International Journal of Law and Information Technology, 2026, **34**, eaag004
https://doi.org/10.1093/ijlit/eaag004
Published: 5 February 2026
Article

OXFORD

Domestic and international approaches to combating ransomware: between contradiction and coherence

Tsvetelina J. van Benthem[1,2], Roxana Radu [3*]

[1]School of Law, University of Reading, Whiteknights Road, Reading, Berkshire RG6 6EP, United Kingdom.
[2]Oxford Lifelong Learning, University of Oxford, 1 Wellington Square, Oxford OX1 2JA, United Kingdom.
[3]Blavatnik School of Government, University of Oxford, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, United Kingdom
*Corresponding author. Blavatnik School of Government, University of Oxford, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, United Kingdom. E-mail: roxana.radu@bsg.ox.ac.uk

Abstract

Ransomware is one of the greatest threats facing contemporary societies. Its harms are widespread and diverse, impacting physical assets, physical and psychological well-being, as well as trust in domestic and international institutions. To counter the ransomware threat, states have adopted a range of measures—from resilience-building at home to extraterritorial enforcement. These measures do not only have domestic implications. They have various touchpoints with international law. In some cases, especially in relation to extraterritorial law enforcement, they may come into tension with international obligations protecting state sovereignty. In others, states may be required by law to take positive measures to protect the rights of individuals and other states. States must take care in crafting domestic responses, as such responses must not conflict with obligations undertaken under international law. This paper explores the interaction between these domestic measures and relevant international obligations, with concrete examples from domestic practice and state signalling at the inter-governmental level.

Keywords enforcement, human rights, international law, ransomware, resilience, sovereignty

INTRODUCTION

Imagine that your country's main healthcare provider just became a victim of ransomware. The criminals exploited a credentials vulnerability and gained access to the provider's data, locking out users from half of the state's hospitals. Emergency services cannot proceed, scheduled operations are delayed. Beyond the direct physical impact on patients, there is a society-wide psychological effect—an uncertainty over access to essential medical services. Should the healthcare provider pay the ransom? Would the ransom payment be used to fuel additional ransomware incidents or other criminal activity? How are the interests of individuals, organizations and the state to be balanced, especially in the calculation of concrete, tangible harms of non-payment and reasonably foreseeable future consequences of payment?

The criminal group operates from a foreign jurisdiction, with all key operatives out of reach to the victim state's law enforcement. While the victim state is a member of counter-ransomware international initiatives and a party to treaties on mutual assistance in legal matters, the state harbouring the ransomware group refuses to collaborate. What, if anything, can the victim state do to redress the harm and prevent further ransomware targeting its essential services?

It is not difficult to imagine this scenario playing out in real life. Real-world cases of ransomware harm abound. The 2017 WannaCry operation, which affected over 300 organizations in 150 countries, including NHS hospitals in the UK,[1] was an early wake-up call to the severity of ransomware. In early 2025, it was reported that there has been a 300 per cent increase in ransomware attacks on healthcare since 2015.[2] In 2024, pathology testing organization Synnovis was targeted by ransomware, with consequences for the operation of major London hospitals.[3] The 2022 ransomware attack against Costa Rica had a disproportionate impact on its healthcare sector.[4] As affirmed by the Director-General of the World Health Organization, ransomware operations against hospitals and healthcare systems have become issues of life and death.[5]

Despite the clear harms—some already manifested, some foreseeable—states have struggled to find strategies at the domestic and international level that effectively counter ransomware groups and prevent or mitigate the operations' consequences. In their attempt to counter ransomware, they have, on the one hand, developed domestic measures to build resilience and bolster enforcement, and, on the other hand, signalled their understanding of international law's applicability and content through national positions and statements at inter-governmental fora. But the two directions of action are not separate. As states craft their domestic measures to combat ransomware, they must be mindful of the boundaries imposed by international law and stay within these boundaries. This article aims to shed light on the international legal framework that shapes the contours of lawful measures that states

[1] Emerge Digital, The WannaCry attack and the NHS, available at: <https://emerge.digital/resources/the-wannacry-attack-and-the-nhs/>.

[2] IBM, 'When Ransomware Kills: Attacks on Healthcare Facilities', available at: <https://www.ibm.com/think/insights/when-ransomware-kills-attacks-on-healthcare-facilities>.

[3] BBC, 'NHS Confirms Patient Data Stolen in Cyberattack', 24 June 2024, available at: <https://www.bbc.co.uk/news/articles/c9777v4m8zdo>.

[4] CyberPeace Institute, Statement: Cyberattack against the public health service in Costa Rica, 2 June 2022, available at: <https://cyberpeaceinstitute.org/news/statement-cyberattack-against-the-public-health-service-in-costa-rica/>.

[5] UN, 'Ransomware Attacks on Healthcare Sector "Pose a Direct and Systemic Risk to Global Public Health and Security," Executive Tells Security Council', SC/15891, 8 November 2024, available at: <https://press.un.org/en/2024/sc15891.doc.htm>.

can—or must—take to fight the ransomware threat. In doing so, the article also considers a number of measures already taken by states at the domestic level and analyses them against the background of international law. It emphasizes the importance of coherence between the domestic and international levels, as any contradictions may be seen as undermining the international legal system, and the viability of international law as a tool for shaping responsible state behaviour.

The article is structured into four sections. Following this introduction, it turns to a description of the ransomware threat, highlighting its particularities compared to other harmful cyber activities (Part II). It then examines the interaction between domestic and international approaches to ransomware (Part III). Finally, the analysis turns to the content of international law, with key obligations relevant to the fight against ransomware. This section, therefore, advances a framework for navigating the boundaries that international law imposes on the freedom of states to undertake domestic action (Part IV). A final section concludes (Part V).

FIVE CHALLENGES TO COMBATING RANSOMWARE

Ransomware, understood as a form of malware designed to take control of a target's assets, with assets rendered unavailable until a demand is met,[6] is one of the main challenges facing international society. Its magnitude, flourishing criminal ecosystem and capacity to wreak societal havoc have all made it central in international discussions on combating harmful cyber behaviour. At the same time, it must be borne in mind that ransomware is not *unique* in either its methods or harms. Indeed, many features of the ransomware threat can be analogized to other phenomena, such as extortion (whether cyber-enabled or not) or any cross-border cyber criminality.

This explains why states have so far shied away from ransomware-specific legislation at the domestic level and the development of ransomware *lex specialis* at the international level. For instance, states seldom specifically single out ransomware in their national positions on the application of international law to cyberspace. Their general review of legal obligations —which would apply to any other cyber operation—applies to the ransomware threat, and ransomware is sometimes used as an illustration of unlawful conduct. Thus, ransomware operations are used as illustrations in the 2024 position of Austria (in the section on due diligence),[7] the 2024 position of the Czech Republic (in the section on sovereignty)[8] and the 2023 position of Costa Rica (in the sections on sovereignty, intervention, due diligence

[6] 'Oxford Statement on International Law Protections in Cyberspace: The Regulation of Ransomware Operations' (2021), available at: <https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-ransomware-operations/#:~:text=3.-,States%20must%20refrain%20from%20conducting%2C%20directing%2C%20authorising%20or%20aiding%20and,and%20opinion%2C%20freedom%20of%20expression%2C>.

[7] Republic of Austria, 'Cyber Activities and International Law' Position Paper (April 2024) 11. Example of the principle of 'due diligence': 'State A is aware of a criminal hacker group operating on its territory and targeting other states. The group is conducting a cyber attack against state B, encrypting all the files of state B's Ministry of Foreign Affairs and requesting a ransom payment. State B is able to trace the activity to state A, but is unable to clearly attribute the attack to state A. It notifies state A of the cyber activity by the group emanating from state A's territory. State A rejects the allegation and refuses to investigate the conduct on its territory. Thereby, state A violates its due diligence obligation.'

[8] Czech Republic, 'Position Paper on the Application of International Law in Cyberspace' (2024) para 6(c). Example used in the section on sovereignty: 'a cyber operation interfering with any data or services which are essential for the exercise of inherently governmental functions, and thereby significantly disrupting the exercise of those functions; for example, distributing ransomware which encrypts the computers used by a government and thus disables the payment of retirement pensions or other social benefits.'

and attack).[9] Ransomware is also reviewed generally to demonstrate the scale and severity of the cyber threat, as well as its impact on international peace and security, for instance in the Common position of the European Union.[10] A further example of the general approach taken by states can be found in the negotiations on the newly adopted UN Convention on Cybercrime, which does not contain a specific provision on ransomware, though ransomware is captured under a number of its provisions on unlawful access and interference with data.[11]

Even if the characteristics and consequences of ransomware are not unique, its rise has highlighted important challenges to combating harmful cyber operations more generally. Existing research identifies a range of distinct challenges posed by ransomware. These challenges can be synthesized into five interrelated categories that impede effective prevention and mitigation: (1) the variety of harms and vulnerabilities; (2) its direct and indiscriminate effects; (3) the complexity of its criminal ecosystem; (4) the enforcement gap; and (5) its nature as a collective action problem.

A variety of harms and vulnerabilities

Ransomware not only affects its direct victims. It has wide-ranging and pervasive effects for both individuals and society as a whole.[12] Wider societal consequences are also notable beyond the immediate disruption of services, as recovering from a ransomware attack also diverts valuable resources from other priorities.[13] One of the most pernicious societal effects of ransomware is the constant sense of insecurity,[14] coupled with a normalization of cybersecurity breaches. Through that sense of insecurity, trust in governments[15] and their capacity

[9] Costa Rica, 'Position on the Application of International Law in Cyberspace' (2023) paras 20, 25, 28, 49. Examples: 'loss of functionality may occur if the operating system or database upon which the targeted cyber infrastructure relies stops functioning as intended, as may be the case, for instance, as a result of ransomware' in the section on sovereignty; '[a] prominent example of a breach of non-intervention are ransomware attacks crippling or simply interfering with a State's ability to run public services, such as finance, education, and social security. Moreover, foreign election interference may also infringe the principle of non-intervention' in the section on non-intervention; in the section on due diligence, '[i]t covers acts that contravene the sovereign rights of another State, such as ransomware and cyber electoral interference, whether or not these are perpetrated by a State or a non-State actor', and in the section on attack under international humanitarian law, '[i]n Costa Rica's perspective, encrypting data through ransomware, despite being temporary and reversible, would be considered an attack under IHL and therefore must not be directed against civilian systems.'

[10] Council of the European Union, Declaration on a Common Understanding of International Law in Cyberspace, 18 November 2024, Introduction.

[11] 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, Res 79/243, 24 December 2024, available at: <https://www.unodc.org/unodc/en/cybercrime/convention/home.html>.

[12] Pia Hüsch and others, '"Your Data is Stolen and Encrypted": The Ransomware Victim Experience', RUSI Occasional Paper, July 2024; Finnish Police, 'Criminal Investigation into Vastaamo Hacking Case to be Completed in Late Summer—Police Urge Victims to Fill in Statement Form' (2023) <https://poliisi.fi/en/-/criminal-investigation-into-vastaamo-hacking-case-to-be-completed-in-late-summer-police-urge-victims-to-fill-in-statement-form> accessed 10 December 2025.

[13] Jamie MacColl, Pia Hüsch and Jason RC Nurse, 'Beyond the Bottom Line: The Societal Impact of Ransomware' RUSI, 13 November 2022, available at: <https://www.rusi.org/explore- our-research/publications/commentary/beyond-bottom-line-societal-impact-ransomware>.

[14] Home Office, 'The Experiences and Impacts of Ransomware Attacks on Individuals and Organisations' (2025), available at: <https://www.gov.uk/government/publications/the-experiences-and-impact-of-ransomware-attacks-on-victims/the-experiences-and-impacts-of-ransomware-attacks-on-individuals-and-organisations>.

[15] Ryan Shandler and Miguel Alberto Gomez, 'The Hidden Threat of Cyber-attacks—Undermining Public Confidence in Government' (2022) 20 J Info Tech & Pol 359-374, available at: <https://www.tandfonline.com/doi/full/10.1080/19331681.2022.2112796>.

to counter the ransomware threat can be eroded, with further downstream consequences for societal cohesion and democratic processes.

Furthermore, individuals, organizations, and societies may exhibit a range of vulnerabilities to such harms. Vulnerabilities to ransomware can take many forms. Some of them are institutional—the absence of adequate legal frameworks, regulatory guidelines and coordination between relevant actors can hamper both prevention and response to ransomware operations. The vulnerabilities can also be technical, and vested in the systems of individuals, the private sector, NGOs and state institutions.

So far, instead of being targeted, the majority of ransomware operations are opportunistic,[16] using automated attacks that indiscriminately target numerous systems using common exploits.[17] Absence of adequate security measures then allows access to a particular system. The vast majority of attackers exploit vulnerabilities in unpatched systems or remote access to systems without multi-factor authentication.[18] A missing culture of security in organizations, even in terms of basic cyber hygiene, can provide an opening for ransomware actors.

Given this, the only way to adequately counter ransomware harms is to adopt a whole-of-society approach[19] to prevention and recovery. A first step is to identify the particular vulnerabilities, which may require sufficient reporting from public and private organizations. Once vulnerabilities are mapped, states can focus on a strategy to patch them, and tailor contingency and recovery plans.

Direct and indiscriminate effects

Beyond the direct harms sought by ransomware criminals, a further challenge is ransomware's propensity for indiscriminate harms. For instance, the NotPetya cyber operation unleashed in the context of the conflict in Ukraine impacted networks worldwide, with estimated financial losses of 10 billion USD.[20] Another cyber operation, WannaCry, spread at a rate of up to 10,000 computers per hour and impacted both the private and public sectors around the world.[21]

When operations target IT supply chains, the breadth of impacted end users can be both significant and unforeseeable. The exploitation of one vulnerability can impact both a nursery and an electric power supplier, an e-Government platform and a hospital. In the current ransomware practice, there is a high reliance on defence evasion techniques, such as 'living-off-the-land' (using legitimate tools to deploy ransomware without raising security alerts) or living-off-trusted-sites (using legitimate cloud services to disguise command-and-control communications), thereby complicating detection and response. When financial gains are sought, ransomware operations tend to 'target the data or

[16] National Cyber Security Centre (NCSC) and National Crime Agency (NCA), 'Ransomware, Extortion and the Cyber-crime Ecosystem' (2023), p. 11, available at: <https://www.ncsc.gov.uk/files/White-paper-Ransomware-extortion-and-the-cyber-crime-ecosystem.pdf>.

[17] European Union Agency for Cybersecurity (ENISA), 'Understanding Cyber Threats in Transport' (Press release, 23 March 2023), available at: <https://www.enisa.europa.eu/news/understanding-cyber-threats-in-transport>.

[18] Rapid7. 2024 Threat Landscape Statistics: Ransomware Activity, Vulnerability Exploits, and Attack Trends.

[19] Joe Burton and Clare Lain, 'Desecuritising Cybersecurity: Towards a Societal Approach' (2020) 5 Journal of Cyber Policy 449–470, available at: <https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1856903>.

[20] NotPetya: A Columbia University Case Study, SIPA-21-022.1, available at: <https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf>.

[21] Maria F Prevezianou. 'WannaCry as a Creeping Crisis', in Arjen Boin, Magnus Ekengren and Mark Rhinard, *Understanding the Creeping Crisis* (Palgrave 2011).

infrastructure that has the highest impact on the operations of victims',[22] rendering both the method and the effects of many operations indiscriminate.

A complex criminal ecosystem

Ransomware actors operate in an increasingly professionalized ecosystem.[23] Ransomware is now offered as a 'service', with platforms such as RansomHub and Farnetwork removing barriers to access.[24] The cryptocurrency market is used to facilitate criminal transactions and obfuscate payment transits and destinations.

In this ecosystem, private and state interests are often enmeshed, with ransomware gangs operating with different degrees of proximity to state actors.[25] This, in turn, triggers difficult questions around the attribution of the behaviour of ransomware actors to states.[26] Some of these groups may operate as *de facto* organs of the state, completely dependent on the latter for their existence and operation though not formally recognized as such in law.[27] Other groups, entities and individuals may be independent from the state, but have some of their operations instructed, directed and controlled by it.[28] In both of these cases, we can speak of responsibility of the state *for* the conduct of the ransomware operation. In contrast, when states merely tolerate the operation of non-state criminal actors from their jurisdiction, the state will only be responsible for its own failure to prevent and stop activities harmful to the interests of other states and individuals.[29] Though conceptually clear, this framework becomes muddled in practice, where evidence of connections between non-state groups and a state may be sparse, and their alignment—economic, ideological or other—may be either planned or coincidental.

Within this complex criminal ecosystem uniting state and criminal interests, it becomes clear that, to be able to effectively counter ransomware, domestic and international law must be brought to bear on the entire criminal ecosystem.

Enforcement gaps

Crucially, ransomware groups often operate from safe haven jurisdictions that are unwilling to take decisive steps to dismantle them, thus impeding or effectively precluding traditional

[22] European Union Agency for Cybersecurity (ENISA), 'ENISA Threat Landscape 2024' (ENISA, 2024), p. 20, available at: <https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf>.

[23] Michael Bátrla and Jakub Harašta, '"Releasing the Hounds?" Disruption of the Ransomware Ecosystem Through Offensive Cyber Operations' (2022) Proceedings of the 14th International Conference on Cyber Conflict 96.

[24] European Union Agency for Cybersecurity, 'ENISA Threat Landscape 2024' (September 2024) 30 https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf (accessed 12 April 2025).

[25] Global Initiative against Transnational Organized Crime, 'The Rise and Fall of the Conti Ransomware Group' (27 June 2023), available at: <https://globalinitiative.net/analysis/conti-ransomware-group-cybercrime/>.

[26] The recognized 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 (acknowledgement and adoption)—International Law Commission, Articles on the responsibility of states for internationally wrongful acts (2001).

[27] Articles on State Responsibility, art 4, and ICJ, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide, Bosnia and Herzegovina v Yugoslavia*, Judgment, Merits, ICJ GL No 91, ICGJ 70 (ICJ 2007).

[28] Articles on State Responsibility, art 8, and ICJ, *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v US)* [1986] ICJ Rep [202].

[29] Vladyslav Lanovoy, *Complicity and Its Limits in the Law of International Responsibility* (Bloomsbury 2016).

law enforcement action.[30] Despite as increase in cross-border law enforcement operations since 2020, only a handful of countries participate, and the USA takes the lead in about 50 per cent of these initiatives.[31]

While this again emphasizes the need for more comprehensive responses to ransomware, it also brings to light the importance of geopolitical realities—allowing criminal groups to operate from one's jurisdiction can be a powerful tool to undermine the sovereignty of other states, while acting under a cover of deniability (that is, that the territorial state is unaware of the operation of these criminal groups, or that it lacks the tools to dismantle them). Moreover, there is a degree of convergence between cybercriminal ransomware operations and their strategic use by states, which renders international law enforcement increasingly more complicated.[32]

While some states are well-known for their harbouring of cyber criminals—the Russian Federation, Iran, and North Korea—the ransomware criminal ecosystem is spreading across the world. For instance, it has been reported that many cyberthreat actors involved in online scams reside in Nigeria.[33]

A collective action problem

Much like climate change, cybersecurity—and, on the flipside, cyber vulnerability—is a collective action problem. Given global inter-connectedness, vulnerabilities in systems located in one state can affect the security of individuals and organizations in another. Collective action problems require collective solutions. Yet, power imbalances and inequality in resources can affect the degree to which the international community of states, even if willing, can address the risk of ransomware. This, in turn, highlights the need for international collaboration, including on the level of capacity- and confidence-building.

International efforts, such as the International Counter-Ransomware Initiative,[34] seek to pool knowledge, build collective resilience and develop common policies to counter the threat. However, these initiatives are yet to bridge the 'capacity' gap, and also suffer from partial participation, with key 'sanctuary' states, such as Russia, remaining outside their framework.[35]

Beyond these collaborative initiatives, some states have added another—enforcement—dimension to the 'collective' nature of the threat and its response—the possibility of third-party countermeasures meant to induce the compliance of a wrongdoing state. According to some state views, such third-party measures can be taken at the request of an injured state, which, for instance, may struggle to protect itself,[36] or in the collective interest of the

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

[31] Virtual Routes. 2025, available at: <https://virtual-routes.org/ransomware-countermeasures-tracker/>.

[32] Virtual Routes. 2025, available at: <https://virtual-routes.org/pharos-report-no-3-ransomwares-new-masters-how-states-are-hijacking-cybercrime/>.

[33] Alexander Hinchliffe, 'Nigerian princes to kings of malware: the next evolution in Nigerian cybercrime' (2017) 5 Computer Fraud & Security 5.

[34] The International Counter-Ransomware Initiative is an initiative uniting more than 70 member states and organizations to build cross-border resilience and collectively disrupt and defend against cyber actors; see 'About' (*International Counter-Ransomware*), available at: <https://counter-ransomware.org/>.

[35] CSIS, Next Steps for the International Counter Ransomware Initiative, available at: <https://www.csis.org/analysis/next-steps-international-counter-ransomware-initiative>.

[36] President of Estonia: international law applies also in cyber space (May 2019); New Zealand, The Application of International Law to State Activity in Cyberspace (December 2020).

international community as a whole.[37] For instance, Estonia has suggested that collective countermeasures are lawful under international law, a view no doubt anchored in its own experience as a state injured by a crippling cyber operation.[38]

These five challenges make the study of ransomware a particularly apt one in connection to international law. They highlight the difficulties of attribution, the range of interests impacted—from state sovereignty to individual rights, and the importance of focusing on both positive obligations, that is, obligations to take protective measures, and negative ones, that is, obligations to abstain from particular behaviours. These challenges further explain the race to action against the ransomware threat, and at the same time, they caution against overreach. Before turning to the substantive analysis of relevant obligations under international law, and their application to types of domestic measures, the next section addresses the dynamics of interaction between the domestic and international levels.

DOMESTIC AND INTERNATIONAL APPROACHES TO RANSOMWARE: AN INTERPLAY

While measures to counter ransomware may be seen as primarily a matter for domestic law and policy, they necessarily implicate international legal frameworks. How states respond to ransomware individually and collectively must happen within the boundaries of international law. Action outside the confines of the law would only serve to delegitimize domestic action and erode the already fragile understandings achieved internationally. A commitment to the rules-based international order must apply both in times of calm and in times of crisis.

There are a number of nexus points between domestic responses and international law. For instance, as ransomware harms impact individual rights, responses that emphasize resilience-building can be seen as ways to discharge positive obligations arising under international human rights law. That ransomware operations constitute a significant threat to the enjoyment of these rights is acknowledged by states: '[w]hen hospitals, laboratories, and emergency services are paralyzed by ransomware, the impact extends beyond any single nation—placing patient lives at risk, destabilizing healthcare systems, and undermining trust in essential public services.'[39] More difficult are the interactions between domestic measures aimed at the extraterritorial enforcement of domestic criminal law and the substantive boundaries of permissible action drawn by the international legal rules of sovereignty, non-intervention and non-use of force. International law is therefore both an enabler and a disabler of domestic measures: it requires domestic measures but, in the same breath, constrains state responses to the ransomware threat.[40]

There are three main dimensions through which the interaction between domestic measures and international law can be analysed: (1) signalling of willingness to act; (2) methodology of law-making; and (3) responsibility for counter-ransomware action.

[37] Republic of Austria, 'Cyber Activities and International Law' Position Paper (April 2024); Ministry of Foreign Affairs of Colombia, 'Colombia's National Position on the Application of International Law in Cyberspace' (2025); Costa Rica, 'Position on the Application of International Law in Cyberspace' (2023).

[38] Lisandra Novo, '"Specially Affected States" Push for Collective Countermeasures' (2024) CyCon 2024: Over the Horizon, Proceedings of the 16th International Conference on Cyber Conflict, available at: <https://ccdcoe.org/uploads/2024/05/CyCon_2024_Novo-1.pdf>.

[39] EU Statement—UN Security Council: Briefing on Threats Posed by Ransomware Attacks against Hospitals and Other Healthcare Facilities, 8 November 2024, available at: <https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-un-security-council-briefing-threats-posed-ransomware-attacks-against-hospitals-and_en>.

[40] Tsvetelina van Benthem and Christian Tams, 'Regulating Ransomware Through International Law' (2024) Report of the Scottish Council on Global Affairs, available at: <https://scga.scot/wp-content/uploads/2024/02/Ransomware-Report-Final-January-2024.pdf>.

Signalling of willingness to act

Discussions of the international law regulation of cyberspace have provided a platform for signalling on the need to take decisive action to tackle cyber threats, and on the importance of international law in allowing and facilitating such action. Beyond the general signalling of illegality of certain types of cyber intrusion and harm, domestic perceptions of ransomware affect state interpretations of their international obligations. While it is true that national positions do not explicitly suggest that ransomware operations are shifting or specifying their interpretations of the law—as explained above, there is no *lex specialis* of ransomware—certain legal interpretations may be seen as implicitly tied to the ransomware threat.[41] Furthermore, 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.

Beyond the signalling on the contours of international law, there is signalling of responsibility. That is to say, the very framework of 'responsible' state behaviour implies that there are consequences to irresponsibility. If a state acts contrary to its international law obligations, it commits an internationally wrongful act and owes reparation to the injured state or the beneficiaries of the obligation. Illegality can be a basis for the invocation of state responsibility in front of international courts and other competent mechanisms. And, depending on the nature of the wrong, it can open up scope for the taking of response action, such as countermeasures and the use of force in self-defence. In other words, signalling of illegality is also signalling of willingness to bring the law to bear on wrongdoing states.

Methodology for determining the content of the law

Domestic measures are not consequence-free for the content of international law. To begin with, when it comes to customary international law, what states do domestically can qualify as state practice, one of the two elements for the identification of custom.[42] How they justify their domestic measures could also amount to *opinio iuris*, the second element of customary law. For treaties, such measures could constitute subsequent practice of relevance to the interpretation of particular provisions.[43]

This is well understood by states. The debates over the international law regulation of cyber threats, including ransomware, is not merely an exercise of clarifying existing international law. In fact, international law is silent on many aspects highlighted by contemporary cyber threats. There is a clear *lex ferenda* component to the intergovernmental conversation, with states investing in legal capacity-building to shape international law for the coming years. If a state confers authority to its law enforcement agency for cross-border collection of evidence without the consent of the territorial state of the evidence, then this is a practice of relevance to the content of the rules governing extraterritorial enforcement jurisdiction.

[41] 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.

[42] 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.

[43] Vienna Convention on the Law of Treaties, arts 31(3)(b) and 32; and International Law Commission, 'Draft Conclusions on Subsequent Agreements and Subsequent Practice in Relation to the Interpretation of Treaties' (2018).

An important dynamic within this methodological interaction is the possibility of inconsistency in the practice of states. For instance, a state that adopts a very strong and comprehensive sovereignty approach (in essence, prohibiting any extraterritorial access or effect) yet engages in cross-border operations would be sending mixed signals internationally due to its inconsistent practice. This can, in turn, minimize the value of its practice.[44]

Responsibility of states in taking measures

Beyond the impact of domestic measures on the methodology of identifying international law, domestic measures can, in and of themselves, constitute violations of international rules that entail the responsibility of the state taking them. Thus, if international law absolutely prohibits extraterritorial enforcement jurisdiction without the consent of the territorial state—and a state cannot resort to justifications—then the state whose law enforcement agencies or military do access systems extraterritorially will be responsible for an internationally wrongful act. Domestic measures can also implicate human rights both domestically and extraterritorially, in particular the rights to privacy and property.

Importantly, responsibility entails secondary obligations of cessation and reparation. This could, in turn, require states to amend their legal and regulatory framework, adjust the powers of their enforcement agencies, and provide reparation to those injured through restitution, compensation, and/or an offer of apology and acknowledgement of responsibility.

INTERNATIONAL LAW CONSTRAINTS ON DOMESTIC ACTION TO COUNTER RANSOMWARE

As societies continue to grapple with the ransomware threat, it has become clear that there is no one silver bullet to combating its criminal ecosystem and resultant harms. Instead, states have—at different paces and with different emphasis—adopted a whole-of-society approach, which includes collaboration intra-state (between relevant governmental units) and inter-state (through multilateral fora), measures for institutional and technical resilience, the establishment of an appropriate legal framework for criminal accountability and private-sector regulation. In developing these measures, states are also generating domestic practice that bears on the identification of international law, both treaty-based and customary.

Crafting these measures requires grappling with the prohibitions, requirements and permissions of international law. International law is a framework that both protects states and individuals against ransomware and constrains domestic action to counter it. This is because measures taken domestically can interfere with both the sovereignty of other states, undermining the principle of sovereign equality, and with human rights, undermining the rights of those under a state's jurisdiction when the state acts territorially or extraterritorially. Many domestic measures, and in particular those related to institutional cooperation, technical resilience-building, and international cooperation, cohere with the constraining rules of international law. One could go even further and suggest that these measures implement existing positive obligations under international law—under human rights law, cybercrime instruments, and the Corfu Channel due diligence customary rule.

At the same time, regulatory and legal measures with an extraterritorial component can come into tension and interfere with negative obligations binding states under international law. States may be particularly tempted to adopt such measures, as many ransomware actors

[44] International Law Commission, 'Draft Conclusions on the Identification of Customary International Law' (2018), Commentary to Conclusion 7(2), p 135.

operate from safe-haven jurisdictions beyond the reach of law enforcement authorities of target states. However, 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. As in most cases, such consent will not be forthcoming, the capacity of states to enforce their laws and bring consequences to bear on ransomware actors will be limited by international law.

Yet, some states signal an interest in a proactive 'offensive' approach to countering ransomware. It is public knowledge that the Australian Signals Directorate undertakes offensive cyber operations to support national security. One of the functions of the Directorate is to prevent and disrupt offshore cyber-enabled crime.[45] It has also been reported that the United States disrupted the criminal group REvil in 2021, hacking into the group's servers and forcing it to shut down.[46]

Such extraterritorial signalling and action could be aimed at shaping the content of existing law to allow such extraterritorial action, especially given the pixelated nature of many existing rules. However, if these measures are seen to conflict with existing law, then the state taking them will be held responsible, with the consequent obligations to cease the wrongful conduct and provide reparation.

The following sections will detail the analytical framework for thinking about the content of international law, as relevant and applicable to domestic measures to counter ransomware. As a first step, the analysis will turn to a number of primary rules of international law that may provide meaningful constraints to state conduct with an extraterritorial dimension. It will be explained that states may be able to resort to justifications (either in the primary rules themselves, or from the customary law of state responsibility) for their conduct. Finally, the article turns to the positive measures that states must take to protect state and individual interests from the ransomware threat.

Prohibitions

Tensions can arise when states seek to counter ransomware through measures that have extraterritorial effects, as such extraterritorial effects may interfere with the sovereignty of other states. International law offers robust protections of state sovereignty. It does so through a range of obligations that require state abstention from conduct that causes effects in the territory of other states, or otherwise interferes with their internal or external affairs. The prohibitions of the use of force, intervention, and extraterritorial enforcement all flow from the principle of state sovereignty. Furthermore, many states have by now asserted that there is a distinct self-standing obligation to respect state sovereignty with a scope that goes beyond the prohibitions on the use of force, intervention and extraterritorial enforcement. Depending on the type of domestic measure to counter ransomware envisioned and/or implemented, a number of these prohibitions may be engaged. This section reviews the content of these obligations to clarify how international law constrains states in their design and operationalization of extraterritorial counter-ransomware measures.

To begin with, under the Charter of the United Nations and reflected in custom, '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

[45] Australian Government, Australian Signals Directorate, 'ASD Corporate Plan 2023–24', available at: <https://www.asd.gov.au/about/accountability-governance/publications/asd-corporate-plan-2023-24>.

[46] Kristen Eichensehr, 'The Biden Administration Cracks Down on Ransomware' (2022) 116 AJIL 445, 449.

inconsistent with the Purposes of the United Nations'.[47] While states overwhelmingly agree that cyber operations whose scale and effects are comparable to the kinetic use of armed force would fall within the ambit of the prohibition, there are ongoing interpretative debates over the precise meaning of 'force'. As has been summarized in the CyberLaw Toolkit, 'there is emerging consensus that "a cyber attack that causes or is reasonably likely to cause physical damage to property, loss of life or injury to persons would fall under the prohibition contained in Article 2(4) of the UN Charter," including both direct and indirect consequences'.[48] As noted by Colombia, issues remain at the level of determining the precise threshold of force in cyberspace.[49] According to Australia, the determination of scale and effects 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'.[50] And France has opined that one cannot rule out that cyber operations without physical effects may, depending on the circumstances, be characterized as a use of force.[51] It is therefore conceivable that extraterritorial state action to disrupt ransomware groups, if causing certain effects—whether physical or not—could meet the threshold of the prohibition of the use of force, as enshrined in the Charter of the United Nations and customary international law.

Uses of force are particularly severe examples of intervention between states. Even if certain conduct does not meet the elements of the prohibition of the use of force, it could still qualify as a prohibited intervention. The obligation to abstain from coercive intervention in the *domaine réservé* of other states has been clarified by the International Court of Justice in the *Nicaragua* case.[52] While states agree that this customary obligation exists, they continue debating its substantive contours, and in particular the meaning of 'coercion'—as such and in its application to cyberspace. According to Milanovic, 'coercion' can be met by both interfering with the will of another state and by depriving it of its 'ability to control its sovereign choices'.[53] A wide conception of 'coercion' is present in the national position of the United Kingdom: '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'.[54] Especially if one adopts a 'deprivation of control' approach to the delineation of coercion, operations to dismantle ransomware groups extraterritorially could fall foul of the prohibition, especially if they are considered to deprive the territorial state of its control over enforcement action.

Furthermore, it is well-established under customary international law, as explained by the Permanent Court of International Justice in the *Lotus* case, that a state 'may not exercise its power in any form in the territory of another State' without a permissive rule to the

[47] Charter of the United Nations (adopted 26 June 1945, entry into force 24 October 1945) 1 UNTS XVI, art 2(4).

[48] CyberLaw Toolkit, Use of Force, available at: <https://cyberlaw.ccdcoe.org/wiki/Use_of_force>.

[49] Ministry of Foreign Affairs of Colombia, 'Colombia's National Position on the Application of International Law in Cyberspace' (2025).

[50] Australian Government, 'Australia's Submission on International Law to Be Annexed to the Report of the 2021 Group of Governmental Experts on Cyber'.

[51] French Ministry of the Armies, 'International Law Applied to Operations in Cyberspace' (2019).

[52] *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v US)* [1986] ICJ Rep [202].

[53] Marko Milanovic, 'Revisiting Coercion as an Element of Prohibited Intervention in International Law' (2023) 117(4) AJIL 601, 626–48.

[54] Attorney General, the Rt Hon Suella Braverman QC MP, 'International Law in Future Frontiers', available at: <https://www.gov.uk/government/speeches/international-law-in-future-frontiers>.

contrary.[55] Unless a state has consented to the exercise of enforcement jurisdiction on its territory, or international law otherwise confers such authority, extraterritorial enforcement action will be unlawful.[56] Extraterritorial access to digital evidence by law enforcement agencies for the purposes of domestic investigations and prosecutions of ransomware actors can also interfere with the rule against extraterritorial enforcement. Such access is increasingly becoming the norm rather than the exception, and states and other stakeholders have developed various approaches to tackle the 'cross-border data access problem'.[57]

And finally, many states have suggested that, in addition to the prohibitions outlined above, there is also a residual self-standing rule of sovereignty that constrains the causation of extraterritorial effects or interference with governmental functions.[58] The United Kingdom is an outlier in explicitly rejecting the existence of such a rule under customary law.[59] On the other end of the spectrum, the African Union adopts a very extensive view of the contours of sovereignty, suggesting that 'any unauthorized access by a State into the ICT infrastructure located on the territory of a foreign State is unlawful'.[60] Most states adopt a middle-ground approach by accepting the existence of the rule in custom yet conditioning it through a *de minimis* threshold. Thus, Canada has suggested that '[i]n assessing the possible infringement of a State's territorial sovereignty, several key factors must be considered. The scope, scale, impact or severity of disruption caused, including the disruption of economic and societal activities, essential services, inherently governmental functions, public order or public safety must be assessed to determine whether a violation of the territorial sovereignty of the affected State has taken place'.[61]

Depending on how a primary rule of sovereignty is delineated, it can provide more or fewer limitations on the freedom of states that seek to counter ransomware actors extraterritorially.

How do these rules relate to what states do domestically? A key component of some state responses to ransomware is the legal framework regulating enforcement under their domestic law. What can be observed in certain states is a more proactive approach to the disruption of the ransomware ecosystem, including through extraterritorial enforcement measures. Both Singapore and Australia have bolstered the powers of law enforcement and government agencies to ensure more operational tools are available to combat ransomware. Countries with advanced offensive cybersecurity capabilities, like Australia, are more inclined to adopt

[55] *SS Lotus (France v Turkey)* [1927] PCIJ Series A No 10, [45].

[56] Tsvetelina van Benthem and others, 'Jurisdiction in Cyberspace' (2024) Sino-European Expert Working Group on the Application of International Law in Cyberspace (EWG-IL), Research Group Report 2024, available at: <https://www.gcsp.ch/sites/default/files/2024-12/EWG-IL_Partnered_Jurisdiction_2024-11%3Bdigital.pdf>.

[57] Halefom H Abraha, 'Law Enforcement Access to Electronic Evidence Across Borders: Mapping Policy Approaches and Emerging Reform Initiatives' (2021) 29 International Journal of Law and Information Technology 118, 121–137.

[58] See, for instance, 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; Council of the European Union, Declaration on a Common Understanding of International Law in Cyberspace (18 November 2024); Ministry of Foreign Affairs of Colombia, 'Colombia's National Position on the Application of International Law in Cyberspace' (2025).

[59] Attorney General, the Rt Hon Suella Braverman QC MP, 'International Law in Future Frontiers', available at: <https://www.gov.uk/government/speeches/international-law-in-future-frontiers>: '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.'

[60] African Union, 'Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace' (February 2024), para 16.

[61] Government of Canada, International Law applicable in cyberspace (April 2022) para 14.

assertive tactics, proactively disrupting and dismantling cybercriminal networks. Australia stands out for its proactive measures in addressing cyber threats, particularly through the establishment of task forces aimed at disrupting cybercriminal networks beyond its borders. The country's commitment to leveraging defensive and active cyber defence capabilities is evident in both its domestic and international approaches. The suite of legal reforms (Parliament of Australia 2024) was foreshadowed in the 2023–2030 Australian Cyber Security Strategy.

Such approaches raise concerns over compliance with, at a minimum, the rule of sovereignty and the application of the prohibition of non-consensual extraterritorial enforcement jurisdiction. When the foreign state is deprived of control over its internal affairs, or the effects of the operation are comparable to kinetic uses of force, then the prohibitions against intervention and use of force will also be engaged. Of course, much would depend on the particular action taken at the domestic level and its extraterritorial effects. If one were to adopt the African Union approach to sovereignty, barely any extraterritorial acts of access would escape illegality under international law. If, on the flipside, one were to follow the United Kingdom in its rejection of sovereignty, it may be that certain actions with extraterritorial effects would be considered lawful.

Justifications

As stated above, 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. There are ongoing debates over the trigger of the right of self-defence—the gravity of the use of force required for it to rise to the level of armed attack, and the possibility of non-state armed groups launching such attacks. Under the orthodox restrictive view of the content of self-defence, states can act in self-defence only where an armed attack is attributable to another state.[62]

The law of state responsibility provides a further array of justifications under the customary regime of circumstances precluding wrongfulness.[63] Of particular import to our analysis are countermeasures and necessity. Countermeasures are response measures that breach international obligations. They would themselves be unlawful but for the prior internationally wrongful act of the responsible state against which the countermeasure is taken. Because countermeasures may be particularly prone to abuse, they are conditioned by a number of stringent requirements.[64] Thus, countermeasures cannot be punitive—their aim must be to induce compliance with international obligations. They must also be proportionate, and must not affect a number of foundational obligations of international law, including the obligation to refrain from the threat or use of force enshrined in the Charter of the United Nations and obligations for the protection of fundamental human rights. States must also comply with the procedural preconditions of sommation and notification. In the context of ransomware, states could have a basis to resort to countermeasures not only against states that themselves conduct ransomware but also against those that harbour criminal groups in contravention of their obligations under international due diligence

[62] For instance, the African Union has adopted this restrictive view in its common position—African Union, 'Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace' (February 2024), para 43.

[63] International Law Commission, Articles on the responsibility of states for internationally wrongful acts (2001), arts 20–27.

[64] Talita Dias, 'Countermeasures in International Law and Their Role in Cyberspace' (2024) Chatham House Research Paper, 9–32.

obligations. State practice from recent years suggests a growing acceptance that states not injured by a particular wrongful act can take countermeasures in the collective interest.[65]

Beyond countermeasures, states could also rely on necessity as a circumstance precluding wrongfulness. What is notable about the ground of necessity is that it does not require a prior unlawful act: the act must be the only way for the state to safeguard an essential interest against a grave and imminent peril, and it must 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] It is a ground that can be asserted vis-à-vis conduct of non-state actors.[67] Some states and organizations have already addressed necessity in their positions on the application of international law to cyberspace. The Netherlands clarifies 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.'[68] The European Union adds that '[i]n the cyber context, an interest may be considered essential on account of the type of infrastructure actually or potentially targeted by a cyber operation and when that infrastructure is relevant for the State as a whole'.[69]

What can be gleaned from the analysis here is that there are certain inevitable tensions between extraterritorial state conduct and the sovereignty-related rules of international law. At the same time, at least some states are signalling their willingness to act decisively against ransomware actors harboured in safe-haven jurisdictions. How states want to respond to such groups impacts how they interpret the relevant treaty and customary rules, thereby exerting an influence on the content of international law, as it evolves through time. And finally, states must bear in mind that their extraterritorial actions may themselves be unlawful—when they breach their obligations in circumstances where they cannot rely on justifications. Whatever is undertaken at the national level must therefore be closely aligned with the boundaries of existing international law.

Positive obligations

In the previous sections, it was shown how international law can be breached by state action with extraterritorial effects. Sometimes, international law can be breached through *inaction*. This is when international law imposes obligations on states to undertake a particular behaviour, known as positive obligations. Such positive obligations exist under different legal regimes and under different sources of law—treaties and custom. Under international human rights law, for example, states must take positive steps in cases of foreseeable risks to particular rights of individuals under their jurisdiction. These measures must prevent the risk, mitigate its effects, or bring responsibility to bear for harms suffered. Importantly, such positive

[65] For instance, in the context of measures responding to Russia's aggression against Ukraine, Philippa Webb, 'Legal Options for Confiscation of Russian State Assets to Support the Reconstruction of Ukraine', Study of the European Parliament (2024), available at: <https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2024)759602>.

[66] International Law Commission, Articles on the responsibility of states for internationally wrongful acts (2001), arts 20–27.

[67] CyberLaw Toolkit, The plea of necessity, available at: <https://cyberlaw.ccdcoe.org/wiki/Plea_of_necessity>.

[68] Government of the Kingdom of the Netherlands, 'Appendix: International Law in Cyberspace' (2019) 7–8. See also Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views' (2020) The Hague Program for Cyber Norms Policy Brief, pp 20–21.

[69] Council of the European Union, Declaration on a Common Understanding of International Law in Cyberspace (18 November 2024) p 12.

obligations compel states into action even where the risk originates in the conduct of a non-state actor.[70]

Specification of such positive obligations has been given by the Human Rights Committee, interpreting the right to life under the International Covenant on Civil and Political Rights. The Committee has clarified that the obligation to take positive, reasonable measures in response to 'reasonably foreseeable threats to life' is one of due diligence nature, not meant to impose disproportionate burdens on states.[71] Positive obligations also arise under other rights, such as the right to privacy.[72] Importantly, when states fail to discharge these positive obligations, they are themselves responsible for an internationally wrongful act.

The international human rights law framework is a particularly apt one for thinking about ransomware harms, as it is always possible to individualize the impact on a person—on their property, privacy, life, health, and education. There is no prescriptive list of measures that must be implemented to discharge these human rights obligations in each and every case and across contexts. As we see from domestic measures, there are a variety of ways to protect individuals from ransomware harms.

For instance, an effective way of protecting individuals is ensuring that there is a coherent institutional framework protecting their rights. In a number of countries, including Australia, Costa Rica, France, and Singapore, efforts are being made to streamline and centralize responsibility for ransomware mitigation for critical infrastructure. Streamlining authority through cross-departmental units not only facilitates continuous communication but also supports stronger data-sharing among trusted networks. At the same time, developing such institutional structures can be difficult for states that struggle with a lack of resources. Costa Rica, for instance, is yet to develop a fully-fledged institutional framework for tackling cybersecurity challenges.[73]

Furthermore, states can safeguard rights by developing robust regulatory measures. These regulatory measures can capture a wide variety of conduct, focusing on the implementation of rules, guidelines, and compliance mechanisms to enforce cybersecurity standards and practices across the public and private sectors, through rules, compliance mechanisms, incident reporting, audits, and adherence to regional frameworks to ensure resilience and preparedness. Debates over the most effective and appropriate regulatory framework(s) for combating ransomware have been ongoing at the national level for years.

One aspect of the debate centres around the role of ransomware insurance as a tool to mitigate attacks. On the one hand, cyber insurance can act as governance, making insurance contingent on higher security standards in organizations.[74] In this way, it can incentivize good practices of risk management within public and private entities. More straightforwardly, cyber insurance can offset financial risks and reduce concerns over the discontinuance of operations. On the other hand, cyber insurance could be seen as a potential contributor to the criminal ecosystem, emboldening criminals.[75] There is also a clear nexus between

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

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

[72] Human Rights Committee, 'General Comment 16 on the Right to Privacy' (1988) paras 9–11.

[73] Roxana Radu, 'Countering Ransomware: Government Responses in a Comparative Perspective' 2025). *Cycon 2025: The Next Step*, Proceedings of the 16th International Conference on Cyber Conflict, available at: https://ccdcoe.org/uploads/2025/05/CyCon_2025_The-Proceedings-of-the-17th-International-Conference-on-Cyber-Conflict.pdf.

[74] Gareth Mott and others, 'Between a Rock and a Hard(ening) Place: Cyber Insurance in the Ransomware Era' (2023) 128 Computers & Security.

[75] Asaf Lubin, 'The Law and Politics of Ransomware' (2022) 55 Vanderbilt Journal of Transnational Law 1177.

insurance regulation on the domestic level and international legal obligations—ransom payments made through insurance can fall into the hands of sanctioned entities, including terrorist organizations. In France, this debate has shaped the regulatory approach to allow the insurability of cyber ransoms under the Orientation and Programming Law of 2023. However, this is strictly contingent on reporting the incident to authorities within 72 hours, a requirement that strikes a balance between risk mitigation and accountability.[76]

Another regulatory route is the potential introduction of reporting requirements in cases of ransomware incidents. What such requirements aim to tackle is under-reporting, which has effects on states' understanding of the vulnerabilities of domestic entities, the modalities of ransomware attacks and the evolving criminal ecosystem. Mandatory reporting is increasingly viewed as a solution to these challenges. In the EU, the NIS 2 Directive introduces stricter reporting obligations for entities across critical and essential sectors, requiring them to notify national authorities of significant cybersecurity incidents within 24 hours of detection. This directive is a key component of the EU's regulatory stewardship on cybersecurity, aiming to harmonize practices across member states to ensure a higher level of resilience and preparedness. In Australia, the Cyber Security Bill mandates reporting of ransomware payments to the Australian Signals Directorate within 72 hours.

Finally, states can seek to disincentivize ransomware groups by criminalizing ransomware activity. Debates have arisen at the domestic level on the question of criminalization of ransomware, as such (including different forms of participation in ransomware, including complicity), and of ransom payments, on the one hand, and on the legal powers of law enforcement to dismantle ransomware groups, on the other. On the application of a criminal framework to ransomware, a first question is how best to regulate this offence—as a self-standing ransomware criminal one, or as a general cyber offence related to illegal access and/or extortion. It has been argued that a ransomware-specific criminal offence can only provide a snapshot in time of the type of harmful conduct: the constantly evolving nature of ransomware requires a time-proof approach focusing on its characteristic means and harms. In Australia, national discussions on the topic date back to 2021. In accordance with the Australian Ransomware Action Plan, the 2024 Cyber Security Bill introduces a stand-alone offence for all forms of cyber extortion and a stand-alone offence for cybercriminals targeting critical infrastructure.

Beyond the criminalization of the offence of ransomware, there is a related discussion over the legal regulation of the cryptocurrency infrastructure that facilitates ransomware money-laundering. Cryptocurrency exchanges facilitate the conversion of illicit crypto ransoms into real-world currency.[77] By criminalizing the use of cryptocurrencies in ransomware payments, authorities aim to disrupt the flow of illicit transactions, making it more difficult for cybercriminals to launder money and profit from their activities. This includes measures such as requiring cryptocurrency exchanges to comply with anti-money-laundering regulations, conducting thorough know-your-customer checks, and monitoring suspicious transactions.

In addition to institutional coordination and regulatory measures, states can ensure rights by mainstreaming technical resilience. Such resilience is a key vector in countering ransomware. It can work both at the entry stage (making the success of a ransomware exploit less

[76] Ministère de l'Économie, des Finances et de l'Industrie, 'Lettre de la DAJ—La loi d'orientation et de programmation du ministère de l'Intérieur' (2023), available at: <https://www.economie.gouv.fr/daj/lettre-de-la-daj-la-loi-dorientation-et-de-programmation-du-ministere-de-linterieur>.

[77] Alexandra Alper, 'Biden Sanctions Cryptocurrency Exchange over Ransomware Attacks' (*Reuters*, 21 September 2021), available at: <https://www.reuters.com/business/finance/biden-sanctions-cryptocurrency-exchange-over-ransomware-attacks-2021-09-21/>.

likely) and at the recovery stage (creating tools for swift operation of systems despite a successful ransomware attack). Across states, there is a shift towards regulatory measures that mandate the implementation of 'security by design' principles across all sectors, thereby complementing and enhancing previously established guidelines. In France, it happens in part through transposing the European NIS 2 Directive, whereas in Singapore and Australia, it is supported by legal reforms passed in 2023 and 2024.

Domestic government action has focused not only on proactive defence but also on rapid recovery, to ensure swift organizational rebound following a breach. For example, in 2022, Singapore's Cyber Security Agency released an updated Cybersecurity Code of Practice to aid critical infrastructure owners in countering cyberattacks and enhancing public-private collaboration. Similarly, the Australian Cyber Security Centre offers technical advice and a free Cyber Security Assessment Tool in accordance with the Ransomware Action Plan 2021 (Department of Home Affairs 2021). These efforts are further supported by initiatives aimed at building societal resilience, such as Singapore's centralized ransomware portal and Costa Rica's national cybersecurity education plan. Costa Rica's national strategy on digital transformation (2023–2027) is specifically anchored in the experience of recovering from the Conti attack and presents a comprehensive vision of cybersecurity preparedness.

As this overview demonstrates, states have already taken many measures that cohere with human rights demands and operationalize protections. There are two main considerations that must be borne in mind.

First, the adoption of such measures is not discretionary, as international obligations demand state action. 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'.[78] And the United Nations Convention on Cybercrime, upon entry into force, would impose a number of substantive criminalization obligations and jurisdictional, enforcement and institutional ones on its parties. 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. Adopting an obligation lens to such measures can also open the door to mechanisms for international enforcement. For instance, subject to meeting jurisdictional and admissibility criteria, individuals can claim their rights in front of human rights bodies, such as the Human Rights Committee and the African, European and Inter-American courts of human rights, and the Cybercrime Convention also enables states parties to continuously discuss compliance with the terms of the Convention.

Second, these positive obligations arising under international law are subject to the capacity of the state. Even a glimpse at the state measures reviewed above shows that they are resource-demanding and could impose disproportionate burdens on developing states. This is why international cooperation is necessary to enable all states to protect those under their jurisdiction—and, by extension, other states—from the threat of ransomware. In many ways, the discussions around cybersecurity and cyber preparedness are also about fighting the inequalities of the international system.

Looking ahead, states should clarify the content of positive obligations in particular contexts of their application. In this way, there will be better foreseeability of what a state owes—that is to say, what regulatory, institutional and cybersecurity measures, among others, can be demanded as a matter of *law*.

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

CONCLUSION

This paper explored the nature of the ransomware threat, and the main challenges it poses to states and other stakeholders. Ransomware exposes existing vulnerabilities, creates new ones and generates whole-of-society harms. Because of the often extraterritorial nature of the ransomware threat, states are impeded from traditional territorial law enforcement action, leading to the under-implementation of the law. Importantly, ransomware is a collective action problem: a vulnerability in one state can lead to harms in another, and countering ransomware meaningfully can only be done with international partners.

Given these challenges, states have begun to adopt a range of national measures to combat ransomware—to protect their own interests, and those of persons under their jurisdiction and other states. The measures range from institution-building and establishment of legal frameworks to offensive cyber operations aimed at disrupting the threat and ensuring domestic resilience. In establishing and implementing these measures, states must remain mindful of their commitments under international law, especially at a time when the international system is coming under increasing strain.

Coherence between domestic responses to ransomware and international obligations is of particular significance to the international legal system and its role in constraining technologically-enabled harms. Achieving such coherence requires a genuine commitment to international law through investment in expertise and inter-state cooperation.

States must, first, design any domestic measures following careful consideration of their legality under the various relevant and applicable international legal frameworks. Domestic discussions on the design of national measures must involve relevant stakeholders from different governmental and other state structures to ensure a streamlined and consistent approach.

Second, states must invest in deep-dive clarification of relevant international law at the inter-governmental level. The contours of many international law rules remain blurry, and the ransomware ecosystem thrives in the grey areas of legal uncertainty. Further clarification efforts would thus strengthen legal certainty and predictability in the international system, and could exert a deterrence effect on potential wrongdoers. For instance, further research is needed on the interplay between the prohibition of non-consensual extraterritorial enforcement jurisdiction and the rules of sovereignty, non-intervention and non-use of force, and the application of the existing legal framework to cross-border access to data and cross-border disruptive action.

Finally, states must invest in collaborative, inter-state approaches to combating the ransomware threat. It has already been shown that the most successful law enforcement action against cyber criminals is transnational enforcement action.[79] Joint training, pooling of cyber expertise and sharing of lessons learned can assist states that are yet to achieve high levels of resilience to cyber threats. International law, as a system of sovereign equals, is the

[79] For instance, Interpol, ''Avalanche' network dismantled in international cyber operation' (2016), available at: <https://www.interpol.int/en/News-and-Events/News/2016/Avalanche-network-dismantled-in-international-cyber-operation>; INTERPOL cracks down on global cybercrime networks (DigWatch, 12 June 2025), available at: <https://dig.watch/updates/interpol-cracks-down-on-global-cybercrime-networks>; Interpol, 'More than 300 arrests as African countries clamp down on cyber threats' (2025), available at: <https://www.interpol.int/en/News-and-Events/News/2025/More-than-300-arrests-as-African-countries-clamp-down-on-cyber-threats>.

most viable platform for cooperation among states. It must therefore be carefully preserved and respected—even in times of heightened risks.

Funding

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