Political Declaration Between EU Member States, the United States of America, and the People's Republic of China on Protecting Select Critical Infrastructure from Cyber Threats During Peacetime[1]

PREAMBLE

The preamble reiterates previous commitments of the signatories.

The signatories of this voluntary and non-binding political declaration, the European Union Member States [MS], the United States, and the People's Republic of China reiterate the voluntary, non-binding norms of responsible state behavior that emerged under the GGE and OEWG processes, in particular Norms 13c and f.[2] They especially reaffirm the following passages pertaining to critical [information] infrastructure [henceforth in this document referred to as CI and CII] during peacetime: "[a] state should not conduct or knowingly support information and communication technology (ICT) activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public." In addition to this, "[s]tates should not knowingly allow their territory to be used for internationally wrongful acts using ICTs".[3]

SCOPE

China has the most restrictive definition of CI (8 sectors) compared to the EU (11 sectors) and the United States (16 sectors). Of course, all CI should be off-limits for cyberattacks, as recommended in several GGE reports and the 2021 OEWG report.

Before drafting this fictional declaration, a "war test" was conducted to identify which critical infrastructure is of utmost criticality and deserves the most protection, i.e., is absolutely off-limits. This criticality would be elaborated in an actual EU-US-China declaration.

A "war test" means the following: if a state were to launch an attack against another, what systems would it prioritize over others in its attack? In order to pass the war test, these prioritized infrastructures must receive additional protection. Here three systems are found to be in need of such protection: early warning satellites (space), electrical grids (energy), and government (nuclear command and control systems).

I. Defining "select" critical infrastructure

The parties to this declaration concur that while any CI in the EU, US, or China – as listed in the Appendix – should not be subject to disruptive or destructive attacks during peacetime, they recognize that attacks on some CIs have special potential to escalate interstate relations and might lead to cascading effects on other CI. The following infrastructure is exceptional in this regard:

Early warning satellites
EU MS, US, and China rely on space assets for situational awareness, detecting attacks on the strategic level, and distinguishing false alarms from actual attacks. Losing this situational awareness due to external malicious cyber interference would detrimentally impact strategic stability.

Nuclear command and control
Akin to certain space assets, nuclear command and control systems are a vital component of strategic stability. In times of geopolitical crisis, any perceived targeting of those systems could incentivize the targeted entity to respond prematurely to the attacking entity.

1 The Roman text is part of the fictional agreement while the italicized text offers context and explanation.

2 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, "UNGGE Report," 2015: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement; Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, "OEWG I Final Substantive Report," 2021: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (both accessed September 26, 2023).

3 Ibid.

Electrical grids
Malicious cyber behavior against one element of an electrical grid could lead to uncontrollable and cascading effects on other CI sectors, such as health, sanitation, and transport. Electrical grids are of central importance because all other CI and CII rely on it for their functioning.

II. Logic bombs

One distinguishes between active and passive logic bombs. Active logic bombs are like time bombs planted in the infrastructure of an adversary that are set to detonate at a specific time. This cyber conduct is reckless as the operator of such bombs could lose access to the adversary's system before detonation, thereby also losing control over the ability to deactivate the malware. In contrast, passive logic bombs consist of malware inserted into an enemy's system that would only be activated once war is imminent or has already begun. This fictional declaration further restrains state behavior by explicitly stating that the planting of any logic bomb – be it active or passive – in select critical CI is off-limits during peacetime.

A logic bomb in this context is defined as malware that is inserted in critical information systems within the EU, US, or CN with (1) the goal of preparing the ground for potential future scenarios of war; (2) launching the malware at a later point in time, possibly during an armed conflict; or (3) other types of escalation. Parties declare to refrain themselves from placing one or multiple logic bombs in early warning satellites, nuclear command and control systems, and the electrical grid during peacetime.

III. Espionage

During the Cold War, the United States allegedly had an espionage research project called Canopy Wing that aimed to exploit a vulnerability in Soviet high-frequency command and control communications and would allow the United States to launch a "decapitation strike" against its adversary. If the US had had such a capability – and both the US and Soviet Union knew that Moscow could not fix its own vulnerabilities – this would have considerably increased the chance for either side to act prematurely and start a spiral of misperceptions. Equally, gaining access to sensitive space assets (e.g., early warning satellites) or electrical grids could propel misperceptions.

The EU MS, US, and China declare to refrain from espionage activities – here understood as cyber operations that are aimed at undermining the confidentiality of nuclear command and control systems, electrical grids, and sensitive space assets of the parties involved – as this could lead to misperceptions and catastrophic consequences.

IV. Overseas infrastructure

Components of a state's critical infrastructure may extend outside its geographical borders. EU MS, the United States, and China rely on entities that are located abroad or in space that provide vital functions to their societies.

The parties to this declaration declare not to conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of early warning satellites, nuclear command and control systems, and electrical grids that are not located on the sovereign territory of each respective party.

APPENDIX

Full list of critical national infrastructures that are currently defined as such by China, the United States, and the European Union:

China[4]
- Public telecommunications and information services
- Energy
- Transport
- Water
- Finance
- Public services
- E-government
- National defense science and technology industry
- Critical information systems

United States[5]
- Chemical
- Commercial facilities
- Communications
- Critical manufacturing
- Dams
- Defense industrial base
- Emergency services
- Energy
- Financial services
- Food and agriculture
- Government facilities
- Healthcare and public health
- Information technology
- Nuclear reactors, materials, and waste
- Transportation systems
- Water and wastewater systems

European Union[6]
- Energy
- Transport
- Banking
- Financial market infrastructure
- Health
- Drinking water
- Wastewater
- Digital infrastructure
- Public administration
- Space
- Production, processing, and distribution of food

This fictional draft declaration is part of the DGAP Memo "How German (Cyber) diplomacy Can Strengthen Norms in a World of Rule-Breakers" by Dr. Valentin Weber, which was originally published on September 26, 2023 at https://dgap.org/en/research/publications/how-german-cyberdiplomacy-can-strengthen-norms.

4 State Council of the People's Republic of China, "Translation: Critical Information Infrastructure Security Protection Regulations (Effective Sept. 1, 2021)," DigiChina (blog), 2021: https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021/; Huijie Shao, "China Releases New Regulations on the Protection of Critical Information Infrastructure," Perkins Coie, October 25, 2021: https://www.perkinscoie.com/en/news-insights/china-releases-new-regulations-on-the-protection-of-critical-information-infrastructure.html (both accessed September 26, 2023).

5 The White House, "Presidential Policy Directive – Critical Infrastructure Security and Resilience," whitehouse.gov, February 12, 2013: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed September 25, 2023).

6 There is a difference between what is defined on an EU level as critical and what is perceived to be so by EU member states. France, for instance, defines military activities as critical although they are not included in the EU list of sectors. Secretariat-General for National Defence and Security, "The Critical Infrastructure Protection in France," January 2017: https://www.sgdsn.gouv.fr/files/files/Publications/plaquette-saiv-anglais.pdf; European Parliament and Council of the European Union, "DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC," December 27, 2022: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557; European Commission, "COMMUNICATION FROM THE COMMISSION on a European Programme for Critical Infrastructure Protection," December 12, 2006: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN (all accessed September 25, 2023).