



Task Force 7
Towards Reformed Multilateralism: Transforming Global
Institutions and Frameworks



HARNESSING THE G20'S POTENTIAL FOR GLOBAL COUNTER- RANSOMWARE EFFORTS

May 2023

Tobias Scholz, PhD Candidate, King's College London and National University
of Singapore


Sameer Patil, Senior Fellow, Observer Research Foundation, Mumbai

वसुधैव कुटुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE




Abstract




Ransomware attacks have emerged as a massive cybersecurity challenge for states, civil society, the private sector, and individuals around the world. These attacks have disrupted national and commercial computer networks, caused data breaches, and in 2021 alone cost the global economy an estimated US\$20 billion. Multilateral and plurilateral initiatives are working to raise awareness and create diplomatic solutions to the challenges posed by the application of ransomware. The G20 can contribute to global counter-

ransomware efforts through its Digital Economy Working Group. The grouping should assert itself as a global leader in countering ransomware while complementing existing international efforts. It should facilitate existing efforts of multilateral platforms for responsible state behaviour, declare its support to commence negotiations for a new United Nations Cybercrime Convention, and create a multi-stakeholder capacity-building platform to enhance awareness and strengthen the cyber-resilience of countries in the Global South.



The Global Ransomware Challenge

1




Since the WannaCry and NotPetya attacks in 2017, ransomware has emerged as a potent cybersecurity threat to states and citizens alike.¹ Cyber criminals and hacking syndicates have leveraged ransomware to disrupt and destabilise systems by exploiting the need of countries and organisations for continued functionality of their computer networks. These malicious elements make ransom demands in exchange for the resumption of services and regaining access to data. The business has become more lucrative for cyber criminals, and there has been an increase in the frequency and intensity of ransomware incidents in the past few years.

Ransomware attacks target businesses and organisations of all sizes. A primary target, however, are organisations that do not possess valuable or critical data—such as power grids, energy companies, and small and medium enterprises—as they often do not have sufficient cyber defence mechanisms in place and their focus is on operating critical infrastructure facilities and services. Consequently, critical infrastructure—such as hospitals, power grids, and the financial services industry—have

become ransomware’s favourite prey. Any disruption of these infrastructures can cause crucial damage and financial losses.

Moreover, as some ransomware incidents have shown, disruption of these services can have a domino effect. For instance, the May 2017 NotPetya ransomware attack in Europe, described by the media as the biggest ever, disrupted operations at many firms, including the Danish shipping company, Maersk.² The incident caused delays in cargo container deliveries, negatively impacting the global supply chain and causing further disruptions in manufacturing operations across several countries. Likewise, a ransomware attack on Colonial Pipeline in the United States in May 2021 forced the company to shut down its operations for several days, causing fuel shortages and price spikes across the East Coast of the United States.³

Such damages and disruptions caused by ransomware attacks compel victimised organisations to make ransom payments in exchange for regaining access to their systems. For example, the Colonial Pipeline company paid US\$5 million in bitcoins as ransom




to resume operations.⁴ According to a study by cybersecurity firm Sophos, 66 percent of the organisations surveyed were hit with ransomware in 2021 alone—an increase from 37 percent in 2020.⁵ Furthermore, the analysis noted a dramatic rise in ransom payments: in 2021, 11 percent of organisations surveyed had paid ransoms of at least US\$1 million, an increase from 4 percent who did so in 2020. The percentage of organisations paying less than US\$10,000 dropped to 21 percent in 2021 from 34 percent in 2020. Moreover, 90 percent of organisations said the attack had impaired their ability to operate, and 86 percent of private sector victims said they lost revenue due to the breach, or their business altogether.

Yet, these figures may be understated, as there is significant under-reporting of ransomware attacks.⁶ Organisations, particularly in the private sector, are reluctant to disclose their vulnerabilities to ransomware attacks because they fear exposing themselves and losing a competitive edge over their business rivals. Instead, many pay a quick ransom, avoid negative publicity, and ensure business continuity.⁷

Quick ransom payments such as the one made by Colonial Pipeline are driving the growth of a business model—what is known as the ‘Ransomware-as-a-Service’ (RaaS) ecosystem—whereby malware developers are leasing out ransomware and its control infrastructure to cybercriminals for launching attacks.⁸ This includes data theft tools for publishing stolen data to coerce victims into paying the ransom. The RaaS ecosystem has mainly proliferated with the darknet, where marketplaces specialise in selling malicious software and other associated tools.⁹ In addition to the anonymity afforded by the darknet, cybercriminal groups have exploited cryptocurrency platforms for use in their activities.¹⁰ Furthermore, the development of artificial intelligence-enabled predictive language tools and chatbots has made it easier for cybercriminals to develop advanced forms of ransomware.

The COVID-19 pandemic altered the threat landscape across geographies, widening the opportunities for saboteurs to target organisations that are unprepared to tackle increased threats. As many organisations shifted



to work-from-home models in 2020 and relied heavily on digital infrastructures, the attack surface expanded, giving malicious elements more opportunities to disrupt infrastructures and everyday services and steal sensitive information.¹¹ Moreover, cyber criminals have deliberately leaked stolen data from organisations and individuals who refused to pay a ransom.¹² According to a study by the European Union (EU) Agency for Cybersecurity, cyber criminals and hacking syndicates working in the United Kingdom and the US managed to steal 10 terabytes of data every month between May 2021

and June 2022. They were primarily employees' personal data.¹³


To be sure, the instances of ransomware attacks may be only a fraction of all cybersecurity incidents the world is currently witnessing. However, their rapid surge presents a grave threat to international security and cyberspace stability; every time a ransomware attack succeeds, it spawns more such breaches. These events also encourage rogue state actors to utilise the tool themselves or outsource attacks to proxy cybercriminal gangs and hacking syndicates to target their adversaries.



G20's Counter- Ransomware Initiatives

2





The G20 has a crucial responsibility in helping shape norms and standards for secure and accessible digital spaces. The continuously growing threat that cybercrime poses to the global economy, and the need to protect the security of nations, has pushed the subject of cybersecurity to the centre stage of discussions at various international platforms in the recent years.¹⁴ The G20 should widen and deepen their cooperation on countering ransomware attacks, and tap into its experiences in four domains.

1. Maintaining global financial stability


In 2013, the G20 Leaders' Declaration acknowledged the challenges posed by digitalisation to the international financial system.¹⁵ The G20 has been supporting efforts of the Financial Stability Board (FSB) to create a common framework for reporting cyber incidents, as well as response and recovery. The FSB's 2022 report outlined a key toolkit for all types of organisations to heighten their cyber resilience and capacity.¹⁶ It suggests a number of best practices for incident reporting, sets out the vision for a format for incident reporting exchange (FIRE), and emphasises the role of a shared taxonomy for all stakeholders.

2. Preserving the integrity of critical infrastructures

The G20 is not a security forum, and thus has responded to cybercrime challenges by pointing to the significance of national institutions and regulations for international stability. More serious G20 efforts to mitigate cybersecurity risks began with the document, *G20 Examples of Practices Related to Security in the Digital Economy 2020*.¹⁷ The mapping effort of various national cyber institutions and laws reflects the platform's reticence in advocating for one specific solution to cyber challenges.

3. Bridging the global digital divide

G20 declarations refer to the importance of the global commitment to reduce the digital divide, enunciated in the United Nations Sustainable Development Goals (SDGs). Ransomware matters to SDGs in the contexts of unequal access to cybersecurity software, knowledge over cyber hygiene, and varying impacts on different intersectional groups, particularly concerning privacy and security. To close the digital gap, the G20 has developed the Quality Infrastructure Investment (QII) Indicators, the Global Infrastructure Hub (GI Hub), and the



G20 Compendium of Case Studies on Digital Infrastructure Finance.

4. Upholding the global and interconnected Internet

The G20 has been advocating for a global and interconnected internet, free cross-border data flows, and integrated networks. The worsening threat of ransomware attacks incentivises states to revert from such principles and seek greater national control over the internet and data flows.


In the Bali Leaders' Summit Declaration of November 2022, heads of states and governments concluded that they aspire to "advance a more inclusive, human-centric, empowering, and sustainable digital transformation."¹⁸ Considering the four areas of shared interests as well as the urgency of challenges, the G20 constitutes an important platform to advance the global agenda on countering ransomware.

The G20 operates in an international environment which it can learn from and where it can leverage existing plurilateral and multilateral as well as multistakeholder initiatives on ransomware. The Counter Ransomware Initiative (CRI) has begun setting out principles for appropriate state behaviour.¹⁹ Workshops, capacity trainings, and gaming approaches are important tools to build expertise and resilience, which the Shanghai Cooperation Organisation (SCO) and the Council of Europe (CoE), together with EUROJUST, have pioneered.²⁰ INTERPOL's Global Complex for Innovation (IGCI) in Singapore is leading efforts in conducting research and training towards more efficient ways of prosecuting cybercrime.²¹ Under the Paris Call for Trust and Security in Cyberspace, a multi-stakeholder working group has evaluated the work and impact of the most significant initiatives countering the spread of ransomware.²²



Recommendations to the G20

3



1. Utilise existing global counter-ransomware initiatives.

The G20 can build on earlier efforts in countering the threat of ransomware. As discussed earlier in this brief, there are several plurilateral and multilateral initiatives being implemented to prevent and respond to ransomware attacks.

The G20 can support these strategies by promoting international cooperation, supporting law enforcement efforts, raising awareness, and promoting best practices as well as developing international norms and standards for cybersecurity. Japan, for instance, presented its national best practices on critical infrastructure protection during the G20 Digital Economy Ministers' meeting in July 2020. These practices could be expanded as capacity-building or mutual assistance programmes that will involve the member states' respective national agencies.

2. Address ransomware threats explicitly in global norms-building for responsible state behaviour.

G20 members must work together to create norms for responsible state behaviour. These findings may lead to the development of coordinated responses to ransomware incidents as well as joint strategies to combat ransomware. G20 members should also commit to criminalising ransomware attacks and holding perpetrators accountable, including the actors responsible for creating, distributing, and using ransomware. They should also be transparent in sharing the outcomes of their counteractions with other members. Some of these norms can be developed through forums such as the United Nations Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG), where efforts have centred around discussions on protecting and securing critical infrastructure.

For example, the UNGGE of 2015 introduced a norm that stipulates that states must refrain from any action “that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.”²³ Members can also complement existing efforts of multilateral norms for responsible state behaviour by adopting a G20 pledge that member states’ territory will not be used for ransomware campaigns. By supporting norms such as these, the G20 can counter the threat of ransomware and protect their citizens and businesses from its harmful effects.


3. Leverage the potential of the FSB and national CERTs as facilitators for global norms and standards pertaining to ransomware.

The FSB should explore realistic and appropriate means of information-sharing and cooperation between law enforcement agencies that value the imperative of national laws regarding privacy and data protection. A multi-stakeholder capacity-building platform can be facilitated through the FSB with the

goal of allowing G20 states to better assess risk perception and the threat landscape across countries and sectors. Such a platform could form a pillar of the G20’s commitment towards enhancing threat awareness and cyber resilience of countries in the Global South. A G20 dialogue format between Computer Emergency Response Team (CERT) representatives can be established to share their experiences and set up a Ransomware Resilience Repository (RRR), supported by the FSB.

4. Address the need for a global normative and institutional order to counter cybercrime and its effects.

The G20 should drive efforts for a UN treaty on cybercrime. G20 nations should strengthen the work of the Ad Hoc Committee on countering the use of information and communications technologies for criminal purposes. The G20 should specifically welcome the participation of multiple stakeholders in the conciliatory process towards a global cybercrime treaty, which remains,



in principle, led by states. The G20 should specifically welcome the participation of multistakeholder actors in the conciliatory process towards a global cybercrime treaty, which still continues to be, in principle, led by state actors. The process can benefit from insights that can be shared by members that have experience in cybercrime governance and investigations with existing international treaties, most importantly, the Budapest Convention on Cybercrime.²⁴

In a rapidly digitising world, this is an opportune time for the G20 to take steps towards addressing the growing numbers and impacts of ransomware incidents. The rapid polarisation

between global powers in cyberspace has adversely impacted the prospects for international cyber cooperation. This casts doubt on the efficacy of global multilateral institutions in responding to the emerging challenges in cyberspace.

As a group that brings together leading digital and industrial powers, the G20 could be key in building trust in the global economy as well as functional and equitable multilateral institutions. If the G20 can take the lead on advancing cooperation against ransomware incidents, it will contribute to strengthening the resilience of digital economies and shaping global digital governance and institutional frameworks.

Endnotes

- 1 Alex Hern, "WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017," *The Guardian*, December 30, 2017, sec. Technology, <https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware>.
- 2 Jacob Gronholt-Pedersen, "Maersk Says Global IT Breakdown Caused by Cyber Attack," *Reuters*, June 27, 2017, sec. Technology News, <https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN1911NO>.
- 3 Emma Newburger, "Ransomware Attack Forces Shutdown of Largest Fuel Pipeline in the U.S.," *CNBC*, May 8, 2021, <https://www.cnbc.com/2021/05/08/colonial-pipeline-shuts-pipeline-operations-after-cyberattack.html>.
- 4 William Turton, Michael Riley, and Jennifer Jacobs, "Colonial Pipeline Paid Hackers Nearly \$5 Million in Ransom," *Bloomberg*, May 13, 2021, <https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom>.
- 5 Sally Adam, "The State of Ransomware 2022," *Sophos News*, April 27, 2022, <https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/>.
- 6 Lance Johnson and Lisa Plaggemeier, "The Threat of Ransomware Attacks," interview by Mark Meissner, Security Standards Council, February 10, 2022, <https://blog.pcisecuritystandards.org/the-threat-of-ransomware-attacks>.
- 7 "Ransomware: Publicly Reported Incidents Are Only the Tip of the Iceberg," European Union Agency for Cybersecurity (ENISA), July 29, 2022, <https://www.enisa.europa.eu/news/ransomware-publicly-reported-incidents-are-only-the-tip-of-the-iceberg>.
- 8 "Ransomware-as-a-Service (RaaS)," in *Encyclopedia by Kaspersky* (Kaspersky), accessed April 5, 2023, <https://encyclopedia.kaspersky.com/glossary/ransomware-as-a-service-raas/>.
- 9 Sameer Patil, "Partnering for Prosperity: India-Canada Collaboration to Curb Digital Black Markets," Canada-India Track 1.5 Dialogue, Centre for International Governance Innovation (CIGI), January 25, 2019, <https://www.cigionline.org/publications/partnering-prosperity-india-canada-collaboration-curb-digital-black-markets/>.
- 10 David Hickton, "Disrupting Ransomware," *Directions Blog*, March 30, 2023, <https://directionsblog.eu/disrupting-ransomware/>.
- 11 Danny Palmer, "Fewer Ransomware Victims Are Paying Up. But There's a Catch," *ZDNET*, January 23, 2023, <https://www.zdnet.com/article/fewer-ransomware-victims-are-paying-up-but-theres-a-catch/>.
- 12 Danny Palmer, "Ransomware Has Now Become a Problem for Everyone, and Not Just Tech," *ZDNET*, January 15, 2023, <https://www.zdnet.com/article/ransomware-has-now-become-a-problem-for-everyone-and-not-just-tech/>.
- 13 "Ransomware"

- 
- 14 See, e.g., “International Counter Ransomware Initiative 2022 Joint Statement,” The White House, November 1, 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/>.
 - 15 G20 Leaders, “G20 Leaders’ Declaration,” University of Toronto, September 6, 2013, <http://www.g20.utoronto.ca/2013/2013-0906-declaration.html>.
 - 16 “Effective Practices for Cyber Incident Response and Recovery,” Financial Stability Board (FSB), October 18, 2020, <https://www.fsb.org/wp-content/uploads/P191020-1.pdf>.
 - 17 “Achieving Greater Convergence in Cyber Incident Reporting: Consultative Document,” Financial Stability Board (FSB), October 17, 2022, <https://www.fsb.org/2022/10/achieving-greater-convergence-in-cyber-incident-reporting-consultative-document/>; “Ministerial Declaration: G20 Digital Economy Ministers Meeting, July 22, 2020,” G20 Research Group, University of Toronto, accessed 5 April 2023, <http://www.g20.utoronto.ca/2020/2020-g20-digital-0722.html>.
 - 18 G20 Leaders, “G20 Bali Leaders’ Declaration,” G20, November 16, 2022, https://www.g20.org/content/dam/gtwenty/gtwenty_new/about_g20/previous-summit-documents/2022-bali/G20%20Bali%20Leaders%27%20Declaration,%2015-16%20November%202022.pdf.
 - 19 “International Counter Ransomware Initiative 2022 Joint Statement”
 - 20 “RATS SCO Practical Seminar on “SECURING THE CYBER SPACE FRONTIERS” Organized by National Security Council Secretariat of India,” December 15, 2022, <https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1883880>; “CyberSouth Activities. Council of Europe and EUROJUST: Cooperation on Ransomware,” Council of Europe (CoE), accessed April 5, 2023, <https://www.coe.int/en/web/cybercrime/-/council-of-europe-and-eurojust-cooperation-on-ransomware>.
 - 21 “INTERPOL Global Complex for Innovation Opens Its Doors,” Interpol, September 30, 2014, <https://www.interpol.int/en/News-and-Events/News/2014/INTERPOL-Global-Complex-for-Innovation-opens-its-doors>.
 - 22 “Ransomware. Paris Call for Trust and Security in Cyberspace: Multistakeholder Workstream on Public-Private Partnerships in Fighting Ransomware Threats,” Paris Peace Forum, 2022, https://parispeaceforum.org/wp-content/uploads/2022/11/20221105_Paris-Call-Compendium-of-transnational-PPP-against-ransomware_FINAL_v1.pdf.
 - 23 “Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015,” The United Nations, accessed April 5, 2023, <https://www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf>.
 - 24 “Budapest Convention (ETS No. 185) and Its Protocols,” Council of Europe, accessed May 2, 2023, <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.



वसुधैव कुटुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE