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

Countering Ransomware: Government Responses in a Comparative Perspective

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

Abstract: Ransomware is currently a top national security threat in many countries around the world. From the disruption of critical infrastructure providers in the US in 2021 to the 2022 paralysis of governmental systems in Costa Rica, ransomware has affected millions of people as direct or indirect victims of extortion practices, data theft, and information access restrictions. Exploring how governments have responded to ransomware since its surge in 2020, this paper expands on current literature that analyzes individual incidents or isolated responses. By incorporating new data from four cases—Australia, Costa Rica, France, and Singapore—this study provides a comprehensive overview of global trends in ransomware mitigation. It introduces an analytical framework based on five levers, ranging from technical to political. The findings underscore a dual focus on improving government coordination through policy centralization and responsibility-sharing while reinforcing public-private partnerships. Across the cases examined, ransomware responses have been multifaceted yet closely aligned with each country's overall cybersecurity posture.*

Keywords: *ransomware, cybercrime, mitigation, national cybersecurity strategies, offensive capabilities*

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

1. INTRODUCTION

Since 2020, ransomware has disrupted critical sectors around the world, causing widespread societal and economic harm. The 2021 Colonial Pipeline attack was among the first to make the headlines in a series of hundreds targeting critical infrastructure. A ransomware group called DarkSide was behind this attack on the payment processing system of Colonial Pipeline, resulting in fuel shortages across the eastern United States and impacting millions of businesses and consumers (Kerner 2022; Easterly and Fanning 2023). Two weeks later, Conti's ransomware attack on Ireland's Health Service Executive crippled healthcare services nationwide, jeopardizing patient care and forcing the cancellation of critical medical procedures (Winder 2021). By 2022, ransomware had escalated to the level of national crisis, as seen in Costa Rica, where Conti's attack on government institutions forced the government to declare a "state of emergency," a first for a ransomware attack. Multiple government institutions, including the Ministry of Finance, had their essential services, such as tax collection and customs processing, disrupted for weeks (Murray 2022).

As this brief overview of highly disruptive incidents shows, ransomware attacks have not been confined to specific regions or sectors. They have permeated global systems, including critical supply chains, both physical and virtual. In July 2021, South Africa's Transnet fell victim to a ransomware attack that disrupted port operations, including the Port of Durban. Attackers used strains like "Death Kitty" to encrypt files, grinding logistics to a halt and illustrating the fragility of critical infrastructure (Njini and Viljoen 2021). That same month, a REvil attack on a key United States software vendor, Kaseya, exploited software vulnerabilities to infect more than 1,500 downstream companies. Retailers, manufacturers, and other businesses worldwide faced operational paralysis, including nurseries, schools, pharmacies, and supermarkets in 17 countries, from Sweden to New Zealand, revealing a "new threshold of collective vulnerability" (Radu 2021). Ransomware has firmly established itself as the dominant global cyber threat over the past four years (ENISA 2024), drawing significant international attention and rising on the political and diplomatic agenda. Its prominence grew conspicuously after the June 2021 Biden-Putin summit in Geneva, where it became a key focus of negotiations.

The highly lucrative and adaptable modus operandi of ransomware groups has been driven in large part by the rise of ransomware-as-a-service (RaaS) (Blessing et al. 2022). This model allows cybercriminals to lease advanced ransomware tools and take a cut of the profit, making sophisticated attacks accessible to those with minimal technical expertise. Double extortion—encrypting data while threatening to leak it—has become commonplace in cybercrime, as attackers move to directly blackmailing victims in some cases. RaaS has professionalized the industry, featuring specialized

roles like access brokers and distributors within structured networks (NCA and NCSC 2024). These platforms provide customer support and profit-sharing schemes, making ransomware scalable. Despite some operators shutting down (Murray 2022) or being arrested (NCA 2024), over 70 groups (Rapid7 2024; CyberInt 2024) continue to operate from jurisdictions with weak law enforcement cooperation, enabling them to act with impunity.

For these reasons, governments across the globe have faced significant challenges in keeping up with the increasing sophistication and expanding reach of cyberattacks. Despite efforts to combat these threats, cybercriminals are continuously evolving their tactics, swiftly adapting to new security measures in what has often been described as a perpetual game of "whack-a-mole" (NCA and NCSC 2024). This paper examines the public responses to these challenges between 2021 and 2024, offering a structured framework to analyze the levers available to governments. Section 2 delves into the rapid expansion of ransomware attacks, exploring their broader societal impact and the increasing recognition of the harm they inflict on individuals and critical infrastructure. Section 3 explores key policy and academic debates, setting the stage for the analysis by introducing the five levers examined in this study. Section 4 presents the findings, highlighting both commonalities and differences across four different jurisdictions. Finally, the concluding section summarizes the key insights and their broader implications.

2. UNDERSTANDING THE EVOLVING RANSOMWARE THREAT AND ITS HARMS

Despite increased sophistication, ransomware remains largely opportunistic. It relies mostly on "spray and pray" tactics—automated attacks that indiscriminately target numerous systems using common exploits and affecting all systems that lack security measures rather than precisely targeting particular ones. The vast majority of attackers exploit vulnerabilities in unpatched systems or remote access to systems without multi-factor authentication (Rapid7 2024). Only a small percentage resort to zero-day vulnerabilities, or faults not yet known to the manufacturers.[1] Since 2020, over 130 ransomware strains have been identified, with 95 percent of attacks targeting Windows-based systems (VirusTotal 2021). The number of reported active ransomware groups varies, depending on the source. CyberInt (2024) reports an increase from 68 groups in 2023 to 95 in 2024. Rapid7 identifies 75 active groups, including 33 new or rebranded ones. These groups extort their victims through data leaks, resulting in 5,477 posts across leak sites (Rapid7 2024). As of February 2025, Ransomwarelive (2025) documented 238 active ransomware groups.

1 A notable exception is the Clop group, which intensified its activities in 2023 by exploiting a single zero-day vulnerability that, they claimed, breached 130 organizations (Gatlan 2023).

Many of these groups operate on RaaS platforms, whose developers take a percentage of every successful ransom payment. Average payouts skyrocketed from US$812,380 in 2022 to US$1,542,333 in 2023 (Sophos 2023). Collaboration among ransomware gangs has further enhanced the capabilities of these attacks. LockBit provided a prime example of that in 2023, when it adopted 25 percent of leaked Conti code and released a newly built encryptor to replace its proprietary one (Constantinescu 2023). This cooperative approach, combined with the financial incentives of RaaS, turns ransomware into a criminal activity that keeps pushing boundaries.

Since 2020, the healthcare sector has been particularly vulnerable to ransomware attacks due to its reliance on sensitive data and legacy software. Healthcare systems, in particular, became attractive targets during the COVID-19 pandemic because of their critical nature: one in three health institutions reported at least one ransomware attack in 2020 (Mishra 2024). By 2024, the business services sector became the most targeted, accounting for 24.1 percent of ransomware cases, followed by retail at 15.2 percent and manufacturing at 10.5 percent. A notable shift from 2023 is a 50 percent increase in ransomware incidents within the construction industry, which rose to fourth place, ahead of the financial, education, and health-care sectors, which had been more heavily targeted in 2023 (CyberInt 2024).

In recent years, the harm caused by ransomware has started to be more clearly understood, though challenges in data availability and underreporting persist. Much of the available data is concentrated in the United States, which skews the broader global picture. Initially, reporting on ransomware focused predominantly on financial losses, such as extortion payments and business interruptions and recovery costs. However, there has been a growing recognition of ransomware's broader societal consequences and cyber harms, including disruptions to daily life and services, as well as erosion of public trust and internal morale (Agrafiotis et al. 2018). In a 2024 UN Security Council briefing, the director-general of the World Health Organization referred to ransomware attacks on hospitals and health facilities as "issues of life and death" (Mishra 2024).

These societal harms are now a focal point in academic and policy discussions on the topic, as researchers and NGOs have started collecting systematic data and exploring the experience of victims (MacColl et al. 2024; Virtual Routes 2025). The CyberPeace Institute (2021) has documented the short- and long-term effects of cyberattacks on healthcare, from the immediate disruptive impact on service and patient care to the less visible impact on the mental health of healthcare professionals and IT specialists. An academic study looking at the impact of the first ransomware incident to make the headlines—the WannaCry attack from 2017—showed a significant decrease in the activity of the hospitals infected across the National Health Service in England.

Over the week of the attack, there were 13,500 appointments cancelled, 1,100 fewer emergency department admissions, and 2,200 fewer elective admissions (Ghafur et al. 2019).

The broader consequences of ransomware extend beyond the immediate disruption of services, particularly within public sectors, where recovering from a ransomware attack also diverts valuable resources from other priorities (MacColl et al. 2022; Martin 2024). While the downtime or interruption post- attack can vary significantly—from an average of 24 days for businesses and organizations in the US (Statista 2024) to months in the case of Costa Rica (Murray and Srivastava 2022)—other effects last for years. Reduced trust in government has been evidenced in the aftermath of a ransomware attack against a Düsseldorf hospital, in particular among segments of the population exposed to the attack (Shandler and Gomez 2022).

However, there is no consistent data collection to allow for a comprehensive analysis. Existing research on the topic has offered fragmented and inconclusive evidence regarding the proactive measures adopted by technologically advanced nations (primarily the United States, the United Kingdom, and the European Union). My contribution addresses this major gap by examining evidence from four jurisdictions—Australia, Costa Rica, France, and Singapore—across four continents. These four countries have various levels of cybersecurity maturity, regulatory stewardship, and resilience. All four have publicly acknowledged the threat that ransomware poses to national security, as a first step in crafting their ransomware responses. Each country offers insights into varying levels of preparedness, legal framework development, and institutional arrangements designed to counter ransomware.

3. HOW HAVE GOVERNMENTS RESPONDED?

Despite abundant policy documents and measures to counter ransomware, research on what has guided the government responses remains sparse. Many case studies of previous ransomware attacks have been used as evidence to prioritize the focus on protecting critical infrastructure, particularly in Australia and the UK (Department of Home Affairs, 2021; UK Government, 2024). The existing scholarly literature primarily identifies general trends and debates, yet it offers limited insight into how these are translated into concrete government actions. This section clarifies what has materialized so far and how these elements inform the identification of relevant levers in government action.

Three key debates on ransomware have structured the policy conversations and continue to underpin many of the policy tools under discussion around the world: 1)

criminalization of ransomware; 2) the role of ransomware insurance; and 3) mandatory reporting requirements. These debates introduce new variables for how to tackle the ransomware threat through legal, economic, and regulatory measures.

A. Criminalization of Ransomware and Crypto Payments

A major debate centers on whether ransomware should be recognized as a distinct criminal offense. This issue gained prominence during negotiations for the recently adopted UN Convention on Cybercrime. Proponents argue that ransomware's unique characteristics within the typology of cyberattacks, such as its extortion-based model and rapid evolution, justify criminalizing it as a specific offense (Robles-Carrillo 2023). Critics, however, caution that such an approach carries practical challenges, given the diverse and constantly evolving forms of ransomware (Robles-Carrillo 2023). In Australia, national discussions on the topic date back to 2021 (Department of Home Affairs 2021). In accordance with the Ransomware Action Plan, the 2024 Cyber Security Bill introduces a stand-alone offense for all forms of cyber extortion and a stand-alone offense for cybercriminals targeting critical infrastructure.

The association with cryptocurrency exchange action has been widely discussed, in an effort to target the financial infrastructure that enables ransomware actors to profit from their attacks. Cryptocurrency exchanges—typically underregulated—facilitate the conversion of illicit crypto ransoms into real-world currency (Alper 2021; TRM 2021). 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. Such measures are two- fold. On the one hand, they aim to reduce the effectiveness of ransomware campaigns by targeting the financial systems that support them; on the other, they seek to increase the accountability of cryptocurrency platforms in order to prevent their misuse. Targeted action in the area of payment tracing has shown significant progress in 2024 (Chainalysis 2025).

B. Role of Ransomware Insurance

The second debate concerns the role of ransomware insurance as a policy tool to mitigate attacks. Critics argue that it creates perverse incentives by fostering a private market for mitigation and encouraging ransom payments, which embolden cybercriminals (Dudley 2019; Lubin 2022). Insured businesses may also opt to pay ransoms quietly rather than report incidents, complicating law enforcement efforts (Blessing et al. 2022). By contrast, advocates emphasize the benefits of ransomware insurance, particularly for offsetting financial risks faced by large organizations.

Research by Mott et al. (2023) highlights how cyber insurance can act as governance, requiring organizations to meet higher security standards as a condition of coverage and rewarding good risk management. However, challenges persist, including rising loss ratios for insurers and ethical concerns over financing criminal groups (Pauch 2023). O'Connell (2023) advocates banning ransomware payment reimbursements altogether, arguing that this could deter future attacks. In France, this debate has shaped the regulatory approach to allow the insurability of cyber ransoms under the Orientation and Programming Law (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 (Ministère de l'Économie 2023).

C. Mandatory Reporting Requirements

The third debate addresses the issue of underreporting and the limited sharing of information about vulnerabilities, both of which hinder effective policy responses. 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 recently enacted Cyber Security Bill mandates reporting of ransomware payments to the Australian Signals Directorate within 72 hours.

D. A New Framework of Analysis

The debates presented above highlight the need to act at the legal and regulatory level. In addition to these dimensions, implementing technical measures and collaborating internationally to counter ransomware can be important levers for governments to tackle the complex challenge of ransomware. Building on these, the following framework of analysis was developed for this comparative study (Figure 1).

This framework is multi-dimensional, designed to encompass a wide array of strategies and policies adopted between January 2021 and September 2024, which are categorized as part of technical, institutional, regulatory, legal, or political levers. By mapping out these strategies, the framework enables a deeper understanding of how governments approach cybersecurity, particularly in the context of countering evolving threats like ransomware. The categorization is grounded in qualitative research, with data collected between April and September 2024 as part of the JFF project conducted at the University of Oxford.

FIGURE 1: FRAMEWORK OF ANALYSIS BASED ON FIVE LEVERS COVERING DOMESTIC AND INTERNATIONAL ACTION

Lever	Description
Technical	The deployment of advanced technologies and tools to prevent, detect, and recover from cyberattacks, including endpoint protection, intrusion detection, automated threat sharing, and backup solutions.
Institutional	The development and coordination of organizational frameworks, policies, and governance structures to define roles and responsibilities for effective ransomware response and recovery.
Legal	The application of laws and legal instruments to deter, respond to, and mitigate cyberattacks, including criminalizing ransomware, enabling cross-border investigations, and prosecuting ransomware actors operating in different jurisdictions.
Regulatory	The implementation of rules, guidelines, and compliance mechanisms to enforce cybersecurity standards and practices across the public and private sector, through rules, compliance mechanisms, incident reporting, audits, and adherence to regional frameworks to ensure resilience and preparedness.
Political	The role of political leadership in shaping national and international cybersecurity strategies, allocating resources, and fostering diplomatic efforts for global cooperation against ransomware.

By examining these dimensions, the framework provides valuable insights into the priority areas that governments are addressing, revealing the progress made in key areas such as legislation, institutional development, and international cooperation. Moreover, this comparative analysis reveals where different approaches fall along a spectrum that ranges from defensive to proactive strategies. Finally, this framework serves as a tool for assessing not just the actions taken by individual countries but also the broader trends in governmental responses to cybersecurity challenges.

4. FINDINGS

This section presents the findings of the study, illustrating how the four countries included in the analysis have approached the evolving ransomware threat and discussing their posture in comparative perspective. In doing so, it advances the scholarship on ransomware, which has primarily focused on individual incidents or isolated responses within a few Western jurisdictions. The new data presented here provides a more comprehensive understanding of global trends in ransomware mitigation, highlighting patterns in public responses to this persistent cybersecurity challenge. Starting from a summary of key developments in each jurisdiction (presented in Table I), I discuss commonalities and differences in ransomware mitigation strategies across the five identified levers. Subsequently, I reflect on the effectiveness of the measures adopted and recent changes in the ransomware ecosystem.

TABLE I: SUMMARY OF KEY DEVELOPMENTS (2021–2024) ACROSS FOUR JURISDICTIONS

Lever	Australia	Costa Rica	France	Singapore
Technical	Pressure testing critical systems Protecting the most valuable datasets Active cyber defense to fight ransomware	Tool for peripheral protection of ministries Periodic analysis of vulnerabilities Cloud computing solutions for public sector	Focus on domestic industrial capabilities and digital autonomy Separation of defensive and offensive capabilities in combating ransomware	Curated ecosystem of partners for local businesses One-stop ransomware portal Implementing protective DNS Plans to augment ransomware payment tracing capabilities Cybersecurity labeling scheme
Institutional	Executive Cyber Council (public-private threat info sharing) Cyber Incidents Review Board 2024	Cyber Cluster—improvement of cyber ecosystem (2022) Permanent national Security Operations Center (SOC-CR)	CyberCrisis Coordination Centre (since 2018)	Counter Ransomware Task Force (2022) CyberSG TIG Collaboration Centre and the Talent, Innovation and Growth Plan (2023) Government Cyber Security Operations Centre (2022), integrating the Government IT Security Incident Response
Legal	Data Disruption Warrants and Covert Access Obligation 2021 Cyber Security Bill 2024 Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024 Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024	Law 10500—Authorization of interception of cybercrimes • Contingency plans for ICT security in the public sector • Guidelines to reduce the impact and likelihood of ransomware and data extortion incidents in public and private organizations	Guidance and Planning Law of the Ministry of the Interior 2023 Law to secure and regulate the digital space 2024 Transposition of the EU Network and Information Systems Security Act (NIS2) 2024 Regulation on digital operational resilience for the financial sector (DORA) 2022	Online Criminal Harms Act 2023 Cybersecurity (Amendment) Act 2024

Regulatory	Mandatory ransomware payment reporting obligation Ransomware playbook	Strengthening of CSIRT-CR Public entities obligation to inform CSIRT about incidents	Reporting of incidents (NIS2) Major operational incident reporting obligation (DORA) Critical infrastructure obligations (NIS2) ANSSI can examine compliance with prevention measures	Mandatory cybersecurity Code of Practice for CII operators Licensing of cybersecurity service providers Plans to introduce mandatory obligation to report ransomware payment
Political	Revised National Cyber Security Strategy (2023–2030) Operation Aquila for cybercrime disruption A$9.9 billion committed to boosting AU Signals Directorate's offensive capabilities Co-lead of CRI pillar	National strategy on digital transformation 2023–2027 OAS, EU, CoE cooperation Bilateral agreements in Latin America and beyond CRI member	Stratégie d'Accélération Cybersécurité 2021 Coordination with the EU and NATO Follow-up work as part of the Paris Call (2018) CRI member	Singapore Cybersecurity Strategy 2021 ASEAN Voluntary Lead Shepherd on Cybercrime Chairing UN OEWG on Security of and In the Use of ICTs (2021–2025) Operationalization of the ASEAN regional CERT Co-lead of CRI Pillar

A. Commonalities

Across the four cases, a prominent trend is the consolidation of responsibility for ransomware mitigation for critical infrastructure—a departure from previous decentralized efforts in government. By 2024, enhanced horizontal coordination among ministries and public agencies had become essential for a comprehensive approach to ransomware and a more effective deployment of resources and expertise, as indicated in the revised national cybersecurity strategies of the four countries. Streamlining authority through cross-departmental units not only facilitates continuous communication but also supports stronger data-sharing among trusted networks. This aligns with legal mandates for incident reporting and increased protective responsibilities on providers of essential services.

The governments included in this study all recognize the key role of the private sector in safeguarding sensitive data and key services. Consequently, 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 NIS2 Directive, whereas in Singapore and Australia, it is supported by legal reforms

passed in 2023 and 2024. In addition to amendments to cybersecurity bills, both countries have bolstered the powers of law enforcement and government agencies to ensure more operational tools are available to combat ransomware (Department of Home Affairs 2021; Khan 2024).

Government action has focused not only on proactive defense 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.

Finally, all countries included in this study are members of the Counter Ransomware Initiative (CRI), which is currently the world's largest international cyber partnership between governments. Since its launch as a US initiative, the CRI has doubled its membership to over 70 states and refined its governance to enhance resilience, disrupt criminal operations, and shape policy. A key milestone was the 2022 establishment of the International Counter Ransomware Taskforce (ICRTF), which operationalized CRI efforts through intelligence sharing and industry collaboration. By 2023, CRI had evolved into an action-oriented framework - under US coordination – built around three pillars: Policy (co-leads: UK, Singapore), Diplomacy (co-leads: Germany, Nigeria), and ICRTF (co-leads: Australia, Lithuania). The 2023 summit advanced efforts against ransom payments, ransomware infrastructure, and illicit cryptocurrency flows while expanding mentorship for new members, AI-driven countermeasures, and incident response support (Dobell 2024). These actions have positioned the CRI as a credible international framework to develop collective ransomware mitigation strategies.

B. National-Level Variation

At the national level, there is considerable variation in the approaches adopted to counter ransomware, as each of the four countries developed a posture rooted in its own needs and circumstances. While Costa Rica focused extensively on cyber awareness and technical improvements, Australia pursued a disruption-centered direction in both its domestic coordination and international cooperation, particularly as lead of the CRI Disruption Task Force. France and Singapore combined their regional leadership with broader resilience approaches. The different postures and junctures are discussed in more detail below.

The qualitative analysis also reveals divergences along the defensive-offensive spectrum of ransomware responses. Countries with advanced offensive cybersecurity capabilities, like Australia, are more inclined to adopt assertive tactics, proactively disrupting and dismantling cybercriminal networks. By contrast, nations with less mature cybersecurity ecosystems, such as Costa Rica, focus primarily on defensive strategies aimed at enhancing resilience. Their efforts prioritize securing infrastructure, improving incident response mechanisms, and strengthening recovery systems. These variations underscore how national priorities, resource availability, and strategic capacities shape ransomware action.

In Costa Rica, two key public interventions have been prioritized since 2022: technical advancements (including cloud computing solutions for the public sector) and regulatory environment. The country'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. On the technical side, the country has been working on strengthening peripheral protection tools for public authorities. On the regulatory front, there has been a push to improve Costa Rica's ability to access information on cyber incidents and to enable more effective internal reporting. Despite some institutional progress, Costa Rica, like many other Latin American countries, still lacks a full-fledged institutional framework for tackling cybersecurity challenges. On its way to developing one, the nation has pioneered a national cybersecurity education plan.

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 defense capabilities is evident in both its domestic and international approach. The suite of legal reforms (Parliament of Australia 2024) was foreshadowed in the 2023–2030 Australian Cyber Security Strategy. Aside from the mandatory no-fault, no-liability ransomware reporting obligations, the Cyber Security Bill also enables the government to define mandatory security standards for "connectable products." Under the Security of Critical Infrastructure and Other Legislation (SOCI) Amendment Bill, the government has the power to direct an entity to take action in response to (cyber) incidents. These developments are complemented by technical measures to enhance the preparedness of critical systems and significant investments directed toward the Australian Signals Directorate. The Australian approach is thus both comprehensive and assertive, relying on a strong public-private partnership.

Like Australia, Singapore significantly strengthened its legal framework with the 2024 amendment to its Cybersecurity Act. Key changes include expanding the scope of regulated entities, broadening mandatory incident reporting, and increasing security

responsibilities for both virtual and physical systems, including those overseas (CSA 2025). The Act also grants the commissioner of cybersecurity expanded authority to mitigate threats, including directing entities to take or refrain from actions that could reduce risks. Relatedly, the Online Criminal Harms Act from 2023 covers information-sharing and taking action such as blocking access to online content suspected of being used for crime. As a regional cybersecurity leader, Singapore has introduced vetting and certification schemes for cybersecurity and internet-of-things (IoT) products and protective Domain Name Systems (DNS) for government systems, and it is pursuing ransomware payments tracing. Internationally, it leads multiple ransomware initiatives in the Association of Southeast Asian Nations (ASEAN) and plays a key role in the CRI.

In Europe, France has experienced a high number of ransomware attacks between 2021 and 2023. Throughout this time, it has maintained a clear distinction between defensive and offensive capabilities and its tradition of no public attribution. A strong promoter of digital sovereignty, France has focused on domestic industrial capabilities to boost its autonomy, also investing in protections for its governmental systems and talent development locally. This dual approach—bolstering local industry and government cybersecurity—has made public intervention to counter ransomware less of a priority than efforts to advance cyber resilience frameworks. Broader cyber-related obligations and restrictions on businesses were introduced in new laws passed in 2023 and 2024. As a member of the European Union, France has transposed the European directives relevant to cybersecurity (NIS2, DORA) and has been among the first countries to start the horizontal coordination for cyber crises, years before ransomware surged. On the international stage, France has been proactive on advancing cybersecurity in the European Union and has strengthened NATO's cybersecurity cooperation.

This examination of national approaches shows that no single policy lever suffices; instead, a multi-dimensional strategy is essential to combat this evolving threat. From Costa Rica to Australia, the spectrum of proactive cybersecurity measures introduced in recent years has included: 1) expanding the horizontal coordination across government and industry; 2) imposing more obligations on the private sector, particularly critical infrastructure providers; 3) enhancing the powers of public authorities to counter ransomware; and 4) exploring targeted forms of international collaboration (e.g., CRI). These diverse efforts reflect a global recognition that ransomware mitigation necessitates a combination of legal, strategic, and operational responses. But how effective have these levers been?

C. Discussion

Evaluating the effectiveness of ransomware mitigation strategies is challenging in today's cyber ecosystem. While efforts have concentrated largely on reducing

vulnerabilities at entry points, an emphasis must also be placed on securing the exit points—specifically, the data exfiltration methods and monetization techniques employed by attackers. According to Chainalysis (2025), the notable drop in ransom payments in 2024 can be attributed to intensified efforts against the money-laundering infrastructure, coupled with more advanced defenses and improved response plans implemented by governments.

Despite variations in sources, the available data suggests a decline in successful ransomware attacks in three of the jurisdictions analyzed. In Australia, incidents decreased slightly, from 107 in 2023 to 101 in 2024 (CyberInt 2023, 2024). France reported 130 incidents, a 21 percent reduction from the previous year (CyberInt 2024). Singapore's numbers remained stable, with 132 incidents recorded in both 2022 and 2023 (SPOR 2024), although 2024 data is not yet available. For Costa Rica, data is also missing; however, following the Conti attack on government services in 2022, the country continued to be the second most affected country in Central America, experiencing over 5,000 attempted attacks in 2023 (Kaspersky 2023). In 2024, a new wave of ransomware incidents targeted key institutions in the country (Tico Times 2024).

Incident response data—albeit only partially available and unevenly distributed—indicates important shifts in the ransomware ecosystem. Coveware's latest quarterly report (2025) indicates that a significantly smaller proportion of the victims are paying ransoms: one-quarter of the affected companies, an all-time low. Moreover, the median payment amounts are decreasing. The tracking of ransomware payments in cryptocurrency reveals a 35 percent decline, from US$1.25 billion in 2023 to US$813 million in 2024 (Chainalysis 2025). This change is attributed to the diminished operational capability and market reputation of prominent RaaS groups targeted by coordinated law enforcement operations in 2024.

However, the overall threat persists as new actors have stepped in (Symantec 2025; Coveware 2025). This study shows that governments are also adapting, through the consolidation of public sector responsibilities and improved data-sharing mechanisms, prioritizing threat intelligence and cross-sector partnerships. The shift is grounded in a broader effort to bolster cyber resilience, by clarifying legal obligations, streamlining institutional powers, and reinforcing critical infrastructure preparedness. A "whole-of-society" resilience approach is starting to take shape through the implementation of talent development programs and cybersecurity skills initiatives.

5. CONCLUSION

This study introduced a novel, multi-dimensional framework to analyze government responses to ransomware, incorporating recent qualitative data (2021–2024) from four jurisdictions. By examining progress in technical measures, legislation, regulation, institutional development, and international collaboration, the analysis reveals convergence around key action areas (critical infrastructure protection; security by design approaches) and variation according to the level of maturity and cyber posture of each jurisdiction. While national priorities and resources vary, Australia, Costa Rica, France, and Singapore share an emphasis on both strengthening internal government coordination and enhancing government-industry partnerships in the fight against ransomware.

The analysis reveals a growing centralization of government responsibilities, driven by a wider cyber resilience impetus. New regulatory measures, such as mandatory incident reporting and enhanced data-sharing requirements, are reshaping the partnership between governments and industries. In the face of this persistent threat, both public authorities and industry are adopting more mature and increasingly strategic responses. However, countries differ significantly when it comes to their priorities and alignment with national posture and circumstances, which range from cyber awareness to deploying offensive capabilities to disrupt ransomware networks. While some countries with advanced cyber capabilities favor proactive disruption, others prioritize defensive resilience. Yet the effectiveness of individual measures remains difficult to ascertain due to the lack of harmonized data.

In the future, more attention needs to be directed towards evaluating the mitigation efforts at the national level, through data collection and systematic policy impact assessments. Policy-makers should conduct comprehensive evaluations of ransomware-targeting measures to gauge their success and identify unintended consequences. Governments can learn from one another by analyzing the incentive structures they establish, but the wide variety of mitigation measures warrants more systematic comparative analyses at the regional level. Finally, there is a pressing need for academic research to broaden the perspective by providing deeper qualitative insights and evidence-based analysis.

REFERENCES

Alper, Alexandra. “Biden Sanctions Cryptocurrency Exchange over Ransomware Attacks.” *Reuters*, 21 September 2021. https://www.reuters.com/business/finance/biden-sanctions-cryptocurrency-exchange-over-ransomware-attacks-2021-09-21/

Blessing, Jenny, Jules Drean, and Sarah Radway. “Survey and Analysis of US Policies to Address Ransomware.” *MIT Science Policy Review*, 2022.

Chainalysis. 2025 *Crypto Crime Report*. 5 February 2025. https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

Constantinescu, Vlad. “Lockbit Ransomware Gang Switches to Conti-Based Encryptor.” *BitDefender News*, 3 February 2023. https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

Coveware. “Will Law Enforcement Success against Ransomware Continue in 2025?” *Quarterly Report*, 4 February 2025. https://www.coveware.com/blog/2025/1/31/q4-report.

CSA. *Singapore Cyber Landscape 2023*. 30 July 2024. https://cyberint.com/blog/research/ransomware-annual-report-2024/

CSA. *The Singapore Cybersecurity Strategy 2021*. Government of Singapore, 2021.

CyberInt. *Ransomware Annual Report 2024*. 13 January 2025. https://cyberint.com/blog/research/ransomware-annual-report-2024/.

CyberInt. *Ransomware Trends Report 202*3. 7 April 2023. https://cyberint.com/blog/research/ransomware-trends-and-statistics-2023-report/.

CyberPeace Institute. *Playing with Lives: Cyberattacks on Healthcare Are Attacks on People*. 2021.

Department of Home Affairs. *Ransomware Action Plan*. Australian Government, 2021. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-%20security/strategy/australias-ransomware-action-plan

Dobell, Adam. “The International Counter Ransomware Initiative: From Forming and Norming to Performing.” *Center for Cybersecurity Policy and Law*, 24 September 2024.

Dudley, R. “The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks.” *ProPublica*, 2019.

ENISA. *Threat Landscape Report 2024: June 2023–June 2024*. September 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Gatlan, Sergiu. “Clop Ransomware Claims It Breached 130 Orgs Using GoAnywhere Zero-Day.” *Bleeping Computer*, 10 February 2023. https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/.

Ghafur, S., S. Kristensen, K. Honeyford, G. Martin, A. Darzi, and P. Aylin. 2019. “A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS.” *npj Digital Medicine* 2(98). https:/doi.org/10.1038/s41746-019-0161-6.

Khan, A. 2024. “Reconceptualizing Policing for Cybercrime: Perspectives from Singapore.” *Laws* 13(4): 44. https://doi.org/10.3390/laws13040044.

Lubin, A. 2022. “The Law and Politics of Ransomware.” *Vanderbilt Journal of Transnational Law* 55: 1177.

MacColl, Jamie, Pia Hüsch, and Jason R. C. Nurse. *Beyond the Bottom Line: The Societal Impact of Ransomware*. RUSI, 14 November 2022. https://www.rusi.org/explore-%20our-research/publications/commentary/beyond-bottom-line-societal-impact-%20ransomware

Martin, Ciaran. “On the Matter of the British Library.” 24 January 2024. https://ciaranmartin.substack.com/p/on-the-matter-of-the-british-library.

Milmo, D. “Global Ransomware Payments Plunge by a Third amid Crackdown.” *The Guardian*, 5 February 2025. https://www.theguardian.com/technology/2025/feb/05/global-ransomware-payments-plunge-by-a-third-amid-crackdown.

Ministère de l'Économie, des Finances et de l'Industrie (Ministère de l'Économie). "Lettre de la DAJ – La loi d'orientation et de programmation du ministère de l'Intérieur." 2023. https://www.economie.gouv.fr/daj/lettre-de-la-daj-la-loi-dorientation-et-de-programmation-du-ministere-de-linterieur.

Ministère de l'Économie, des Finances et de l'Industrie (Ministère de l'Économie). *Stratégie d'accélération cybersécurité*. Le Gouvernement de la République Française, 2021. https://www.entreprises.gouv.fr/fr/strategies-d-acceleration/strategie-d-acceleration-cybersecurite.

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Ministerio de Ciencia). *Estrategia Nacional de Ciberseguridad de Costa Rica 2023–2027*. Gobierno de Costa Rica.

Mishra, Vibhu. "Cyberattacks on Healthcare: A Global Threat That Can't Be Ignored." *UN New*s, 8 November 2024. https://news.un.org/en/story/2024/11/1156751

Mott, G., S. Turner, J. R. Nurse, J. MacColl, J. Sullivan, A. Cartwright, and E. Cartwright. 2023. "Between a Rock and a Hard(ening) Place: Cyber Insurance in the Ransomware Era." *Computers & Security* 128: 103162.

Murray, Christine, and Mehul Srivastava. "How Conti Ransomware Group Crippled Costa Rica—Then Fell Apart." *Financial Times*, 9 July 2022. https://www.ft.com/content/9895f997-5941-445c-9572-9cef66d130f5

NCA. "International Investigation Disrupts the World's Most Harmful Cyber Crime Group." 2024. https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group

NCA and NCSC. R*ansomware, Extortion and the Cyber Crime Ecosystem*. White Paper, 2024. https://www.ncsc.gov.uk/files/White-paper-Ransomware-extortion-and-the-cyber-crime-ecosystem.pdf

Njini, Felix, and John Viljoen. "Transnet Declares Force Majeure at SA Ports over Cyberattack." 27 July 2021. https://www.news24.com/Fin24/transnet-declares-force-%20majeure-at-sa-ports-over-cyber-attack-20210727

O'Connell, S. 2023. "To Ban Ransomware Payments or Not to Ban Ransomware Payments: The Problems of Drafting Legislation in Response to Ransomware." *Journal of International Business & Law* 22: 151.

Parliament of Australia. *Cyber Security Legislative Package*. 2024. https:\www.aph.gov.au\Parliamentary_Business\Committees\Joint\Intelligence_and_Security\CyberSecurityPackage

Pauch, D. 2023. "Ransomware Attacks as a Cybersecurity Insurance Coverage Threat." *Humanities and Social Sciences* 30(2): 99–107.

Ransomware Task Force. "Combating Ransomware." Institute for Security and Technology, 2021. https://securityandtechnology.org/ransomwaretaskforce/report/

Ransomware.live. "Ransomware Database." 2025. Accessed: 28 February 2025. https://www.ransomware.live/groups

Rapid7. 2024 *Threat Landscape Statistics: Ransomware Activity, Vulnerability Exploits, and Attack Trends*. Rapid7, 2024.

Robles-Carrillo, M., and P. García-Teodoro. "Ransomware: An Interdisciplinary Technical and Legal Approach." *Security and Communication Networks* 2022 (1): 2806605.

Shandler, Ryana, and Miguel Alberto Gomez. 2022. "The Hidden Threat of Cyber-Attacks—Undermining Public Confidence in Government." *Journal of Information Technology & Politics* 20(4): 359–74.

Sophos. *Ransomware Payouts and Recovery Costs Went Way Up in 2023*. Report, 2023.

SPOR. “Cybersecurity and Digital Resilience.” 8 November 2024. https://spor.performancereports.gov.sg/businesses/strong-and-resilient-economy/data-and-cyber-security

Statista. “Average Duration of Downtime after a Ransomware Attack at Organizations in the United States from 1st Quarter 2020 to 2nd Quarter 2022.” n.d., 2024. https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-%20attack-us

Symantec. “Ransomware 2025: Attacks Keep Rising as Threat Shows Its Resilience.” 20 February 2024. https://www.security.com/threat-intelligence/ransomware-trends-2025

TRM. “OFAC Takes First Action against Cryptocurrency Exchange and Issues Updated Ransomware Advisory.” 2021. https://www.trmlabs.com/post/ofac-takes-first-action-%20against-cryptocurrency-exchange-and-issues-updated-ransomware-advisory

VirusTotal. “Ransomware in a Global Context.” VirusTotal, 2021.

Winder, Davey. “The Five Most Important Ransomware Attacks of 2021.” *Raconteur*, 2021. https://www.raconteur.net/technology/the-five-most-important-ransomware-attacks-of-2021