CyCon 2025: The Next Step
17th International Conference on Cyber Conflict
C. Kwan, N. Gratzer, K. Podiņš, M. Tolppa (Eds.)
2025 © NATO CCDCOE Publications, Tallinn

CyCon 2025: Responding to Ransomware Within the Boundaries of International Law

Tsvetelina J. van Benthem
Research Fellow
Oxford Institute for Ethics, Law and Armed Conflict
Blavatnik School of Government
University of Oxford
Oxford, United Kingdom
tsvetelina.vanbenthem@bsg.ox.ac.uk

Roxana Radu
Associate Professor of Digital Technologies and Public Policy and Hugh Price Fellow
Blavatnik School of Government and Jesus College
University of Oxford
Oxford, United Kingdom
roxana.radu@bsg.ox.ac.uk

Abstract: This paper explores the interaction between state obligations under international law and the domestic measures taken by states to counter the ransomware threat. On the one hand, states are required to take a proactive approach by taking steps to protect against ransomware operations. On the other hand, their freedom to take action against ransomware actors and related harms is not unlimited – obligations under international law, such as those emanating from state sovereignty, constrain state action in important ways. Understanding the boundaries of action compliant with international law is essential: a balance must be struck between pursuing effective ransomware responses and ensuring compliance with international law. Maintaining trust in the international legal system is contingent upon clearly signalled and honoured state commitments to international law – its substance, institutions and processes.*

Keywords: *international law, offensive cyber operations, positive obligations, ransomware, resilience-building*

* This publication arises from research funded by the John Fell Oxford University Press Research Fund (grant no. 14333)

1. INTRODUCTION

Ransomware has established itself as one of the most pervasive and disruptive contemporary threats.[1] According to a 2024 report from the European Union Agency for Cybersecurity, the ransomware threat is characterized by 'ongoing growth' and a changing toolbox of extortion tactics.[2] Experience from past years has shown that effective protection can only be ensured by continuously evolving counter-ransomware strategies, establishing diverse and comprehensive resilience and disruptive measures, and streamlining collective responses.[3]

As the ransomware threat landscape continues to evolve, so do the domestic policies of states to protect themselves and those under their jurisdictions from its criminal ecosystem. States have adopted a range of measures, individually and collectively, to build domestic resilience, criminalize the deployment of ransomware, bolster law enforcement capabilities and, in some cases, offensively disrupt ransomware networks. At the same time, states continue to signal their commitment to the rules-based international order and the important role that international law plays in countering harms produced via information and communications technologies (ICTs).[4] This paper explores the interaction between state obligations under international law and the domestic measures taken by states to counter the ransomware threat. On the one hand, states are required to take a proactive approach to protect against ransomware operations. On the other hand, their freedom to take action against ransomware actors and related harms is not unlimited – obligations under international law constrain state action in important ways. Understanding the boundaries of action compliant with international law is essential: a balance must be struck between pursuing effective ransomware responses and ensuring compliance with international law. Maintaining trust in the international legal system is contingent upon clearly signalled and honoured state commitments to international law – its substance, institutions and processes.

The paper proceeds in four sections. Section 2 lays the foundation for the analysis by defining ransomware and exploring key trends in the evolution of the ransomware ecosystem. Section 3 addresses the interaction between ransomware, domestic responses and international law-making. Section 4 turns to the positive and

1 Microsoft, 'Digital Defense Report 2024: The Foundations and New Frontiers of Cybersecurity' 27 https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024 (accessed 12 April 2025).

2 European Union Agency for Cybersecurity, 'ENISA Threat Landscape 2024' (September 2024) 45 https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf (accessed 12 April 2025).

3 Interpol, Australian Government and International Counter-Ransomware Task Force, 'A Comparative Threat Assessment on Counter-Ransomware Interventions' (September 2024).

4 UNGA, 'Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025' (22 July 2024) UN Doc A/79/214, para 35.

5 ENISA (n 2) 45; 'Oxford Statement on International Law Protections in Cyberspace: The Regulation of Ransomware Operations' (*The Oxford Process*) https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-ransomware-operations/#:~:text=3.-,States%20must%20

negative obligations binding states under international law in their development and implementation of counter-ransomware measures and applies these obligations to concrete examples of measures taken or signalled by states. Section 5 concludes.

2. RANSOMWARE: DEFINITION AND TRENDS

Ransomware is, at base, a form of malware designed to take control of a target's assets, with assets rendered unavailable until a demand is met.[5] While the most prevalent earlier form of ransomware involved the encryption of data on the target's device, with decryption being contingent on the payment of a ransom, current trends suggest an increasing use of exfiltration of data from the victim's device coupled with threats to publish or sell sensitive data in case of non-payment of the ransom.[6]

In recent years, the ransomware model has become steadily more sophisticated and professionalized. A ransomware-as-a-service ecosystem continues to proliferate, with emerging platforms such as RansomHub and Farnetwork.[7] As Bátrla and Harašta explain, this ecosystem contributes

> to the development of [a] complex, diverse, and market-forces driven system comprising interactions between specialized actors, such as malware developers and operators, affiliates, analysts, botmasters, initial access merchants, money processing and laundering specialists, escrow services, forum and illicit marketplace administrators, infrastructure administrators, [and] even negotiation and customer support personnel.[8]

What this means is that any action to counter ransomware must face an entire criminal system. This criminal system is predominantly composed of private actors. That being said, private actors exhibit varying proximity and coordination with state actors. Most often, ransomware groups operate from safe haven jurisdictions that are unwilling to take decisive steps to dismantle them. This, in turn, impedes traditional enforcement action.[9] In some cases, these groups are themselves sponsored by a

refrain%20from%20conducting%2C%20directing%2C%20authorising%20or%20aiding%20and,and%20opinion%2C%20freedom%20of%20expression%2C (accessed 12 April 2025).

6 UK House of Commons and House of Lords, Joint Committee on the National Security Strategy, 'A Hostage to Fortune: Ransomware and UK National Security', First Report of Session 2023–2024 (13 December 2023) 5.

7 ENISA (n 2) 30.

8 M Bátrla and J Harašta, '"Releasing the Hounds?" Disruption of the Ransomware Ecosystem Through Offensive Cyber Operations' (2022) *Proceedings of the 14th International Conference on Cyber Conflict* 96.

9 Ransomware Task Force, 'Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force' (2021) 27.

10 For evidence that North Korea sponsored The Lazarus Group, a hacking team behind the WannaCry 2.0 global ransomware attack, see eg US Department of Justice, 'North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions' (Press Release, 6 September 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and (accessed 22 April 2025).

state.[10] In others, the activities of the criminal groups – disrupting and destroying foreign interests and assets – align with the goals of the territorial jurisdiction and are therefore tolerated.[11] Geopolitical events expose divergent alignments between states and ransomware groups – for instance, the cybercriminal group Conti pledged support for Russia in its war against Ukraine.[12] Depending on the modality of the private actor–state relationship, the actions of the former may be attributable to the latter.[13] Exploring the content of the customary rules of attribution and their application to various ransomware groups is beyond the scope of this paper.[14] For present purposes, it is important that ransomware operations from safe haven jurisdictions significantly hamper efforts to bring the law to bear on perpetrators. This, in turn, sheds light on the importance of international cooperation in criminal matters, including in law enforcement.

Finally, while artificial intelligence (AI) can be used in the fight against ransomware groups – in tracking threat actors, scenario planning and resilience-building[15] – it is equally employed by ransomware actors to facilitate their activities. It is projected that AI will increase the scale and impact of ransomware operations, especially in relation to reconnaissance and social engineering.[16]

Against this background, states continue to tailor their approaches to the evolving ransomware ecosystem, increasingly focusing on domestic resilience-building and cooperation in the dismantling of ransomware criminality.

11 For a discussion of the Kremlin's approach to certain ransomware actors in the United Kingdom, see House of Commons and House of Lords, Joint Committee on the National Security Strategy (n 6) 17–18.

12 Global Initiative against Transnational Organized Crime, 'The Rise and Fall of the Conti Ransomware Group' (27 June 2023) https://globalinitiative.net/analysis/conti-ransomware-group-cybercrime/ (accessed 12 April 2025).

13 The recognised customary grounds of attribution under international law are codified in International Law Commission, Articles on the Responsibility of States for Internationally Wrongful Acts (2001) arts 4–11. Of most relevance are the grounds under arts 4 (most relevantly on *de facto* organs), 8 (instructions, direction or control) and 11 (acknowledgment and adoption).

14 The following sections will focus on the scenario of criminal groups whose conduct is not legally attributable to a particular state or states.

15 International Counter Ransomware Initiative, '2024 Joint Statement' (2 October 2024) https://www.whitehouse.gov/briefing-room/statements-releases/2024/10/02/international-counter-ransomware-initiative-2024-joint-statement/ (accessed 10 April 2025). S Poudyal and D Dasgupta, 'AI-Powered Ransomware Detection Framework' (2020) *IEEE Symposium Series on Computational Intelligence*.

16 UK National Cyber Security Centre, 'The Near-Term Impact of AI on the Cyber Threat' (2024) https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat#section_3 (accessed 12 April 2025).

3. THE INTERACTION BETWEEN RANSOMWARE, DOMESTIC MEASURES AND INTERNATIONAL LAW-MAKING

That ransomware poses a transnational threat to lives and livelihoods, the global economy, and the normal functioning of governments and the private sector is, by now, both undeniable and universally understood. International efforts, such as the International Counter-Ransomware Initiative,[17] seek to pool knowledge, build collective resilience and develop common policies to counter the threat. In November 2024, the United Nations Security Council heard briefings on the challenges posed by ransomware attacks against hospitals and other healthcare facilities and services,[18] with the United States representative stating that 'none of us is doing enough'.[19]

How states respond to ransomware individually and collectively inevitably involves international law. On the one hand, their responses demonstrate the connection between ransomware harms and human rights, including the rights to life and health. Ransomware operations pose foreseeable risks to the enjoyment of these rights: 'Health experts have estimated that ransomware attacks were responsible for the deaths of dozens of patients in the United States.'[20] On the other hand, international law constrains state responses both within their territory (for instance, in taking measures that do not violate the human rights of those under their jurisdiction) and extraterritorially (for instance, through obligations that protect the interests of other states, such as sovereignty, non-intervention and the prohibition of the use of force, and the rights of individuals). International law is both an important item in the state toolkit for combating ransomware[21] and an important reminder that their freedom to take action against ransomware actors is not unlimited.

There are three notable dynamics in the interaction between ransomware, domestic measures and international law-making.

First, while ransomware is clearly a threat of utmost concern to states, their statements on the application of international law to cyberspace do not suggest any difference in

17 The International Counter-Ransomware Initiative is an initiative uniting more than 70 member states and organisations to build cross-border resilience and collectively disrupt and defend against cyber actors; see 'About' (*International Counter-Ransomware*) https://counter-ransomware.org/ (accessed 13 April 2025).

18 WHO, 'Director-General's Remarks at Meeting of the UN Security Council on Threats Posed by Ransomware Attacks Against Hospitals and Other Health-Care Facilities and Services' https://www.who.int/director-general/speeches/detail/who-director-general-s-remarks-at-meeting-of-the-un-security-council-on-threats-posed-by-ransomware-attacks (accessed 8 April 2025).

19 US Mission to the UN, 'Remarks at a UN Security Council Briefing on Ransomware Attacks Against Hospitals and Other Healthcare Facilities and Services' https://usun.usmission.gov/remarks-at-a-un-security-council-briefing-on-ransomware-attacks-against-hospitals-and-other-healthcare-facilities-and-services/ (accessed 10 April 2025).

20 ibid.

21 T van Benthem and C Tams, 'Regulating Ransomware Through International Law' (2024) Report of the Scottish Council on Global Affairs https://scga.scot/wp-content/uploads/2024/02/Ransomware-Report-Final-January-2024.pdf (accessed 10 April 2025).

the specification of international law obligations in their application to ransomware. The approach taken is generic, with specific types of cyber operations often given merely as illustrations. Ransomware operations are used as illustrations in the 2024 position of Austria (exemplifying the trigger for a positive due diligence obligation),[22] the 2024 position of the Czech Republic (exemplifying breaches of sovereignty)[23] and the 2023 position of Costa Rica (exemplifying breaches of sovereignty through loss of functionality in operating systems, intervention and due diligence, and the meaning of attack under international humanitarian law).[24] While certain legal interpretations may be seen as implicitly tied to the ransomware threat,[25] national positions do not explicitly suggest that ransomware operations are shifting or specifying their interpretations of the law.

Second, the development of state positions and their content is bound to states' perceptions of their own vulnerability and their technical capacities to counter the threat. For instance, Costa Rica's national position was adopted in the aftermath of a large-scale and disruptive ransomware attack against the state, and its position paper highlights that ransomware 'may have significant economic, political, and human costs, as the ransomware attacks targeting Costa Rica in 2022 illustrates'.[26] And more limited interpretations of sovereignty-related rules of international law may be connected to the ability and willingness of states to counter ransomware groups extraterritorially through disruptive operations. Though not specifically stated in national positions, the need to protect against and respond to ransomware inevitably shapes the legal positions that states advance internationally.

Third, the changing ransomware landscape, perceived necessity of responses and domestic action may lead to an evolution in the international legal rules, both through development in customary law and evolving interpretations of relevant treaties. For instance, perceived needs to act extraterritorially by accessing criminal infrastructure without the consent of the territorial state may invite a rethinking of the content of sovereignty, non-intervention and the use of force, together with related justifications in primary rules and circumstances precluding wrongfulness under the law of state responsibility. The very methodology of customary international law formation[27] and

22 Republic of Austria, 'Cyber Activities and International Law' Position Paper (April 2024) 11.
23 Czech Republic, 'Position Paper on the Application of International Law in Cyberspace' (2024) para 6(c).
24 Costa Rica, 'Position on the Application of International Law in Cyberspace' (2023) paras 20, 25, 28, 49.
25 For instance, Denmark, 'Denmark's Position Paper on the Application of International Law in Cyberspace' (2023) suggests that 'a cyber operation resulting in the malfunctioning of a State's financial system leads to significant economic damage' may fall within the purview of the prohibition of the use of force under the Charter of the United Nations.
26 Costa Rica, 'Position on the Application of International Law in Cyberspace' (2023) para 3.
27 International Law Commission, 'Draft Conclusions on the Identification of Customary International Law' (2018), with the requirements of (1) practice that is widespread, representative and consistent and (2) acceptance of such practice as law.

the rules on the interpretation of treaties[28] are important bulwarks against expansive interpretations and developments originating in a minority of states.

The following section examines the interaction between domestic measures taken or signalled by states, and their relation to positive and negative obligations under international law.

4. APPLYING INTERNATIONAL LAW TO STATE MEASURES IN COUNTERING RANSOMWARE

States have consistently affirmed that international law applies to the use of ICTs.[29] And while ransomware is not regulated under international law as such, a range of international obligations of general application are relevant to its regulation. Thus, under international law, states are bound by positive and negative obligations in relation to, among others, individuals and other states, and these general obligations apply when states take measures to counter ransomware activity. The following sections examine, first, positive obligations that require states to take steps to tackle the ransomware threat, and second, a subset of negative obligations that constrain states in the measures they are allowed to take.

A. Obligations to Take Steps: Positive Due Diligence Obligations to Counter Ransomware

Ransomware's impact is felt across society. Its harmful effects on the provision of essential services, the operation of governmental entities and the private sector, and the security and well-being of individuals are well-documented.[30] The threat of ransomware is both real and foreseeable. Unsurprisingly, there is increasing state activity in designing domestic strategies to counter ransomware, in coordinating with local and international partners, and in building or enhancing the existing regulatory framework. While this state activity is in line with states' interests, and a reflection of their respective perceptions of vulnerability, the taking of measures to counter the ransomware threat is also a matter of international obligation.

Under international law, positive obligations compel states into action. Such positive obligations exist under different legal regimes and under different sources of law. For

28 See also International Law Commission, 'Draft Conclusions on Subsequent Agreements and Subsequent Practice in Relation to the Interpretation of Treaties' (2018).

29 UNGA, 'Final Substantive Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' (10 March 2021) UN Doc A/AC.290/2021/CRP.2 para 34; 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' (14 July 2021) UN Doc A/76/135, paras 69ff.

30 J MacColl, P Hüsch, G Mott, J Sullivan, JRC Nurse, S Turner and N Pattnaik, 'The Scourge of Ransomware: Victim Insights on Harms to Individuals, Organisations and Society' (2024) RUSI Occasional Paper.

instance, international human rights law treaty instruments[31] and customary human rights contain positive obligations binding states, triggered in cases of foreseeable risks to particular rights of individuals under their jurisdiction. Where such foreseeable risks arise, states must take steps to prevent their materialization or mitigate their effects, including in cases where the risks are created by non-state actors. Elaborating on this obligation in the context of the right to life under the International Covenant on Civil and Political Rights, the United Nations Human Rights Committee explained that

> State parties are thus under a due diligence obligation to take reasonable, positive measures that do not impose disproportionate burdens on them in response to reasonably foreseeable threats to life originating from private persons and entities whose conduct is not attributable to the State.[32]

A similar interpretation of the right to life was given by the African Commission on Human and People's Rights: 'The State has a positive duty to protect individuals and groups from real and immediate risks to their lives caused either by actions or inactions of third parties.'[33]

Positive obligations arise under a wide range of rights, including life, health, privacy, property and education, and there is no prescriptive list of measures that must be implemented to discharge them in each and every case and across contexts. When it comes to countering ransomware, these obligations may be discharged by a number of technical, legal or institutional measures, such as the enactment of domestic legislation to criminalize ransomware and impose cybersecurity requirements on local entities, the adoption of measures and establishment of government structures to prevent ransomware operations or halt ongoing ones, the drafting and publicising of contingency plans and cyber hygiene, the investigation and prosecution of those responsible, the adoption of guidance on ransomware payments, among many others.[34] The Human Rights Committee has previously stated that states should develop, 'when necessary, contingency plans and disaster management plans designed to increase preparedness' in view of 'massive cyberattacks resulting in disruption of essential services'.[35] It bears mentioning that the United Nations Convention on Cybercrime,

31 For instance, under the International Covenant on Civil and Political Rights (16 December 1966) 999 UNTS 171; African Charter on Human and Peoples' Rights (21 October 1986) 1520 UNTS 217; American Convention on Human Rights (22 November 1969) 1144 UNTS 123; European Convention on Human Rights (4 November 1950) 213 UNTS 222.

32 Human Rights Committee, 'General Comment 36 on the Right to Life' (2018) para 21.

33 African Commission on Human and Peoples' Rights, 'General Comment No 3 on the Right to Life' (2015) para 41.

34 For examples of such measures, see 'Oxford Statement on International Law Protections in Cyberspace: The Regulation of Ransomware Operations' (*The Oxford Process*) https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-ransomware-operations/#:~:text=States%20must%20refrain%20from%20conducting,Charter%20of%20the%20United%20Nations (accessed 12 April 2025).

35 Human Rights Committee, 'General Comment 36 on the Right to Life' (2018) para 26.

adopted by the United Nations General Assembly in December 2024 and open for signature in 2025, would impose a number of substantive criminalization obligations and jurisdictional, enforcement and institutional ones on its parties. Although the Convention does not specifically criminalize ransomware, the offences of illegal access, illegal interception, interference with electronic data and misuse of devices, among others, would cover such conduct.[36] In this way, compliance with substantive and procedural obligations under the Cybercrime Convention could align with the demands of positive obligations under international human rights law.

Another example of an international law obligation requiring states to take steps is the obligation for states to not knowingly allow their territory to be used for acts contrary to the rights of other states.[37] This obligation, expounded on by the International Court of Justice in the *Corfu Channel* case, is also characterized by a due diligence standard, and is aimed at the protection of the interests of states.[38] While there are ongoing controversies over the customary scope of this rule,[39] it undeniably has important implications for ransomware operations. A failure of a state to dismantle or otherwise counter ransomware actors under its jurisdiction who are conducting ransomware operations affecting other states, where the state of jurisdiction is or should be aware of their activity, would result in a breach of this rule, and thereby entail the responsibility of the state. This rule therefore has the capacity to provide redress against states that have become safe havens for ransomware criminal groups.

While these positive obligations are flexible and subject to state capacity, they clearly demonstrate that, where their triggering circumstances are met, states are required to be proactive. In the context of ransomware, many states are indeed taking a proactive approach to building resilience against cyber threats, including ransomware. Australia, for instance, has introduced mandatory reporting of cybersecurity incidents for critical infrastructure operators under the Security of Critical Infrastructure Act 2018.[40] The Cyber Security Strategy Action Plan 2023–2030 stresses the importance of building resilience within society, providing clear guidelines for businesses, and creating a comprehensive threat intelligence framework.[41] The United Kingdom, in its '2023 Ransomware White Paper', adopted a holistic and systemic approach to ransomware,

36 UNGA, 'United Nations Convention Against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes' (31 December 2024) UN Doc A/RES/79/243 arts 7, 8, 9, 11.

37 *Corfu Channel (UK v Albania)* [1949] ICJ Rep 4 [22].

38 A Coco and T de Souza Dias, 'Cyber Due Diligence: A Patchwork of Protective Obligations in International Law' (2021) 32(3) European Journal of International Law 771.

39 'Due Diligence' (*CyberLaw Toolkit, CCDCOE*) https://cyberlaw.ccdcoe.org/wiki/Due_diligence (accessed 8 April 2025).

40 Australian Government, 'Security of Critical Infrastructure Act 2018 (SOCI)' (*Federal Register of Legislation*) https://www.legislation.gov.au/C2018A00029/latest/versions (accessed 8 April 2025).

41 Australian Government, 'Cyber Security Strategy Action Plan 2023–2030' 6, 8, 14 https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy-action-plan.pdf (accessed 8 April 2025).

with a particular focus on cyber hygiene.[42] And Costa Rica, following the highly disruptive ransomware operation affecting the country in 2022,[43] has focused on the protection of its critical infrastructure with periodic analyses of vulnerability and risk,[44] and the bolstering of entities tasked with cybersecurity coordination, such as the Centro de Respuesta de Incidentes de Seguridad Informatica. Importantly, Costa Rica has emphasized that measures meant to tackle cybersecurity threats must be undertaken in compliance with human rights, especially freedom of expression and privacy.[45] Specific incidents, notably the ransomware operation against Colonial Pipeline in the United States, have also prompted tailored responses, such as measures to protect the security of supply chains, the development of playbooks for responding to cybersecurity incidents and the establishment of better evidence-sharing arrangements between the government and the private sector.[46]

Effectively discharging positive obligations under international law could also require transnational coordination and cooperation, as individual states may be unable to protect against the ransomware threat on their own. Participation in transnational collaborative initiatives, such as CyberSouth+, jointly launched by the European Union and Council of Europe,[47] can enhance collaborative processes, including by strengthening the tools of criminal justice on the disclosure of electronic evidence.

It can be concluded that states are obliged under international law to take measures to protect individuals and other states from the harmful effects of ransomware. At the same time, the freedom of states to take such measures is not unlimited. The boundaries of their freedom are determined by a number of negative obligations under international law.

B. Limited Freedom: Obligations to Abstain from Particular Types of Measures While Countering Ransomware

While positive obligations require states to act, a range of negative obligations under international law constrain the freedom of states to take these measures. As was discussed in Section 2, most ransomware actors operate from safe-haven jurisdictions

42 UK National Cyber Security Centre and National Crime Agency, 'Ransomware, Extortion and the Cyber Crime Ecosystem' (2023) White Paper https://www.ncsc.gov.uk/files/White-paper-Ransomware-extortion-and-the-cyber-crime-ecosystem.pdf (accessed 8 April 2025).

43 'Costa Rica Ransomware Attack' (*CyberLaw Toolkit, CCDCOE*, 2022) https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022) (accessed 8 April 2025).

44 R García Villalobos and others, 'Protocolo para el desarrollo de acciones que se deben implementar ante una amenaza de un ataque a la ciberseguridad nacional' (2022).

45 Costa Rica, 'Estrategia Nacional de Ciberseguridad' (*2017*) 8 https://www.clubdeinvestigacion.com/wp-content/uploads/2022/11/Estrategia-Nacional-de-Ciberseguridad-Costa-Rica-2022.pdf (accessed 8 April 2025).

46 Kimberly Wood, 'Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack' (2023) (*Georgetown Environmental Law Review*, 7 March 2023) https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack (accessed 8 April 2025).

47 This initiative seeks to entrench collaboration within the framework of the Budapest Convention on Cybercrime with Algeria, Egypt, Jordan, Lebanon, Libya, Morocco, Palestine and Tunisia, available at https://www.coe.int/en/web/cybercrime/cybersouthplus.

beyond the reach of law enforcement authorities of target states. Rules based on the principle of state sovereignty, such as the prohibition on the use of force, the principle of non-intervention and the primary rule of sovereignty all constrain extraterritorial enforcement activities without the consent of the state in whose territory the enforcement operation is to take place.[48] Since in most cases such consent will not be forthcoming, the capacity of states to enforce their laws against ransomware actors will be limited by international law.

At the same time, states signal an interest in a proactive 'offensive' approach to the dismantling of ransomware groups and cyber threats more generally. Australia, for instance, has invested heavily in expanding the range and sophistication of its offensive and defensive cyber capabilities. The Australian Signals Directorate undertakes offensive cyber operations to support national security, with one of its functions being to prevent and disrupt offshore cyber-enabled crime.[49] In a 2018 speech, the Director-General of the Australian Signals Directorate explained that its activities focused on offshore use 'specialized tools and techniques to disrupt their [their adversaries'] communications or interfere with the way they operate online'.[50] And in the United Kingdom, the report of the House of Commons and House of Lords Joint Committee on the National Security Strategy recommended that the Government 'invest significantly more resources in the National Crime Agency's response to ransomware, enabling it to pursue a more aggressive approach to infiltrating and disrupting ransomware operators'.[51]

While a more aggressive extraterritorial approach may *prima facie* seem an effective way of tackling the ransomware threat, it would come into tension with a range of negative obligations under international law that constrain extraterritorial enforcement activities.[52] What complicates the analysis under these negative obligations are the ongoing controversies over their elements and, for some, their very existence as primary rules of international law. Even if a particular extraterritorial activity would constitute a violation of a particular negative obligation, it may still – depending on the obligation breached – be possible to resort to justifications, either in the primary rules themselves or under the customary law of state responsibility. The analysis first

48 International human rights law also imposes constraints on extraterritorial state conduct. For reasons of scope, this strand of analysis is not addressed in this paper.

49 Australian Government, Australian Signals Directorate, 'ASD Corporate Plan 2023–24' https://www.asd.gov.au/about/accountability-governance/publications/asd-corporate-plan-2023-24 (accessed 9 April 2025).

50 Australian Government, Australian Signals Directorate, 'Director-General ASD Speech to the Lowy Institute' https://www.asd.gov.au/news-events-speeches/speeches/director-general-asd-speech-lowy-institute (accessed 9 April 2025).

51 UK House of Commons and House of Lords, Joint Committee on the National Security Strategy, 'A Hostage to Fortune: Ransomware and UK National Security, First Report of Session 2023–2024' (13 December 2023) 66.

52 T van Benthem, J Kulesza, Y Liu and N Sun, 'Jurisdiction in Cyberspace' (2024) Sino-European Expert Working Group on the Application of International Law in Cyberspace (EWG-IL), Research Group Report 2024 https://www.gcsp.ch/sites/default/files/2024-12/EWG-IL_Partnered_Jurisdiction_2024-11%3Bdigital.pdf (accessed 9 April 2025).

turns to the relevant primary obligations before reviewing the possibility of resorting to justifications.

To begin with, as explained by the Permanent Court of International Justice in the Lotus case, under customary law, a state 'may not exercise its power in any form in the territory of another State' without a permissive rule to the contrary.[53] A lawful exercise of extraterritorial enforcement jurisdiction would depend on 'valid consent by a foreign government to exercise jurisdiction on its territory' or 'a specific allocation of authority under international law'.[54] If extraterritorial cyber operations to disrupt ransomware groups qualify as enforcement actions, failing the existence of a permissive ground, they would come into tension with this customary rule.

Further, under the Charter of the United Nations, 'all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations'.[55] The key interpretative question here is over the meaning of 'force', in particular the types of effects and gravity sufficient to qualify as 'force'. Australia's position suggests that '[i]n determining whether a cyber activity constitutes a use of force, States should consider whether the activity's scale and effects are comparable to traditional kinetic operations that rise to the level of use of force under international law', and this entails an analysis of the 'intended or reasonably expected direct and indirect consequences of the cyber activity, including for example whether the activity could reasonably be expected to cause serious or extensive ("scale") damage or destruction ("effects") to life, or injury or death to persons, or result in damage to the victim State's objects, critical infrastructure and/or functioning'.[56] According to some states, including France, cyber operations without *physical* effects may also, depending on the circumstances, be characterized as a use of force.[57] An extraterritorial operation against a ransomware group causing effects in the territory of another state may therefore amount to a use of force under this prohibition.

Beyond the use of force, the principle of non-intervention prohibits states from coercive interferences in the *domaine réservé* of other states.[58] As for the prohibition of the use of force, the contours of this obligation remain contested, in particular regarding the element of coercion. Does coercion imply effects on the 'will' of the other state, or on its 'ability to control its sovereign choices'?[59] The United Kingdom

53 *SS Lotus (France v Turkey)* [1927] PCIJ Series A No 10, [45].
54 Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) rule 11.
55 Charter of the United Nations art 2(4).
56 Australian Government, 'Australia's Submission on International Law to Be Annexed to the Report of the 2021 Group of Governmental Experts on Cyber' 2.
57 French Ministry of the Armies, 'International Law Applied to Operations in Cyberspace' (2019) 7.
58 *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v US)* [1986] ICJ Rep [202].
59 Marko Milanovic, 'Revisiting Coercion as an Element of Prohibited Intervention in International Law' (2023) 117(4) *American Journal of International Law* 601, 626–48.

seems to adopt a wider understanding of 'coercion', explaining that 'an intervention in the affairs of another State will be unlawful if it is forcible, dictatorial, or otherwise coercive, depriving a State of its freedom of control over matters which it is permitted to decide freely by the principle of State sovereignty'.[60] Under a wider interpretation of the element of coercion, an extraterritorial operation to dismantle a non-state ransomware criminal group may indeed be seen as depriving the territorial state of control over enforcement activities in its jurisdiction.

And finally, while it is uncontested that sovereignty is a principle of international law animating a number of primary rules, there are ongoing debates over its existence and content as a self-standing rule. In their national positions on the application of international law to cyberspace, states increasingly adopt the sovereignty-as-a-rule approach.[61] The United Kingdom, however, has consistently rejected this view.[62] Depending on how a primary rule of sovereignty is framed, it can be more or less constraining on states that seek to counter ransomware actors extraterritorially. The African Union, for example, adopts a wide approach to sovereignty, which would capture any unauthorized access:

> By virtue of territorial sovereignty, any unauthorized access by a State into the ICT infrastructure located on the territory of a foreign State is unlawful. Therefore, the African Union emphasizes that the obligation to respect the

60 Attorney General, the Rt Hon Suella Braverman QC MP, 'International Law in Future Frontiers' (*GOV.UK*, 2022) https://www.gov.uk/government/speeches/international-law-in-future-frontiers (accessed 9 April 2025).

61 The following positions accept that sovereignty is a standalone rule of international law: African Union, 'Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace' (February 2024) para 13; Republic of Austria (n 22) 4; Brazil national position in *GGE 2021 Official Compendium* 18 (Brazil argues that any exception to the rule of sovereignty would require broad state practice and sufficient *opinio iuris*); Government of Canada, 'International Law Applicable in Cyberspace' (2022) para 13; China, 'Views on the Application of the Principle of Sovereignty in Cyberspace' 2–3; Costa Rica, 'Position on the Application of International Law in Cyberspace' (2023) para 19; Czech Republic, 'Position Paper on the Application of International Law in Cyberspace' (2024) para 3; Denmark (n 25) 448; Estonia, Contribution to *GGE 2021 Official Compendium* 25; Finland, 'International Law and Cyberspace', National Position, (2020) 2–3; France, 'International Law applied to Operations in Cyberspace', paper shared by France with the open-ended working group established by Resolution 75/240, 3; German Federal Government, 'On the Application of International Law in Cyberspace' Position Paper (2021) 3; Ireland, 'Position Paper on the Application of International Law in Cyberspace' (2023) para 5; Italy, 'International Law and Cyberspace', Position Paper, 4; Ministry of Foreign Affairs of Japan, 'Basic Position of the Government of Japan on International Law Applicable to Cyber Operations' (28 May 2021) 2; Government of the Kingdom of the Netherlands, 'Appendix: International Law in Cyberspace' (2019) 2; New Zealand, 'The Application of International Law to State Activity in Cyberspace' (2020) para 12; Norway, 'Norwegian Positions on Selected Questions of International Law Relating to Cyberspace' (2021); Poland, 'The Republic of Poland's Position on the Application of International Law in Cyberspace' (2022) 3; Romania, Contribution to *GGE 2021 Official Compendium* 76; Singapore, Contribution to *GGE 2021 Official Compendium* 83; Switzerland, Contribution to *GGE 2021 Official Compendium* 87.

62 Attorney General's Office and The Rt Hon Suella Braverman KC MP, 'International Law in Future Frontiers' (GOV.UK, 2022) https://www.gov.uk/government/speeches/international-law-in-future-frontiers (accessed 9 April 2025). 'The general concept of sovereignty by itself does not provide a sufficient or clear basis for extrapolating a specific rule of sovereignty or additional prohibition for cyber conduct going beyond that of non-intervention.'

> territorial sovereignty of States, as it applies in cyberspace, does not include a de minimis threshold of harmful effects below which an unauthorized access by a State into the ICT infrastructure located on the territory of a foreign State would not be unlawful.[63]

While most states condition this rule through a *de minimis* approach regarding effects, the ongoing uncertainty over the content of this rule creates a significant grey area regarding the legality of extraterritorial measures to tackle ransomware groups where the consent of the territorial state has not been obtained.

Importantly, even if a state is in breach of its international obligations when conducting extraterritorial counter-ransomware activities, this is not the end of the analysis. The state may be able to rely on justifications. For instance, states can use force in self-defence if they become the victim of an armed attack. Under the traditional restrictive view of the content of self-defence, it must be determined whether a ransomware operation that amounts to an armed attack actually occurred and whether the actor initiating that attack was a state.[64]

States may be able to rely on justifications under the law of state responsibility, such as countermeasures and necessity. Countermeasures are measures that, but for the internationally wrongful act of the responsible state, would be contrary to the international obligations of the state undertaking the measure. It is the fact that they respond to a prior illegality that provides the basis for their justifiability. The measures must comply with a number of stringent requirements related to their purpose and proportionality, among others, and must not affect a number of foundational obligations of international law, including the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations and obligations for the protection of fundamental human rights.[65] Importantly for counter-ransomware operations, states have a basis to resort to countermeasures not only against states that themselves conduct ransomware operations but also against those that provide a safe haven for criminal groups, thereby violating their obligations under international human rights law and the Corfu Channel rule.

Unlike countermeasures, necessity as a circumstance precluding wrongfulness does not require a prior unlawful act. On the grounds of necessity, the wrongfulness of a breach of an international obligation can be precluded where the conduct in violation

63 African Union (n 61) para 16.

64 Under this view, the acts of private actors must therefore be attributed to a state. On the content of the right to self-defence in the *jus ad bellum*, see African Union (n 61) para 43; T van Benthem and C Tams, 'Regulating Ransomware Through International Law' (2024) Report of the Scottish Council on Global Affairs 31–32 https://scga.scot/wp-content/uploads/2024/02/Ransomware-Report-Final-January-2024.pdf (accessed 9 April 2025).

65 International Law Commission, 'Articles on the Responsibility of States for Internationally Wrongful Acts' (2001) arts 49–54; for further analysis, see Talita Dias, 'Countermeasures in International Law and Their Role in Cyberspace' (2024) Chatham House Research Paper 9–32

is the only way for the state to safeguard an essential interest against a grave and imminent peril and it does not seriously impair an essential interest of the state or states towards which the obligation exists, or of the international community as a whole.[66] Because its potential for abuse is significant, this ground must be approached with caution. In this vein of caution and exceptionality, the position of the Netherlands considers that 'the ground of necessity may be invoked only in exceptional cases where not only are there potentially very serious consequences, but there is also an essential interest at stake for the state under threat. What constitutes an 'essential interest' is open to interpretation in practice, but in the government's view services such as the electricity grid, water supply and the banking system certainly fall into this category.'[67]

What can be gleaned from this overview is, first, that, as the ransomware threat grows, states may face increasing pressure to undertake offensive extraterritorial cyber operations against ransomware actors, and second, that the legality of their measures would depend on the interpretation of international legal obligations and their exceptions, and circumstances precluding wrongfulness under the law of state responsibility. The contours of both substantive obligations and circumstances precluding wrongfulness remain contested.

States consistently signal their commitment to international law. For instance, Australia has, since its first Cyber Security Strategy in 2016, affirmed that '[a]ny measure used by Australia in deterring and responding to malicious cyber activities would be consistent with our support for the international rules based order and our obligations under international law'.[68] One of the operational principles enshrined in the United Kingdom's 'Responsible Cyber Power in Practice Policy Paper' is that 'operations are conducted in a legal and ethical manner, in line with domestic and international law and our national values'.[69] Commitment to the international legal system necessitates further clarification and agreement on the content of the law, limiting as far as possible grey areas which may come into tension with state sovereignty and foreseeably lead to international escalation. And while grey areas remain, as they do in many fields of national and international law, it bears emphasis that the international law discussion is steadily growing in sophistication in national position papers and multi-stakeholder

66 International Law Commission, 'Articles on the Responsibility of States for Internationally Wrongful Acts' (2001) art 25.

67 Government of the Kingdom of the Netherlands, '*Appendix: International Law in Cyberspace*' (2019) 7–8; for further analysis, see Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views' (2020) *The Hague Program for Cyber Norms Policy Brief* 20–21.

68 Australia, *2016 Cyber Security Strategy* 27–28

69 UK National Cyber Force, 'Responsible Cyber Power in Practice' (*GOV.UK*, 2023) https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html#:~:text=What%20this%20means%20in%20practice,exposing%20hostile%20activity%20and%20wrongdoing (accessed 9 April 2025).

initiatives.[70] A more centralized approach to this clarification would be an important next step. This could serve as a signalled commitment to the international legal system, and a capacity- and confidence-building measure between states and other stakeholders.

5. CONCLUSION

The ransomware ecosystem adapts and evolves, and the threat it poses to societies worldwide continues its upward trajectory. As states continue to debate, both nationally and at the international level, the most effective approaches to counter ransomware criminality, international law must remain a central consideration for both policy-makers and those implementing domestic policies. International law requires states to act in the face of mounting ransomware risks. At the same time, it provides important constraints on state action.

This paper argued that positive obligations under international law compel states to take effective measures to protect individuals under their jurisdiction and other states from ransomware harms, including harms originating in non-state criminal groups. It reviewed measures already undertaken by states that are capable of discharging these positive obligations – the adoption of legislative frameworks for criminalization and reporting, whole-of-society cyber hygiene training and protective measures for critical infrastructure providers, among others. Effectively discharging positive obligations would require a comprehensive approach to protection and continuous updating of domestic measures in light of the evolving ransomware ecosystem.

Beyond measures aimed at domestic resilience-building, states may face the pressure of adopting a more 'aggressive' approach to the threat posed by ransomware groups, given their frequent operation from jurisdictions unwilling to take meaningful enforcement action. In crafting any potential extraterritorial measures to interfere with ransomware criminality, states must carefully consider their international law obligations to abstain from unlawful uses of force, coercive interferences and unlawful effects on the sovereignty of other states. Whether a particular activity breaches these negative obligations and whether their breach may be justified would depend on the legal interpretation of the relevant rules, many of which remain pixelated. Especially in areas of heightened geopolitical sensitivity, states must exercise particular caution. One important aspect of being cautious – and responsible – in countering ransomware is to commit to the meaningful clarification of the relevant international law rules.

70 See eg 'Tallinn Manual Process' (CCDCOE) https://ccdcoe.org/research/tallinn-manual/ (accessed 9 April 2025); 'Oxford Process on International Law Protections in Cyberspace' (*The Oxford Process*) https://www.elac.ox.ac.uk/the-oxford-process/ (accessed 9 April 2025); 'International Cyber Law in Practice: Interactive Toolkit' (*CyberLaw Toolkit, CCDCOE*) https://cyberlaw.ccdcoe.org/wiki/Main_Page (accessed 9 April 2025).