



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



# ESTABLISHING GLOBAL NORMS TO PROTECT CRITICAL INFORMATION INFRASTRUCTURE

May 2023

**Srishti Saxena**, Account Director (Public Policy), Chase India


**Kaushal Mahan**, Vice President (Public Policy), Chase India

वसुधैव कुटुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE



# Abstract




**A** key learning during Indonesia's G20 presidency was that technology will define the post-pandemic world and is essential for equitable growth, an agenda that will be carried forward by India. However, technology can also be weaponised by state and non-state actors by creating new warfare techniques in cyberspace. This can pose threats to democracy through misinformation and disinformation, especially during periods of conflict. As such, it is imperative to build a global consensus of trust in technology. The international norms for physical warfare have been clearly laid out through the Geneva and Hague conventions and their protocols. What is missing is a global order on cyber security, the protection of cyber assets, and the prevention of misinformation and disinformation.

What is needed is a federated approach like the Christchurch Call to Action to tackle the evils of hybrid war to prevent human catastrophes and showcase the importance of public-private partnership.


However, attacks on critical information infrastructure are not limited to wartime, and can have ripple effects that lead to citizens being denied basic amenities. For example, an extended power outage due to an attack on the power grid can result in impacted access to medical facilities. Therefore, it is important for each country to modernise its legal and policy frameworks for critical information infrastructure, and for the global community to establish international norms for protect such infrastructure. The G20 can lead such an effort.



# The Challenge



# 1



**T**echnology is all pervasive, and is a key part of national and foreign policies, governance and service delivery, and warfare alike. But such a dependence on technology means any kind of disruption in critical systems can lead to a range of issues, including restricted access to or the denial of essential services such as healthcare. A country is responsible to safeguard its critical systems to ensure the continuity of essential services, and many have found innovative solutions such as data embassies and cloud computing to avoid disruptions in governance caused by cyberattacks or natural calamities. For instance, Estonia<sup>1</sup> launched the world's first data embassy in partnership with Luxembourg to avoid disruptions in its digital services due to cyberattacks. Additionally, since the start of the war with Russia, Ukraine<sup>2</sup> has begun to transfer and store its personal data on the cloud outside its territory.

There is now a need to establish norms for cyber security, trust in data transfers, and against misinformation/disinformation, but the process of arriving at a global consensus to protect critical information infrastructure has

been slow. This stems from a variety of reasons, such as the lack of a shared understanding of critical sectors and critical information infrastructure; difficulties in information sharing (particularly of sensitive information) at the international level;<sup>3</sup> and a lack of adequate national frameworks that define and penalise cyber-crimes, making it difficult to address transnational crimes.<sup>4</sup> These differences often pose difficulties in inter-country cooperation.

The difference in approach can be classified as:


### **Difference in critical sectors**

Each G20 country has identified its own critical sectors. Of the roughly 30 different sectors that have been determined, no single one can be identified as being critical to all countries (see Table 1). Further, even where there is consensus on the broader sectors, there may be differences in sub-sectors/enterprises. For example, in communications, France has identified telecom and broadcasting, India has identified only telecom, and Australia has identified telecom, broadcasting, and domain name system as critical sectors.

**Table 1: Critical sectors in the G20 countries**

	India <sup>5</sup>	Australia <sup>6</sup>	UK <sup>7</sup>	Brazil <sup>8,9</sup>	Argentina <sup>10</sup>	China <sup>11</sup>	Russia <sup>12</sup>	Canada <sup>13,14</sup>	France <sup>15</sup>	Germany <sup>16</sup>	Indonesia <sup>17</sup>	Japan <sup>18</sup>	South Korea <sup>19</sup>	South Africa <sup>20</sup>	Turkey <sup>21</sup>	US <sup>22</sup>	EU <sup>23</sup>
Communication	*	*	*	*	*	*	*		*				*		*	*	
Power	*									*							
Energy	*	*	*	*	*	*		*	*		*		*	*	*	*	*
Transport	*	*	*	*	*	*		*	*		*		*	*	*	*	*
BFSI	*	*	*	*	*	*		*	*		*		*			*	*
Strategic & Public Enterprises	*																
Government	*		*			*		*	*		*		*		*	*	
Data Storage and Processing		*															
Defence		*	*			*			*		*		*			*	
Food		*	*					*	*		*					*	*
Health		*	*					*	*		*			*		*	*
Education		*															
Space		*	*						*								*
Water		*	*	*				*	*					*	*	*	*
Sewage									*								
Chemicals			*													*	*
Nuclear			*													*	*
Emergency Services			*													*	
Oil and Gas					*												
Public Services						*											*
Hydraulic Engineering and Dams						*											*
Technogenic hazardous facilities							*										
Fire and explosion hazardous objects							*										
ICT								*		*	*	*				*	*
Safety								*									
Manufacturing								*								*	
Industry									*							*	
Justice									*								
Disaster Control and Management									*								
Media and Cultural Objects									*								
Aviation												*					
Airports												*					*
Railways												*					
Electricity												*					
Logistics												*					
Security													*				

Note: Details of Italy are covered as part of the EU. Details of Mexico were not accessible in English and so have not been included



Each country or region will identify critical sectors based on national priorities and contexts, but there are still some commonalities in identifying a few critical sectors (for instance, transport, energy, BFSI, and communications). A guiding principle is that if everything is considered critical then nothing is critical due to the absence of special efforts. Therefore, sectors that are either critical to most G20 countries (such as transport, energy, and BFSI) or have a global impact should be used as a starting point for a discussion on global norms. Even sectors that are not a common critical concern for most G20 countries but are globally relevant, such as data storage and processing, can be included.

### **Difference in defining critical information infrastructure**

There are differing criteria to identify critical information infrastructure among the G20 countries (see Table 2 for a snapshot of the criteria for assessing criticality for the G20 countries for

which such information is accessible). For instance, in India, a computer resource whose incapacitation will have a destabilising impact on national security, the economy, public health, or safety is considered as critical information infrastructure. In Germany, failure or degradation of a resource that would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences is considered a critical information infrastructure.

Nineteen different criteria to identify critical sectors have emerged among the 15 G20 countries assessed, with 'economy' the most common. Many of the listed criteria overlap with others (for instance, availability, delivery, or integrity of essential services will also cover vital society functions and the flow of information and communication). Harmonising these will be helpful to arrive at specific criteria to identify critical infrastructure that meets the needs of all G20 countries.

**Table 2: Criteria for assessing criticality**

	India <sup>24</sup>	UK <sup>25</sup>	Brazil <sup>26,27</sup>	Argentina <sup>28</sup>	China <sup>29</sup>	South Africa <sup>30</sup>	Canada <sup>31,32</sup>	France <sup>33</sup>	Germany <sup>34</sup>	Indonesia <sup>35</sup>	Japan <sup>36</sup>	South Korea <sup>37</sup>	Saudi Arabia <sup>38</sup>	US <sup>39</sup>	EU <sup>40</sup>
National Security	*		*		*	*		*		*		*		*	*
Economy	*	*	*		*	*	*	*		*		*	*	*	
Public Health	*													*	*
Safety	*					*			*		*			*	*
Availability, delivery, or integrity of essential services		*				*			*				*		
Social Consequences		*	*												
Loss of Life		*					*								
Political			*												
International Security			*												
Livelihood					*										
Public interest					*					*	*				
Public Confidence							*								
Military Potential								*		*					
Public Services										*					
Society												*	*		
Stability						*									
Maintenance of Law and Order						*									
Vital Societal Functions															*
Flow of Information and Communication				*											

Note: Details for Italy are covered as part of the EU. Details for Mexico were not accessible in English and so have not been included. The Russian definition of critical infrastructure/critical information infrastructure was not available. Australia does not define critical infrastructure as a whole but defines the various critical sectors individually.






# **The Role of the G20**



# **2**



**T**he 2015 G20 Antalya Leaders' communique affirmed "the key role played by the United Nations in developing norms and, in this context, we welcome the 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, affirm that international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the view that all states should abide by norms of responsible state behaviour in the use of ICTs in accordance with UN resolution A/C.1/70/L.45."<sup>41</sup> As such, the G20 is committed to furthering the protection of critical infrastructure, and can play an important role in both initiating a discussion and building a consensus to establish related global norms. These norms should promote international stability and collaboration to achieve global economic cooperation,

which is the fundamental objective of the G20. The G20 must help establish a common understanding and definition of critical information infrastructure to identify common areas of cooperation. This will be in keeping with the Indian presidency's theme *Vasudhaiva Kutumbakam* (One Earth-One Family-One Future).

The G20 countries represent around 85 percent of global GDP, over 75 percent of global trade, and about two-thirds of the world population. These countries are also part of various other multilateral groupings and international organisations. Once the G20 establishes a consensus on norms to protect critical information infrastructure, it can help build an international law to protect critical information infrastructure with voluntary compliance built in. This can be done through the various multilateral and minilateral forums where the G20 countries are participants.



# **Recommendations to the G20**

# **3**



**Common definition and critical**

**sectors:** The G20 members should take a phased approach to arrive at common principles for the protection of critical infrastructure—first, establishing a common definition; next, building a broader consensus on the critical sectors; and finally, arriving at common principles for regulating critical infrastructure. This exercise will be beneficial for building a global consensus and ensuring cooperation, and will also serve as a guide for countries that are just starting to regulate critical infrastructure.

**Common principles:** While arriving at common principles for regulating critical infrastructure, the G20 countries must reaffirm and adopt certain existing norms as the foundation for future discussions. These are:

- The 2017 G20 Hamburg Action Plan,<sup>42</sup> which committed to “promote the resilience of financial services and institutions in G20 jurisdictions against the malicious use of ICT, including from countries outside the G20,” with a special emphasis on addressing terrorism. The Hamburg Action Plan also sets out the G20’s strategy for achieving

strong, sustainable, balanced, and inclusive growth.

- The 2018 G20 Buenos Aires Declaration<sup>43</sup> on the Future of the Internet Economy for promoting “trust and security, as vital for harnessing the potential of digital government, by adopting a risk management approach for appropriate uptake of digital technologies to address security risks, data loss concerns, privacy, threats and vulnerabilities in the use of ICT. Adopt risk management models to identify, assess, monitor, mitigate and manage risks as well as promote resilience and security of systems. Foster the adoption of reliable identity and trust management approaches. Promote international cooperation in regard to this matter.”
- The 2022 G20 Bali Leaders Declared<sup>44</sup> that noted “it is essential to uphold international law and the multilateral system that safeguards peace and stability. This includes defending all the Purposes and Principles enshrined in the Charter of the United Nations and adhering to international humanitarian

law, including the protection of civilians and infrastructure in armed conflicts. The use or threat of use of nuclear weapons is inadmissible. The peaceful resolution of conflicts, efforts to address crises, as well as diplomacy and dialogue, are vital. Today's era must not be of war.”

Other multilateral groupings (including the G7,<sup>45</sup> G8,<sup>46</sup> and OECD<sup>47</sup>) have also focused on protecting critical infrastructure and some of these norms can be adopted by G20:

- **Respecting international law:** The G20 should commit to protect and not damage critical infrastructure. Member countries should conduct themselves in accordance with international law and not intentionally damage critical infrastructure or impede its usage.
- **International cooperation:** The G20 countries must cooperate to prevent, mitigate, trace, and investigate cyber incidents and other malicious activities in cyberspace, and share information regarding such incidents if they target critical infrastructure. The member countries must also adopt

international standards relevant to critical infrastructure to harmonise approaches to regulation and enforcement, thereby reducing conflict. The 2023 India G20 Foreign Ministers meeting<sup>48</sup> reiterated the need for international cooperation in respect of growing threats from misuse of new and emerging technologies for terrorist purposes. Similar recognition should also be extended for international cooperation through information sharing, mutual legal assistance, adoption of international standards, and exchange of best practices in critical infrastructure.

- **Capacity-building efforts:** There is a need to invest in research and development and build capacity in emerging technologies such as AI, drones, and space, and support low- and middle-income countries in accessing such research and technologies. Further, the G20 countries should respond to requests for assistance from other states whose critical infrastructure has been affected and encourage the application of certified security technologies as per international standards.



- **Multistakeholder approach:**

There should be a multistakeholder commitment to protect critical information infrastructure, involving governments, technology companies, and civil society groups. Countries should promote partnerships among public and private stakeholders to share and analyse critical infrastructure information to prevent, investigate, and respond to damage to or attacks on such infrastructure. Countries should raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructure, and the role each must play in protecting them.

- **National laws:** Build these principles into national law to create a culture of enforcement and cooperation at the national and international levels.


**Institutional mechanism:** Creating an institutional mechanism for continuous research on and establishment of new standards for protecting critical infrastructure and assessing their implementation. Learnings should be drawn from initiatives like the Christchurch Call, which showcased the importance of public-private partnership in establishing a global order for a safe cyberspace.

Attribution: Srishti Saxena and Kaushal Mahan, "Establishing Global Norms to Protect Critical Information Infrastructure," *T20 Policy Brief*, May 2023.

## Endnotes

---

1. “Embracing Innovation in Government: Global Trends”, OECD 2018, <https://www.oecd.org/gov/innovative-government/Estonia-case-study-UAE-report-2018.pdf>
2. Catherine Stupp, “Ukraine Has Begun Moving Sensitive Data Outside Its Borders” The Wall Street Journal, June 14, 2022, <https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002>
3. “Development of Policies for Protection of Critical Information Infrastructures”, OECD, June 18 2008, [https://www.oecd.org/sti/\[40761118.pdf](https://www.oecd.org/sti/[40761118.pdf)
4. “Development of Policies for Protection of Critical Information Infrastructures”, OECD
5. “Information Technology Act, 2000”, India, [https://www.indiacode.nic.in/bitstream/123456789/13116/1/it\\_act\\_2000\\_updated.pdf](https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf)
6. “Security of Critical Infrastructure Act 2018”, Australia, <https://www.legislation.gov.au/Details/C2022C00160>
7. “National Infrastructure Strategy”, United Kingdom, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/938049/NIS\\_final\\_web\\_single\\_page.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/938049/NIS_final_web_single_page.pdf)
8. “Decree No. 9,573/2018”, Brazil, [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/decreto/D9573.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm)
9. “Decree No. 10,569/2020”; Brazil, [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/decreto/d10569.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10569.htm)
10. “Unveiling The Cybersecurity Agenda In Latin America The Argentine Case”, ADC, accessed on May 9 2023, <https://adc.org.ar/wp-content/uploads/2019/06/009-B-unveiling-the-cibersecurity-agenda-in-latin-america-the-argentine-case-2-part-01-2016.pdf>
11. “China Released Regulation on Critical Information Infrastructure”, Bird & Bird, accessed on May 9, 2023, <https://www.twobirds.com/en/insights/2021/china/china-released-regulation-on-critical-information-infrastructure>
12. Pursiainen, C. “Russia’s Critical Infrastructure Policy: What do we Know About it?”. *Eur J Secur Res* 6, 21–38 (2021), <https://doi.org/10.1007/s41125-020-00070-0>
13. “The National Strategy for Critical Infrastructure”, Canada, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf>
14. “National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure”, Canada, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf>
15. “The French CIIP Framework”, ANSSI France, accessed on May 11, 2023, <https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/>

- 
16. “National Strategy for Critical Infrastructure Protection (CIP Strategy)”, Germany, [https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis\\_englisch.pdf?\\_\\_blob=publicationFile&v=1](https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=1)
  17. “Presidential Regulation Number 82 of 2022 on Protection for Vital Information Infrastructure”, Cabinet Secretariat of the Republic of Indonesia, accessed on May 11, 2023, <https://setkab.go.id/en/president-jokowi-issues-presidential-regulation-on-protection-for-vital-information-infrastructure/>
  18. “The Cybersecurity Policy for Critical Infrastructure Protection”, NISC Japan, accessed on May 9, 2023, [https://www.nisc.go.jp/eng/pdf/cs\\_policy\\_cip\\_eng\\_v4.pdf](https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf)
  19. “Act on The Protection of Information and Communications Infrastructure”, South Korea, [https://elaw.klri.re.kr/eng\\_mobile/viewer.do?hseq=28812&type=part&key=43](https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=28812&type=part&key=43)
  20. “Act No. 8 of 2019: Critical Infrastructure Protection Act, 2019”, South Africa, [https://www.gov.za/sites/default/files/gcis\\_document/201911/4286628-11act8of2019criticalinfraprotectact.pdf](https://www.gov.za/sites/default/files/gcis_document/201911/4286628-11act8of2019criticalinfraprotectact.pdf)
  21. Emre Halisdemir, “National Cybersecurity Organisation: Turkey”, NATO CCDCOE, National Cybersecurity Governance Series, Tallinn 2021, [https://ccdcoe.org/uploads/2021/08/TUR\\_country\\_report\\_final\\_clean\\_ver\\_2408.pdf](https://ccdcoe.org/uploads/2021/08/TUR_country_report_final_clean_ver_2408.pdf)
  22. “Critical Infrastructure Sectors”, CISA US, accessed on May 9, 2023, <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>
  23. “Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection”, European Union, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008L0114>
  24. “Information Technology Act, 2000”, India
  25. “National Infrastructure Strategy”, United Kingdom
  26. “Decree No. 9,573/2018”, Brazil
  27. “Decree No. 10,569/2020”; Brazil
  28. “Unveiling The Cybersecurity Agenda In Latin America The Argentine Case”, ADC,
  29. “China Released Regulation on Critical Information Infrastructure”, Bird & Bird
  30. “Act No. 8 of 2019: Critical Infrastructure Protection Act, 2019”, South Africa
  31. “National Strategy for Critical Infrastructure”, Canada
  32. “National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure”, Canada
  33. “The French CIIP Framework”, ANSSI
  34. “CIP Strategy”, Germany
  35. “Presidential Regulation Number 82 of 2022 on Protection for Vital Information Infrastructure”, Cabinet Secretariat of the Republic of Indonesia
  36. “The Cybersecurity Policy for Critical Infrastructure Protection”, NISC Japan
  37. “Act on The Protection of Information and Communications Infrastructure”, South Korea



- 
38. “Critical Systems Cybersecurity Controls, (CSCC-1:2019)”, National Cybersecurity Authority Kingdom of Saudi Arabia, accessed on May 11 2023, <https://nca.gov.sa/files/cscce-en.pdf>
  39. “Critical Infrastructure Sectors”, CISA US
  40. “Council Directive 2008/114/EC”, EU
  41. “G20 Leaders’ Communiqué”, G20 Turkey, 2015
  42. “G20 Hamburg Action Plan”, G20 Germany, 2017
  43. “Ministerial Declaration, G20 Digital Economy Ministerial Meeting”, G20 Argentina, 2018
  44. “Bali Leader’s declaration”, G20 Indonesia, 2022
  45. “G7 Declaration On Responsible States Behavior In Cyberspace”, G7 Italia, 2017
  46. “G8 Principles for Protecting Critical Information Infrastructures”, cybersecurity cooperation, accessed on May 11 2023, [http://www.cybersecuritycooperation.org/documents/G8\\_CIIP\\_Principles.pdf](http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf)
  47. “Development of Policies for Protection of Critical Information Infrastructures”, OECD 2008
  48. “G20 Foreign Ministers’ Meeting, Chair’s Summary & Outcome Document”, G20 India, 2023



वसुधैव कुटुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE