National Approaches to Ransomware Protection

Governments are developing different policies to counter the increasing ransomware threat, addressing it either as a national security issue, or through law enforcement and multilateral cooperation. Few have publicly articulated a comprehensive approach. A public policy explicitly addressing ransomware can support coordination across domestic agencies and foster international cooperation.

By Nele Achten

A ransomware attack usually starts with the infiltration of a computer system and the encryption of data using malware. Ransomware is a tool used by nation states, politically motivated hacker groups and criminals alike. Their most frequent motivation is financial gain. If the motive is financial, the encryption phase is followed by a demand to pay a ransom. If the ransom is paid, the victim will usually receive a decryption key to regain access to their data. However, ransomware might also be used for purely destructive or political motives.

Demands to pay a ransom for the decryption of files first appeared in the 1980s. Since then, ransomware groups have ransomware groups have become more professionally organized, and the number of ransomware incidents have increased steadily in the last decade. Over the past two to three years, ransomware has evolved from an activity conducted by sole individuals into a system of multiple actors specialized in different steps of the attack. This evolution, together with the increased economic impact of ransomware incidents, requires the development of public policies explicitly addressing the problem.

Most states already have national cybersecurity strategies in place that clarify the responsibilities of national agencies with regard to cyber threats. However, developing explicit national approaches to counter ransomware would improve coordination between different domestic actors and signal at an international level how states intend to tackle ransomware.

US Cyber Command personnel at Fort George G. Meade in Maryland in October 2020.
Joseph Cole / US Cyber Command

Evolution of Ransomware

Law enforcement agencies have struggled to combat the rise of ransomware due to three factors. First, ransomware has significantly been enabled by the rise of cryptocurrencies. While law enforcement agencies are able to track ransom payments made in cryptocurrencies to a certain extent, they are usually unable to recover them. Law enforcement can recover cryptocurrency payments only when they have gained access to the password of the crypto wallet to which the ransom was transferred.

Understanding the Role of Cryptocurrency

Cryptocurrency is a decentralized digital currency that is secured through encryption. This means that it is not issued by a central authority and can be sent from one user to another without the need for intermediaries. Bitcoin, the first decentralized digital currency, has been in use since 2009 and was invented by an unknown person or group.

All digital currency transactions are public because they are recorded in a publicly distributed ledger called a blockchain. This is a fundamental difference with the traditional banking system. Digital currencies are therefore traceable to a certain degree. However, cryptocurrency mixing services, who offer to mix potentially tainted funds with others, make the tracking of payments more difficult.

Digital currency funds are **not tied to real-world entities** but to digital currency addresses. The addresses are used to identify the destination of a cryptocurrency transfer. This is another difference to physical currencies that makes the association of a cryptocurrency fund with an individual very difficult. However, if a state agency is able to associate a crypto fund with a criminal activity, they can require the digital currency company that maintains the wallet to block access to it.

Second, the identification of individual suspects has been a challenge for criminal investigations (see textbox). And third, a successful criminal investigation of ransomware activities requires cross-border cooperation. Ransomware activities, however, are not prosecuted in the same systematic manner everywhere.

Some cybersecurity experts argue that we are currently in a ransomware pandemic. There are several factors that indicate a significant surge in ransomware, including increases of ransomware detection by automated software, of ransomware-related insurance claims, or of incident notifications received by public agencies. Rising ransomware attacks are partially due to decreasing costs to conduct them. It is relatively easy to purchase malware on the darknet, to target a predetermined victim, and to demand a ransom payment.

Ransomware operations have evolved from an activity conducted by an individual to business-like groups that share the ransom among them.

Most importantly, the ecosystem facilitating ransomware attacks has developed significantly over the past two to three years. Ransomware operations have evolved from an activity conducted by an individual to business-like groups that share the ransom among them. Different groups are responsible for different steps, such as harvesting credentials, upgrading code malware, infecting victims' systems, and monetizing stolen data. The distribution of tasks allows a specialization and fosters the development of new creative extortion practices.

Comprehensive Approaches

After recent ransomware attacks on health care providers worldwide and on a US oil pipeline company in May 2021, the development of adequate measures to counter ransomware has become a priority for many states. Most governments agree that the protection against ransomware attacks requires a whole-of-government effort. The Counter-Ransomware Initiative – an assembly of over 30 states the US government initiated in October 2021 – reflects this. The initiative represents a comprehensive, action-oriented international approach to the threats emerging from ransomware. It is new and remarkable compared to other international cybersecurity policy initiatives for two reasons: it explicitly includes the role of the private sector, and it covers international cooperation of different state agencies instead of focusing only on diplomatic and military responses.

The Counter-Ransomware Initiative correctly points out the various state agencies involved in implementing measures to counter ransomware. However, governments also have to decide whether their military and intelligence services should play an active role in countering ransomware, and – if so – how. This decision requires a thorough evaluation of all measures available to deter ransomware actors, policies to prevent ransomware incidents from occurring, and public recommendations to minimize the damage.

A National Security Threat?

Some states have categorized ransomware as a threat to national security. Consequently, the military plays a role in countering ransomware in these states. This national security approach to ransomware implies the use of offensive cyber operations to counter specific organized ransomware groups that are responsible for incidents with significant impact. Australia, the United States, and Canada have publicly announced that their armed forces have conducted offensive operations to disrupt cybercriminal infrastructure abroad. General Paul Nakasone, head of US Cyber Command and director of the National Security Agency, acknowledged for the first time in December 2021 that the US military took offensive measures against ransomware groups. He justified the involvement of US Cyber Command citing the impact of recent ransomware incidents on US critical infrastructure.

During an event the US-based Institute for Technology and Security organized, experts mentioned some lower criteria that could justify the use of offensive cyber operations in countering ransomware. These include the scale, increase, and severity of recent ransomware incidents as well as the fact that ransomware groups are physically present in areas where there is no direct law enforcement cooperation.

Governments using a national security threat approach to counter certain types of cybercrime may come into conflict with other states' activities against ransomware. One state's disruptive cyber operations against criminal suspects, cryptocurrency exchange businesses, and infrastructure used by ransomware groups can be in conflict with another state's ongoing law enforcement investigations gathering evidence. European governments seem to accept the use of offensive cyber operations against cybercriminals by other states but they have yet to announce their own approach to countering ransomware.

From an international law perspective, the decision whether, when, and how offensive cyber operations are used to counter ransomware depends on each state's legal position regarding the existence and scope of a general rule of sovereignty. States that have not endorsed a general rule of sovereignty have more room for maneuver to conduct offensive cyber operations. However, as soon as infrastructure in third states is involved in an offensive cyber operation, the question of whether sovereignty was violated also depends on this third state's legal position regarding a general rule of sovereignty.

If the third state has publicly endorsed such a rule, a violation will likely only be

claimed if the offensive cyber operation against the cybercriminal infrastructure meets a minimum threshold. This could, for example, be the case if an offensive cyber operation is conducted against a ransomware group in a third country where law enforcement would have had sufficient capabilities itself to take down the ransomware group's server.

Finally, the decision to employ offensive cyber operations against ransomware also depends on a careful evaluation of other tools at states' disposal. There are a number of non-military means available to respond, including diplomatic action, criminal prosecution, and cross-border take-down operations by law enforcement agencies. Diplomatic actions range from calling out the state that provides safe harbor for ransomware groups to imposing sanctions against specific crypto wallets or crypto exchanges that facilitate transactions related to criminal activities. These non-offensive measures pose fewer escalation risks and thus provide a better ground for improving cross-border criminal law investigations, including with the state that is accused of harboring cybercriminals.

Non-offensive measures pose fewer escalation risks and provide a better ground for improving cross-border criminal law investigations.

Criminal Prosecution

Governments that address ransomware solely through law enforcement activities and multilateral cooperation can target different types of suspects. Criminal prosecutions can include investigations against the ransomware group itself and in some jurisdictions against entities that facilitate the ransomware business model, such as crypto exchange businesses that facilitate money-laundering.

Crypto exchanges are businesses that allow customers to trade cryptocurrencies for other assets, including conventional money or other digital currencies. In some jurisdictions, they have a legal obligation to notify public agencies of suspicious activities. They might be criminally liable if they do not comply with their obligation to notify and thereby support financial transactions that demonstrably come from illegal sources. In Switzerland, crypto exchanges have an additional obligation to know the identity of any customer who conducts a major transaction, similar to banks.

Moreover, governments that prioritize law enforcement means to respond to ransomware activities have to develop a good relationship with the private sector. Andreas Popow, a Swiss prosecutor specialized in ransomware, elaborated in an interview that cooperation with the private sector has changed and matured over the past couple of years. Increasingly, businesses that are a victim of ransomware attacks are more comfortable sharing information with law enforcement agencies. In addition, ransomware victims are more frequently supported by specialized incident response companies nowadays and law enforcement can directly coordinate with these companies to secure digital evidence. This often means a lower workload for law enforcement when preserving such evidence.

Prevention and Mitigation

In addition to the different response mechanisms, national policies to protect against ransomware can be complemented by policies on the prevention and mitigation of incidents. Most states have governmental Computer Emergency Response Teams (CERT) that are tasked with disseminating threat intelligence and issuing recommendations to mitigate specific cybersecurity threats. Regarding the ransomware threat, governmental CERTs support businesses by sharing information of vulnerabilities and thereby preventing the infiltration of systems. Finally, law enforcement plays a role in the mitigation of damage. For instance, they may support ransomware victims in decrypting their data or provide guidance regarding ransom payments.

One challenge arises when governments support critical infrastructure and other businesses differently in the protection against cyber threats. Critical infrastructure providers often benefit from being part of threat information exchange groups coordinated by the government and sometimes from other technical support in the case of an incident. Categorizing only certain entities of a sector as "critical" has led to some criticism in the past. One important example is the health care sector, where the disruption of smaller entities can destabilize society as a whole (see CSS Analysis n°296). As a response, the Swiss GovCERT supports any type of entity in the health care and energy sector, regardless of their categorization as critical or not.

Resilience

Finally, there are increasingly public policies and laws aiming to strengthen the resilience of products. This entails promoting the security practices of businesses beyond sharing information on specific vulnerabilities. The focus on resilience is not surprising given that an analysis of the largest ransomware claims in Europe suggests that most attacks could be avoided.

Approaches to incentivize "best practices" depend on each nation's domestic context. State measures are often a mixture of legally binding and voluntary mechanisms. Mandatory legal requirements are mostly limited to critical infrastructure providers. However, recent major cyber incidents have led to a policy change in some countries that were previously reluctant to adopt mandatory requirements. The US Transportation Security Administration, for example, recently issued mandatory security requirements for critical pipeline owners and operators, including the requirement to implement "immediate mitigation measures to protect against cyberattacks".

For all other businesses, best practices are usually only promoted through voluntary recommendations and advice governmental cybersecurity agencies publish. In addi-

"Don't Pay the Ransom!"

This is the advice that government agencies continuously give to ransomware victims. They argue that ransom payments have a negative impact on society because they encourage attackers to continue their business. In addition, ransomware victims who pay risk being targeted again because hackers know about their low security standards and willingness to pay. Ultimately, it is the victim's decision whether to pay the ransom.

Governmental advice not to pay is, however, only credible if the government supports ransomware victims in other ways. For instance, government agencies can provide other solutions to recover encrypted data, which is sometimes easier than the victim expects. The #NoMoreRansom project initiated by Europol, the Dutch police, and the cybersecurity companies Kaspersky and McAfee, for example, provides decryption tools for specific malwares used in ransomware incidents.

Further Readings

Bernard Barbier / Jean-Louis Gergorin / Edouard Guillaud, "Il faut se demander si la France peut continuer à se passer d'une forte coordination stratégique de la cybersécurité auprès du président," *Le Monde,* 14.01.2022.

White House Press Release, "Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting," 04.20.2021.

Institute for Security and Technology, *Combatting Ransomware – A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force,* September 2021.

Stefan Soesanto, "Wrong Turn or Right Lane? Defending Forward Against Cybercriminals Abroad," *Real Clear Defense,* 09.05.2020.

tion, insurance companies influence risk management and loss prevention industry practices by setting minimum security requirements in order to conclude an insurance contract. According to a report Allianz insurance published in 2021, three out of four businesses do not meet the cybersecurity requirements to be eligible for insurance coverage and are consequently adapting their security practices to qualify.

Future Actions and Cooperation

No country will be able to address global ransomware threats on its own. In most cases, attackers are based abroad. This requires international cooperation to prevent and respond. Developing a comprehensive international strategy is complex and calls for a variety of actors to be involved. International cooperation on cybersecurity issues has evolved not only within existing security alliances but also among new groups of states. These efforts, such as the Counter-Ransomware Initiative and the Agile Nations network, often encompass states that have highly developed domestic cybersecurity policies.

Actions in the near future will likely focus on operationalizing bilateral cooperation. One example could be to develop common criteria for digital evidence that should be preserved within the system of ransomware victims. This could help foster an information-sharing ecosystem among countries and particular companies that are part of an alliance to counter ransomware.

Increasing the protection against ransomware will be a long and gradual journey. Domestically, the development of policies that explicitly address ransomware can foster protection by the state. At the international level, the definition of some basic practical steps could strengthen cross-border cooperation.

For more on Cybersecutity Politics, see CSS core theme page.

Nele Achten is Senior Researcher for Cybersecurity Policy in the Swiss and Euro-Atlantic Security Team at the Center for Security Studies (CSS) at ETH Zürich.

CSS Analyses in Security Policy is published by the Center for Security Studies (CSS) at ETH Zürich. The CSS is a center of competence for Swiss and international security policy. Each month, two analyses are published in German, French, and English.

Editor: Névine Schepers
Language Editing: Benno Zogg
Layout and graphics: Miriam Dahinden-Ganzoni

Feedback and comments: analysen@sipo.gess.ethz.ch
More editions and online subscription: www.css.ethz.ch/cssanalyses

Most recent editions:

Regulating Cybersecurity in the Health Care Sector No. 296
Microchips: Small and Demanded No. 295
The Taliban Takeover and China-Russia Relations No. 294
Ukraine, Georgia and Moldova between Russia and the West No. 293
From Robots to Warbots: Reality Meets Science Fiction No. 292
European Fighter Programs: A Preliminary Assessment No. 291

ISSN: 2296-0244; DOI: 10.3929/ethz-b-000528952