



# Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021

OCTOBER 14, 2021 • [STATEMENTS AND RELEASES](#)

Having gathered virtually on October 13 and 14 to discuss the escalating global security threat from ransomware, we the Ministers and Representatives of Australia, Brazil, Bulgaria, Canada, Czech Republic, the Dominican Republic, Estonia, European Union, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Lithuania, Mexico, the Netherlands, New Zealand, Nigeria, Poland, Republic of Korea, Romania, Singapore, South Africa, Sweden, Switzerland, Ukraine, United Arab Emirates, the United Kingdom, and the United States recognize that ransomware is an escalating global security threat with serious economic and security consequences.

From malign operations against local health providers that endanger patient care, to those directed at businesses that limit their ability to provide fuel, groceries, or other goods to the public, ransomware poses a significant risk to critical infrastructure, essential services, public safety, consumer protection and privacy, and economic prosperity. As with other cyber threats, the threat of ransomware is complex and global in nature and requires a shared response. A nation's ability to effectively prevent, detect, mitigate and respond to threats from ransomware will depend, in part, on the capacity, cooperation, and resilience of global partners, the private sector, civil society, and the general public.

Governments recognize the need for urgent action, common priorities, and complementary efforts to reduce the risk of ransomware. Efforts will include improving network resilience to

prevent incidents when possible and respond effectively when incidents do occur; addressing the abuse of financial mechanisms to launder ransom payments or conduct other activities that make ransomware profitable; and disrupting the ransomware ecosystem via law enforcement collaboration to investigate and prosecute ransomware actors, addressing safe havens for ransomware criminals, and continued diplomatic engagement.

## Resilience

Network resilience is about more than technical capabilities – it also requires effective policy frameworks, appropriate resources, clear governance structures, transparent and well-rehearsed incident response procedures, a trained and ready workforce, partnership with the private sector, and consistently enforced legal and regulatory regimes. These efforts will naturally reflect each nation’s unique domestic context, and may vary from one nation to the next.

However, several universal cybersecurity best practices can dramatically reduce the likelihood of a ransomware incident and mitigate the risk from a host of other cyber threats. These basic steps include maintaining offline data backups, use of strong passwords and multi-factor authentication, ensuring software patches are up to date, and education against clicking suspicious links or opening untrusted documents. We are committed to working together and with the private sector to promote improvements in basic cyber hygiene to boost network resilience and mitigate the risk of ransomware.

Nations should also consider appropriate steps to promote incident information sharing between ransomware victims and relevant law enforcement and cyber emergency response teams (CERTs), with protection for privacy and human rights. Such sharing enables cybercrime investigations and prosecutions, and facilitates broad distribution of cyber threat mitigation steps.

Moving forward, we are committed to sharing lessons learned and best practices for development of policies to address ransom payments, as appropriate. We will also engage with private sector entities to promote incident information sharing and to explore other opportunities for collective buy-down of risk. Further, we note that resilience efforts are most

effective when accountable senior leaders with the ability to direct resources, balance associated trade-offs, and drive outcomes are actively involved in cybersecurity decision-making.

### Countering Illicit Finance

Ransomware is primarily a profit-seeking endeavor, commonly leveraging money laundering networks to move ransomware proceeds. We recognize the significant potential for combating ransomware through enhanced international cooperation to inhibit, trace, and interdict ransomware payment flows, consistent with national laws and regulations, which will drive down economic incentives for ransomware actors. Cooperation can include a wide range of activities, such as efforts intended to facilitate customer due diligence, suspicious activity reporting, and transaction monitoring.

Taking action to disrupt the ransomware business model requires concerted efforts to address illicit finance risks posed by all value transfer systems, including virtual assets, the primary instrument criminals use for ransomware payments and subsequent money laundering. We acknowledge that uneven global implementation of the standards of the Financial Action Task Force (FATF) to virtual assets and virtual asset service providers (VASPs) creates an environment permissive to jurisdictional arbitrage by malicious actors seeking platforms to move illicit proceeds without being subject to appropriate anti-money laundering (AML) and other obligations. We also recognize the challenges some jurisdictions face in developing frameworks and investigative capabilities to address the constantly evolving and highly distributed business operations involving virtual assets.

We are dedicated to enhancing our efforts to disrupt the ransomware business model and associated money-laundering activities, including through ensuring our national AML frameworks effectively identify and mitigate risks associated with VASPs and related activities. We will enhance the capacity of our national authorities, to include regulators, financial intelligence units, and law enforcement to regulate, supervise, investigate, and take action against virtual asset exploitation with appropriate protections for privacy, and recognizing that specific actions may vary based on domestic contexts. We will also seek out ways to cooperate with the virtual asset industry to enhance ransomware-related information

sharing.

## Disruption and other Law Enforcement Efforts

Beyond implementing measures to improve resilience and harden our financial system from exploitation, we must also act to degrade and hold accountable ransomware criminal operators. Ransomware criminal activity is often transnational in nature, and requires timely and consistent collaboration across law enforcement, national security authorities, cybersecurity agencies, and financial intelligence units. Such collaboration must be consistent with domestic legal requirements, and may be pursued alongside diplomatic engagement so that malicious activity can be identified and addressed, and the actors responsible can be investigated and prosecuted. Together, we must take appropriate steps to counter cybercriminal activity emanating from within our own territory and impress urgency on others to do the same in order to eliminate safe havens for the operators who conduct such disruptive and destabilizing operations.

We intend to cooperate with each other and with other international partners to enhance the exchange of information and provide requested assistance where able to combat ransomware activity leveraging infrastructure and financial institutions within our territories. We will consider all national tools available in taking action against those responsible for ransomware operations threatening critical infrastructure and public safety.

## Diplomacy

In addition to disruption of the ransomware ecosystem, diplomatic efforts can promote rules-based behavior and encourage states to take reasonable steps to address ransomware operations emanating from within their territory. We will leverage diplomacy through coordination of action in response to states whenever they do not address the activities of cybercriminals. Such collaboration will be a critical component to meaningfully reduce safe havens for ransomware actors.

Noting that law enforcement and cybersecurity capacity can be significant limiting factors in a state's ability to address cybercrime, diplomacy in the form of coordinated capacity building

has potential to serve as a force multiplier in the fight against ransomware. We will share approaches to capacity building, highlight resources and programs that are available, and take steps to coordinate such work when appropriate to ensure capacity building complements other actions to minimize the ransomware threat.

###