International Critical Infrastructure to be discussed in the GGE

Prof. Nohyoung Park at Korea Univ. Law School

Issue raised:

In addition to national critical infrastructures (CIs) that have been well acknowledged as a priority area of national efforts for cybersecurity, international cybersecurity efforts need to cover international CIs such as the Internet infrastructure or shared (trans-national) networks. There are also global networks like SWIFT or SITA that might merit attention in this regard.

As the issue of international CI has not received wide-spread attention and as the GGE is currently discussing the next set of proposed norms, this issue is worth to be discussed before the experts of the international community.

Discussion:

Is there a need to discuss national and international CIs in the GGE? The GGE has developed more norms on critical infrastructures and in particular ***the 4th GGE in its 2015 Report considered it useful to identify possible measures for future work, including "[i]ncreased cooperation at regional and multilateral levels to foster common understandings … on the security of ICT-enabled critical infrastructure".[1] In order for the current GGE to study such possible measures properly, common understanding on ICT-enabled CI[2] such as its meaning, should be better fostered. Without the agreement on its meaning, CIs, national and international, as a concept, should be covered in the recommendations of the GGE fully for international peace and security.***

Cyberspace and the internet are an essential infrastructure for people, business and government worldwide. Malicious cyber operations of States and non-State actors are now a daily occurrence, making the global digital environment increasingly unpredictable and unstable.

First, ***how the issue of international CIs has been dealt with in the GGEs***

The Reports issued by the GGE in 2010, 2013 and 2015 all cover certain recommendations in relation to CIs, which are described in a varied way. For example, the 2010 Report mentions 'critical infrastructures', 'critical national information infrastructure', 'critical national and international infrastructure'. The 2013 Report mentions 'national infrastructure', 'critical infrastructure', 'ICT infrastructure', and 'critical ICT infrastructure'. The 2015 Report mentions 'critical infrastructure and associated information systems of a State', 'ICT-dependent infrastructure', 'critical infrastructure to

---

[1] 2015 Report para. 30(b).

[2] Most CIs are now enabled by the ICTs.

provide services to the public', 'their [States] critical infrastructure', 'critical information infrastructures', 'whose [another State] critical infrastructure', 'critical infrastructure of another State', 'ICT-enabled infrastructure', 'critical infrastructure vulnerabilities that transcend national borders', 'ICT-enabled critical infrastructure', 'ICT infrastructure', 'critical infrastructure of a State', 'critical ICT infrastructure', 'ICT infrastructure within their [States] territory', 'ICT infrastructure located within their [States] territory', and 'ICT infrastructure of a State'.

While the 2010 Report and the 2013 Report clearly mention 'critical national information infrastructure', 'critical national and international infrastructure', and 'national infrastructure', the 2015 Report does not mention directly those national or international infrastructures. However, the 2015 Report indicates those national CIs by mentioning 'critical infrastructure and associated information systems of a State', 'their [States] critical infrastructure', 'whose [another State] critical infrastructure', 'critical infrastructure of another State', 'critical infrastructure of a State', 'ICT infrastructure within their [States] territory', 'ICT infrastructure located within their [States] territory', and 'ICT infrastructure of a State', while it indicates those international CIs or transnational nature of CIs by mentioning 'critical infrastructure vulnerabilities that transcend national borders'. (underlined)

CIs mentioned in the GGE Reports

2010 Report	2013 Report	2015 Report
critical infrastructures'	critical infrastructure'	critical infrastructure
critical national information infrastructure'		critical information infrastructures'
critical national and international infrastructure		
	national infrastructure'	
	critical ICT infrastructure'	critical ICT infrastructure
		ICT-dependent infrastructure'
		ICT-enabled infrastructure'
		ICT-enabled critical infrastructure'
		ICT infrastructure'

Although the 2010 report explicitly recommends further dialogue among States on norms pertaining to State use of ICTs to reduce collective risk and protect 'critical national and international infrastructure',[3] the 2013 Report does not cover explicitly 'critical international

[3] 2013 Report para. 3.

infrastructure'.[4] The 2015 Report also mainly covers national CIs, although it acknowledges a transnational nature of CIs by recommending States to facilitate cross-border cooperation to address 'critical infrastructure vulnerabilities that transcend national borders' as part of confidence-building measures[5] and capacity-building measures[6]. Those CIs without an apparent link to a State or another State may not indicate that they are national CIs only. For example, the 2015 Report recommends that "[a] State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructures or otherwise impairs the use and operation of critical infrastructure to provide services to the public."[7] Here those CIs may not be only national CIs.

Second, ***the meaning of CIs***

The previous GGE reports do not have clear definitions on CIs. ***Like the UNGA resolutions[8], the GGE reports suggest that each State should define the categories of CIs and then voluntarily provide their national views on those categories of CIs as part of voluntary confidence-building measures.[9]***

---

[4] However, the 2013 Report directly and indirectly indicates those national CIs by mentioning '[t]hreats to individuals, businesses, national infrastructure and Governments' (para. 6) and 'their [States] jurisdiction over ICT infrastructure within their territory. (para. 20).

[5] These measures are suggested to include the development of mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure. 2015 Report para. 16(d).

[6] 2015 Report para. 21(e).

[7] 2015 Report para. 13(f).

[8] See UNGA Res. 58/199 on Creation of a global culture of cybersecurity and the protection of critical information infrastructures.

[9] 2015 Report para. 16(d). See also 2015 Report para. 17(c). Critical infrastructure, also referred to as nationally significant infrastructure, can be broadly defined as the systems, assets, facilities and networks that provide essential services and are necessary for the national security, economic security, prosperity, and health and safety of their respective nations. Critical Five, "Forging a Common Understanding for Critical Infrastructure", Shared Narrative, p. 2, (March 2014), available at https://www.dhs.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf.

One of the UNGA resolutions distinguish and clarify the relationship between CIs and critical information infrastructures (CIIs). After recognizing that each country will determine its own CIIs[10], UNGA Res. 58/199 noted "the increasing links among most countries' critical infrastructures[11] … and the critical information infrastructures that increasingly interconnect and affect their operations." Here CIs are distinguished from CIIs, but their increasingly interconnecting links (due to CIIs?) are noted. Thus, effective CI protection is noted to include identifying threats to and reducing the vulnerability of CIIs.[12]

At this stage of discussion of the GGE what CIs are meant may not be properly discussed and agreed. However, there may be a need to eliminate any loophole in protecting CIs whether they are national or not. The 4th GGE already acknowledges a transnational nature of CIs by recommending States to facilitate cross-border cooperation to address CI vulnerabilities 'that transcend national borders' as part of confidence-building measures and capacity-building measures.

Third, ***usage of 'international' CI***

Although it would be inappropriate to explore what kinds of exact infrastructures could be considered as international CIs, the GGE should note that certain regional and global fora have already conceptualized international CIs, such as inter-continental undersea cable, oil and gas pipeline, telecommunication network and international banking system, based on their transnational functions and extraterritorial character.[13] For example, it was confirmed that inter-continental undersea cables are by definition international CI.[14] In addition, New Zealand

---

[10] Each State is to determine its own critical information infrastructures.

[11] Those critical infrastructures are used, for example, for "the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health". UNGA Res. 58/199 on Creation of a global culture of cybersecurity and the protection of critical information infrastructures.

[12] UNGA Res. 58/199.

[13] International CIs like the internet may be called as a global public good. See Broeders, D. (2015) The public core of the internet: an international agenda for internet governance, WRR-Policy Brief no. 2, April 2015. The Hague: WRR.

[14] The Institute of Electrical and Electronics Engineers (IEEE) Global Summit on Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) Report Recommendation No. 4, Best Practices and Trusted Information Sharing; IEEE ROGUCCI Report Recommendation No. 5, New International Governance; IEEE ROGUCCI Report Recommendation No. 6, International

in particular highlights new points of vulnerability from the integrated and networked character of 'national and international infrastructures', such as electricity, gas and water grids, telecommunications networks, air, rail and shipping services, and the extent to which daily life depends on their efficient functioning.[15]

Fourth, facts of international CIs: submarine cables

Submarine cables are the backbone of the international telecommunications network. Over 95% of transoceanic communication is sent via submarine cable. Submarine cables are a fundamental component of the 'critical global infrastructure' as they function as the backbone of the international telecommunications system.[16] Each day the SWIFT (Society for Worldwide Interbank Financial Telecommunications) transmits about 15 million messages to more than 8300 banking organizations, securities intuitions, and corporate customers in 208 countries. The United States CHIPS (Clearing House for Interbank Payment System) process over USD 1 Trillion per day to more than 22 countries for all manner of commodity exchanges, investments, and securities. There is no single global submarine network any more than there is a single world airline network (about 236 cable systems = 997,336 KM). Cable systems are generally owned by consortia of 4-30 private companies or on occasion a single company-About 99% are non-government owned. Cable systems are not "flagged" to any one State.[17]

Submarine cables are protected by international treaties: the 1884 International Convention for the Protection of Submarine Cables; the 1958 Geneva Conventions of the Continental Shelf and High Seas; and the 1982 United Nations Convention on Law of the Sea (UNCLOS). They establish universal norms such as freedom to lay, maintain and repair cables outside of a State's 12 nautical mile territorial sea and national obligations to impose criminal and civil penalties for intentional or

---

Communications Infrastructure Standard for the Financial Sector.

[15] New Zealand's Cyber Security Strategy from June 2011, reprinted in Critical Five, "Forging a Common Understanding for Critical Infrastructure", Shared Narrative, p. 11, (March 2014), https://www.dhs.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf. The Critical Five is an international forum, established in 2012, comprising members from government agencies responsible for critical infrastructure protection and resilience in Australia, Canada, New Zealand, the United Kingdom, and the United States.

[16] Oceans and the law of the Sea, Report of the Secretary-General, A/70/74, 30 March 2015.

[17] Douglas R. Burnett, "Submarine Cables and the UNCLOS", 2016 ABNJ Regional Leaders Program, 25 March 2016.

negligent injury to cables, etc. UNCLOS and state practice have provided adequate governance for international cables outside of national waters, and state practice increasingly recognizes the importance of protecting cables from activities that could damage them. In recognition of its importance as the backbone of the internet, marine activities posing a serious risk of damage to submarine cables are prohibited in in certain zone designated by governments.[18]

In 1988 the first transoceanic fibre-optic cable was installed, and in 1991 Internet-based World-Wide Web (WWW) was introduced. The two new technologies complimented each other. The growing network of fibre-optic submarine cables has enabled large volumes of voice and data traffic to be rapidly carried around the globe. The Internet made data and information accessible and usable for many purposes.

International law, including any norms, governs and restrains States' behavior in many cases by requiring them do and undo certain activities. States have regarded CIs mainly under their own jurisdiction by first letting them decide what infrastructures are designated to be CIs for them. Thus, CIs are different depending on States. However, lots of CIs are based on internet and/or CIIs, which transcends States' borders. Thus, those CIs are increasingly interconnected and influencing each other. While GGEs have given more attention to national CIs, there is a good need for the GGE to also give attention to those international CIs, such as submarine cables and internet, which are connecting national CIs, and those global CIs network, such as SWIFT, which integrates a global network of national CIs such as financial infrastructures.

[18] ACMA (Australian Communications and Media Authority), 2007. NSW protection zones, http://www.acma.gov.au/ WEB/STANDARD/pc=PC_100869.