigation of these crimes and to prevent further harm.

Even where the treaties don’t explicitly apply, they might set the regulatory model for future international ransomware regimes.]

\textsuperscript{52} See some discussion of this position here Mireille Hildebrandt, Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in cyberspace, 63 UNI. TORONTO L.J. 196, 222-23 (2013).

\textsuperscript{53} For a similar discussion see Alexandra Perloff-Giles, Note: Transnational Cyber Offenses: Overcoming Jurisdictional Challenges, 43 YALE J. INT’L. L. 191, 215-225 (2018).

\textsuperscript{54} See CEDRIC RYNGAERT, JURISDICTION IN INTERNATIONAL LAW 190 (2015).
D. Reporting Obligations, Restrictions on Payments, and Cybersecurity Enhancement

[Historical analysis demonstrates the impacts that internationalizing crimes have had on local policies and responses. In the case of piracy, skyjacking, and terrorism, these international treaties and regimes led to greater centralization and harmonization of rules and the formulation of new security protocols. They also helped reshape the public/private partnership and discourse as well as create new transnational agencies and partnerships which in turn created new opportunities for standard setting. Take skyjacking as a great example, once international regimes were introduced states began stepping in and taking over for what was essentially seen as the responsibility of individual airliners. National and international programs were formulated to subsidize and help train and support the adoption of better security measures at airports and onboard aircrafts. The same can be envisioned here.

Moreover, the criminalization of ransomware as an international crime, could impact what commercial insurers and individual victims are willing to do, by generating a normative and ethical discourse. It could force greater reporting to law enforcement and reduce the number of ransom payments, knowing that such an is now branded as complicity in “a crime against mankind.” It 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 torture or terrorism, individual victims could develop a completely different lens through which to view what reasonable responses are once a ransomware attack materializes.]

CONCLUSION

[To be completed]

* * *