International Critical ICT Infrastructure and Norms?

Liisi Adamson, Leiden University

Critical Infrastructure

The question of international critical ICT infrastructure begins by asking what is meant by the notion of 'international' in this context. Whether it indicates that something belongs to the international community as a whole or does international indicate the cross-border nature of some critical ICT infrastructure. As there seems to be at least on the physical infrastructure level no such infrastructure that would belong to the community as a whole, the second interpretation is apt. For example undersea cables need to begin and come out somewhere and they belong to someone, whether it is a State or a private company. Satellites, similarly, belong to companies and countries.

Much of physical international critical infrastructure is covered by respective bodies of norms and law. It is clear that UNCLOS,[1] Outer Space Treaty,[2] ITU telecommunications regulations[3] and other relevant regulatory instruments already offer protection to some of the critical infrastructure components. Not only that, but undersea cables and satellites are additionally protected by State sovereignty and fall under their jurisdiction. However, when it comes to undersea cables, the international regulation could be improved. UNCLOS does not offer protection for intentional damage by foreign nationals or other States. It establishes prescriptive jurisdiction and arguably does not afford enforcement jurisdiction. Thus, cable security in general, is not comprehensively regulated under international law.

More generally, ITU is the body with a more general mandate for telecommunications regulation, unless there is a specific and explicit regulation stating otherwise (as there is in the case of undersea cables and satellites). As telecommunication qualifies the transmission of signs, signals, messages, writings, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems. Telecommunications occurs when the exchange of information between communication participants includes the use of

[1] Also consider: International Convention for Protection of Submarine cables (1884), Geneva Convention of the Continental Shelf (1958), Geneva Convention of the High Seas (1958)

[2] Also consider: Convention on International Liability for Damage Caused by Space Objects (1972), Convention on Registration of Objects Launched into Outer Space (1975), Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (1968), Agreement Governing the Activities of States on the Moon and other Celestial Bodies (1979). Additionally, the UN Principles Declarations: The Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries (Res 51/122, 13.12.1996) (Benefits Declaration), The Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting (Res 37/92, 10.12.1982) (Broadcasting Principles), The Principles Relating to Remote Sensing of the Earth from Outer Space (Res 41/65, 03.12.1986)(Remote Sensing Principles), Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space (Res 18/1962, 13.12.1963)(Declaration of Legal Principles), Principles Relevant to the Use of Nuclear Power Sources in Outer Space (Res 47/68, 14.12.1992)(Nuclear Power Sources Principles)

[3] ITU Constitution, Radio regulations etc.

technology. It is transmitted either electrically over physical media or via electromagnetic spectrum.[4]

Additionally, one should consider already existing non-binding norm initiatives for critical infrastructure. For example, the OECD Recommendation of the Council on the Protection of Critical Information Infrastructures focuses on national but also on cross-border critical infrastructure protection. Similarly, the 2002 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security aimed at providing norms for critical infrastructure protection, now replaced by 2015 Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity.[5]

OSCE adopted in 2016 additional CBMs to reduce the risks of conflict stemming from the use of information and communication technologies, adding to the previous CBM, which stated that member states will protect 'critical national and international ICT infrastructures including their integrity' (from 2013 CBMs), that the member states may collaborate in 'developing, where appropriate, shared responses to common challenges including crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure'.[6] The OSCE conference in the previous week concluded that even though given the importance of critical infrastructure to national and transnational security and the rapid expansion of cyberspace, it has become more and more likely that tensions will arise between States over cyber incidents involving critical infrastructure, OSCE is uniquely positioned to give states both the platform and the instruments to co-operate to avoid tensions in cyberspace.[7]

Furthermore, the UN resolution on 'Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures' (A-RES-58-199) and EU 2009 Communication on Critical Information Infrastructure Protection: 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience' and the follow up actions set out in 2011 in Communication on Critical Information Infrastructure Protection: 'Achievements and next steps: towards global cyber-security',[8] go to show that there are multiple normative initiatives pertaining to critical information infrastructure already in the works. The EU work has concluded that purely national approaches to tackling security and resilience challenges when it comes to critical infrastructure are not sufficient. Instead States continue their efforts to build a coherent and cooperative approach across the region.[9]

---

[4] Article 1.3 ITU Radio Regulations, ITU, Constitution and Convention of the International Telecommunication Union, Annex, 1992

[5] http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf

[6] http://www.osce.org/pc/227281?download=true

[7] http://www.osce.org/cio/300271

[8] https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip

[9] The European Parliament Resolution of 12 June 2012 on "Critical Information Infrastructure Protection: towards global cyber-security" broadly endorsed the 2011 Communication and made recommendations to the Commission for the way forward.

However, there is also a logical layer (the protocols and systems that allow the hardware to function and communicate (DNS, TCP/IP, Border Gateway Protocol, UDP etc.) that enables the functioning of the Internet and inherently belongs to the physical infrastructure (i.e. the hardware, cables, satellites). The question now becomes, whether the logical layer is already covered by existing norms or not.

Here, there seem to be two options in addressing the logical layer. One option is to say that one should treat it as the physical infrastructure. Such interpretation would mean that all the existing norms on infrastructure and telecommunications would apply to the logical layer protection as well (OECD, EU, OSCE initiatives, ITU telecom norms, UN culture of cybersecurity, IETF standards)**.**

It is clear that for example the DNS system, root servers, and protocols are essential to the functioning of the Internet, this has been also affirmed by the IETF.[10] As a matter of fact, the scale and importance of the DNS is often overlooked. When it comes to DNS, then ICANN policies and IETF standard proposals are of great importance here. IETF has produced over 8000 informational, standard-setting or otherwise relevant commentaries to the issue, including dozens of recommendations, proposed standards and best practices on network security.[11] If the logical layer is to be considered as forming a part of telecommunications in general, then ITU general regulations of no harm and no harmful interference would apply here as well. In that case, there would be no need for a separate norm that would re-state this *per se*, as interpretation would most likely suffice.

The second option is to say that it is something different than physical infrastructure. Then it also needs to be something different than content matter (information). The discourse of critical ICT infrastructure or critical infrastructure in general commonly follows the so-called silo model, where different sectors or parts of them are deemed critical, e.g. financial sector, energy sector etc. Logical layer however, runs horizontally across all the different sectors. It is the same for all the silos and thus here the sectorial approach is correct, but insufficient. Thus, stating that the logical layer does not fall under the same regulation as physical infrastructure, would mean that the community needs to have a broader discussion on the nature of such logical layer. If then the analysis yields that there is no norm, binding or non-

[10] https://www.rfc-editor.org/rfc/pdfrfc/rfc2065.txt.pdf IETF stated already in 1997 that the Domain Name System (DNS) has become a critical operational part of the Internet infrastructure yet it has no strong security mechanisms to assure data integrity or authentication.

[11] See for example: Recommended Internet Service Provider Security Services and Procedures T. Killalea [November 2000] (TXT = 27905) (Also BCP0046) (Status: BEST CURRENT PRACTICE) (Stream: IETF, Area: ops, WG: grip) (DOI: 10.17487/RFC3013) (BEST PRACTICE); DNS Security Introduction and Requirements (https://www.rfc-editor.org/rfc/pdfrfc/rfc4033.txt.pdf), Domain Name System Security Extensions: providing data integrity and authentication to security aware resolvers and applications through the use of cryptographic digital signatures (https://www.rfc-editor.org/rfc/pdfrfc/rfc2535.txt.pdf). Including the latest security-related proposed standard: Transport Layer Security (TLS) Cached Information Extension S. (https://www.rfc-editor.org/rfc/pdfrfc/rfc7924.txt.pdf)

binding, that addresses these issues, it concerns issues of international peace and security, it could be concluded that a new norm might be needed or a new norm is emerging.

Therefore, is wise to talk about international ICT infrastructure, due to the fact that global interdependencies are to an extent redefining understandings of critical infrastructure. As of now, each country approaches the topic of critical infrastructure in different ways and often without a common shared language. This is something that the UN GGE has started to create and will work on hopefully in the future as well. Without having a clear common understanding what exactly is international ICT infrastructure, it becomes difficult to assess the comprehensiveness of existing regulation, i.e. what is covered with norms and what needs to be regulated. Moreover, ambiguity in defining and delineating what do we mean under 'international' critical infrastructure is hindering the development of comprehensive security measures as well as policy and regulatory responses to threats.

Cross-boundary effects

Due to extensive interconnectedness on the physical as well as logical infrastructure layer, restricting access to the Internet and individual functions and services may affect also neighbouring countries. We have seen in over 8 years more than 50 bans (*data until first quarter of 2016*),[12] some of which have had cross-border effects. In those cases, a growing trend is for the State that has caused the lack of connection to restore it as soon as possible. As there might be besides due diligence, no better norm to regulate situations as these, there could be seen a norm emerging dealing with internet bans with cross-border effects.

However, this could be also seen as an emerging standard of due diligence in the context of ICT activities emerging from State practice. When the cut-off emanates from States' territory as a result of States' activities, it is responsible for the consequences. Third option is to look into the ITU regulations on harmful interference and the no harm clause in this context. If the State interferes also with other countries availability of functions and services, it at least is responsible under the due diligence rules for the interference emanating from its territory.

Threats

The largest threat if one considers for example the DNS and root servers is the availability and integrity of the whole system and the data therein. If DNS system is attacked, it means that the directory of domain names and translating them to Internet protocol (IP) addresses, will not work. Access, unless the IP address is known, will be cut off. This way, without facilitation requests to certain webpages, one could isolate not only whole services but also countries.

[12] CPI, State practice analysis, May 2016.

Similarly, the TCP/IP protocol has vulnerabilities on each of its layer, which can be manipulated to gain an advantage or undermine a service or function.

DNS allows attackers to redirect all incoming traffic to a server of their choosing. This enables them to launch additional attacks, or collect traffic logs that contain sensitive information. Secondly, DNS enables attackers to capture all in-bound email. More importantly, this second option also allows the attacker to send email on victims' behalf and pose as the victim. It is true that the effects can be local, when the attack is localised to specific servers, but DNS also allows attackers to take over one or more authoritative DNS servers for a domain. If an attacker were to compromise an authoritative DNS the effect would be global. For example in 2009, Twitter suffered a separate attack by the Iranian Cyber Army. The group altered DNS records and redirected traffic to propaganda hosted on servers they controlled.[13] Furthermore, some DNS attacks are even more complicated to undo. This happens when an attacker compromised the registration of the domain itself, and then uses that access to alter the DNS servers assigned to it.[14] These instances compromise the integrity as well as the availability of the system.

Logical layer hacks, and especially DNS hacks, are increasingly politically motivated. For example The Syrian Electronic Army, a pro-Assad hacking group, altered the DNS records used by the New York Times, Twitter, and the Huffington Post. The changes forced one site offline and caused problems for the others.[15] The same can happen to governmental vital services. Undermining access and availability of systems and services means that access can be lost and later regained. Attacking the integrity of a system or service on the other hand compromises and degrades the whole system, when trust is lost on who is who and what information can be trusted. Therefore, the biggest threat pertaining to the logical layer of critical ICT infrastructure is that the functionalities offer multiple opportunities to coerce States, isolate and bargain with access.

[13] http://www.computerworld.com/article/2522253/security0/twitter-s-own-account-caused-blackout--says-dns-provider.html
[14] http://dyn.com/blog/dns-101-explaining-how-hijacks-can-happen/
[15] http://www.csoonline.com/article/2133916/malware-cybercrime/three-types-of-dns-attacks-and-how-to-deal-with-them.html