GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

BRIEFINGS FROM THE RESEARCH ADVISORY GROUP

BRIEFINGS TO THE GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE FOR THE FULL COMMISSION MEETING, NEW DELHI 2017

New Delhi, November 2017

GCSC **ISSUE BRIEF №1**

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

PROMOTING STABILITY IN CYBERSPACE TO BUILD PEACE AND PROSPERITY

The Global Commission on the Stability of Cyberspace (GCSC) engages the full range of stakeholders to develop proposals for norms and policies to enhance the international security and stability of cyberspace.

@theGCSC

www.cyberstability.org

info@cyberstability.org

cyber@hcss.nl

The GCSC does not specifically endorse the respective publications, nor does it necessarily ascribe to the findings or conclusions. All comments on the content of the publications should be directed to the respective authors.

This work was carried out with the aid of a grant from GCSC partners: the Ministry of Foreign Affairs of the Netherlands, Cyber Security Agency of Singapore, Microsoft, ISOC, Ministry of Foreign Affairs of France. The views expressed herein do not necessarily represent those of the partners.

The Hague Centre for Strategic Studies

Lange Voorhout 1
2514 EA The Hague
The Netherlands

info@hcss.nl
HCSS.NL

EastWest Institute (EWI)

www.eastwest.ngo
communications@eastwest.ngo

ABOUT THE GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE

The Global Commission on the Stability of Cyberspace (GCSC) helps to develop norms and policies that advance the international security and stability of cyberspace. It promotes mutual awareness and understanding among the various cyberspace communities working on issues related to international cybersecurity. By finding ways to link the various intergovernmental dialogues on international security with the new communities created by cyberspace, the GCSC fulfils a critical need: supporting policy and norms coherence related to the security and stability in and of cyberspace by applying a multi-stakeholder approach to its deliberations on peace and security.

Chaired by Marina Kaljurand, and Co-Chairs Michael Chertoff and Latha Reddy, the Commission comprises 26 prominent Commissioners representing a wide range of geographic regions as well as government, industry, technical and civil society stakeholders with legitimacy to speak on different aspects of cyberspace.

The GCSC Secretariat is provided by The Hague Centre for Strategic Studies and supported by the EastWest Institute.

ABOUT THE BRIEFINGS

The briefings and memos included in this issue were developed by independent researchers working within the GCSC Research Advisory Group. The papers included here were submitted to the Global Commission on the Stability of Cyberspace (GCSC) in order to support its deliberations.

The opinions expressed in the publications are those solely of the authors and do not necessarily reflect the views of the GCSC, its partners, or The Hague Centre for Strategic Studies. The Commission does not specifically endorse the respective publications, nor does it necessarily ascribe to the findings or conclusions. All comments on the content of the publications should be directed to the respective authors.

The research was commissioned by the GCSC in a Request for Proposal after its Commission Meeting in Tallinn in June 2017. The Commissioners selected the winning proposals at the Commission Meeting in Las Vegas in July 2017. The researchers received the funding associated with the Request for Proposal and were invited to present their work to the Commissioners during the Commission Meeting in New Delhi in November 2017.

TABLE OF CONTENTS

OVERVIEW OF CYBER DIPLOMATIC INITIATIVES

Alex Grigsby, *assistant director of the Digital and Cyberspace Policy program at the Council on Foreign Relations*

BRIEFING №1

TABLE OF CONTENTS

INTRODUCTION

Cyberspace poses at least five unique challenges to maintaining international peace and security:

1. It is hard to attribute an attack to an actor, and when attribution is possible, it often occurs too slowly for leaders under pressure to "do something;"[1]
2. Determining the intent of a cyber operation is difficult—the same methods used for routine espionage can also be used for offensive activity;[2]
3. The use of proxies allows their sponsors to obfuscate the attribution process, but also raises questions as to the effective control that a sponsoring state has over its proxies;[3]
4. Given that cyber operations can be hard to detect, adversaries believe they can gain an advantage by attacking first, heightening the risk of a crisis;
5. The costs of entry are fairly low—even small states can buy commercially-available cyber tools to infiltrate sensitive networks.[4]

These challenges make it more likely that two or more rival states misinterpret cyber operations directed at them, and in the fog of cyberspace, take escalatory measures to protect themselves.

In successive UN reports, states have recognized that their online activities has the potential to trigger offline conflicts and that they have a common interest in improving the stability of cyberspace. What stability looks like and how it is achieved is, however, a major point of contention. Some states accept that they and their peers will continue to use cyberspace as a vehicle to pursue their interests, and seek to implement rules to make state activity predictable to decrease the risk of conflict. Others argue that stability is best achieved if states refrain or are prohibited from undertaking cyber operations in the first place.

Despite this disagreement, there is broad consensus that three types of activity help promote cyber stability: norms, both legal and voluntary, that clearly set out what states can and cannot do online; confidence building measures (CBMs) that aim to enhance states' understanding of their rivals actions' online; and capacity building to improve the ability of states to address cybersecurity incidents as well as abide by norms and participate in CBMs.

This briefing provides an overview of the diplomatic efforts and initiatives to improve the stability of cyberspace. Section one examines the interests and measures proposed by states. Section two examines multilateral initiatives. Section three examines the states' bilateral efforts. Section four examines the initiatives put forth by non-government actors. It concludes with suggestions for possible future stability measures.

---

[1] "The Problems with Seeking and Avoiding True Attribution to Cyber Attacks," RobertMLee.org, last modified March 4, 2016, http://www.robertmlee.org/the-problems-with-seeking-and-avoiding-true-attribution-to-cyber-attacks/; Tobias Feakin, "Developing a Proportionate Response to a Cyber Incident," The Council on Foreign Relations, last modified August 24, 2015, https://www.cfr.org/report/developing-proportionate-response-cyber-incident.

[2] Ben Buchanan, *Hacking, Trust, and Fear between Nations,* New York: Oxford University Press, 2016.

[3] Tim Maurer, "'Proxies in Cyberspace," Journal of Conflict & Security Law 21 no. 3 (2016): 383–403, http://carnegieendowment.org/files/JConflictSecurityLaw-2016-Maurer-383-403.pdf.

[4] Nick Carr, "Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations," *FireEye Blogs*, May 14, 2017, https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html.

Throughout this briefing, the term "offensive cyber operation" will refer to actions taken through cyberspace with the purpose of disrupting, degrading, or destroying a computer or networked system. The term "cyber operations" will refer to both offensive cyber operations and cyber espionage. The use of the term "cyber tools" refers to software and techniques that enable states to conduct their cyber operations.

SECTION 1: THE STATED INTERESTS OF MAJOR STATES ACTIVE IN THE CYBER NORMS DEBATE

All states mentioned in this section are unanimous in their agreement that the following poses a threat to international peace and security:

- States using cyberspace or information operations to pursue their foreign policy objectives;
- The buildup of cyber tools for military purposes;
- Terrorists' use of the Internet;
- Cybercrime; and
- The disruption of critical infrastructure using cyber tools.

Major powers differ on other perceived threats. Russia, China and France argue that the dominance of one state in cyberspace threatens the strategic balance of the online domain, whereas the United States, United Kingdom, European Union and India make no mention of dominance. Russia, China and India argue that the misuse of ICTs and social media can inflame social tensions and should be considered threats. Russia and China make explicit that they view interference into the internal affairs of states a threat to their sovereignty.

States also differ on the language they use to frame the threats. The United States, the European Union, and others define cybersecurity as the protection of data, software and hardware from unauthorized use. Russia, China, and certain central Asian states prefer the term information security and information space, arguing that the content of information or a message being transmitted online can interfere in the internal affairs of states and, by extension, threaten international stability. For their part, the United States, the European Union, and others place less emphasis on the content of online communications, believing it could be used to justify restrictions on expression protected by the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. This difference in framing fundamentally shapes how states perceive threats, identify their interests, and propose (and oppose) solutions.

1.1 RUSSIA

Russia identifies four primary threats in the information space:[5]

[5] Basic Principles for State Policy of the Russian Federation in the Field of International Information Security to 2020," NATO Cooperative Cyber Defense Centre of Excellence, accessed October 30, 2017, https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf.

1. The "use of information as a weapon for military and political purposes that are inconsistent with international law"—an example of which could be the leak of the Panama papers, which some analysts believe Russia interpreted as an information attack against it;6
2. The use of ICTs for terrorist purposes, such as terrorist groups using the internet to spread their message and recruit adherents;
3. The use of ICTs to interfere in the internal affairs of states;
4. The use of computer-based tools for criminal purposes, such as the creation and dissemination of malware.

Russia advocates for an "international legal regime aimed at creating conditions for the establishment of a system of international information security." This legal regime would be supported by a proposed Convention on International Information Security, a UN code of conduct, and regular bilateral and multilateral consultations, as well as establishing the International Telecommunication Union as the governing body for the Internet and developing confidence building measures to reduce the risk of misperception. Russia acknowledges that international law applies online but also argues that new law and institutions are necessary to maintain stability.

Russia's approach assumes that a state can be dominant in cyberspace, and that a unipolar environment is inherently destabilizing. Russia's strategy documents make numerous references to the need for Russia to seek "technological parity" and "equitable strategic partnership" with states, and that some countries seek to "use their technological superiority to dominate the information space."

1.2 **UNITED STATES**

The United States seeks to maintain an "open, interoperable, secure, and reliable cyberspace," and argues this should be done by: norms, confidence building measures, capacity building, law enforcement cooperation, and whole of government bilateral consultation, and participation in regional forums. Having states abide by the same norms allows their actions to become predictable, reduces misunderstandings that can lead to conflict, and contributes to the stability of the international system. Unlike Russia, the United States does not believe that new law or treaty-based mechanisms are necessary to promote stability in cyberspace. Instead, Washington argues that states should identify how existing international law, such as international humanitarian law, apply to cyberspace.

Unlike China and Russia, the United States has explicitly stated that it will seek to deter hostile state activity in cyberspace directed against it. Washington has also signaled through its confrontation with Pyongyang in 2014 and Beijing in 2014-15 that it will respond to cyber actions using a full spectrum of diplomatic tools at its disposal and that its responses will not necessarily be domain- specific.

---

[6] Adam Taylor, "Putin saw the Panama Papers as a personal attack and may have wanted revenge, Russian authors say," *Washington Post*, August 28, 2017, https://www.washingtonpost.com/news/worldviews/wp/2017/08/28/putin-saw-the-panama-papers-as-a-personal-attack-and-may-have-wanted-revenge-russian-authors-say/?utm_term=.3203df03e043; Vladimir Putin, "Remarks at the Truth and Justice regional and local media forum," April 7, 2016, http://en.kremlin.ru/events/president/news/51685.

1.3 THE UNITED KINGDOM

The United Kingdom takes a position similar to that of the United States, arguing that the rules-based environment that guides state activity offline should also guide it online. It also advocates for norms, a common understanding on how international law applies in cyberspace, confidence building measures, capacity building—namely through the Global Cyber Security Capacity Centre at the University of Oxford—, and cooperation on cybercrime.[7] The United Kingdom acknowledges that it is building a "National Offensive Cyber Program" and that it will publicly attribute state sponsored incidents when "it is in the national interest to do so."[8]

The United Kingdom has sought to shape the international debate on norms through the 2011 London Conference on Cyberspace, and subsequent conferences in Hungary (2012), Seoul (2013), the Netherlands (2015), and India (2017).[9] Known as the "London Process," these conferences seek to socialize the ideas of: cyber norms, based on existing international law; a free and open Internet, governed by the multistakeholder model; and that capacity building is necessary to bring more people safely online.

1.4 CHINA

China argues that states should be bound by four principles to guide their conduct online to improve cyber stability.[10] First, states should promote a peaceful cyberspace by opposing "acts of hostility and aggression" and "prevent arms races and conflicts." Second, states have a sovereign right to shape the online space within their jurisdiction, such as protecting critical infrastructure from malware to regulating the information on online platforms accessible within its borders. Third, states should take a multilateral approach to governing cyberspace, with the United Nations taking a leading role in building international consensus on rules to regulate online activity. Fourth, states should strive to share the benefits of online connectivity, namely by implementing the Sustainable Development Goals.[11]

In order to implement these principles, China proposes states:

- Establish dialogues on a bilateral, regional or multilateral level to increase communication, promote mutual trust, and prevent conflicts in cyberspace;

---

[7] "Global Cyber Security Centre," the University of Oxford, accessed November 1, 2017, http://www.oxfordmartin.ox.ac.uk/cybersecurity/

[8] Alex Grigsby, "Four Takeaways from the New UK Cybersecurity Strategy," Net Politics (blog), The Council on Foreign Relations, November 14, 2016, https://www.cfr.org/blog/four-takeaways-new-uk-cybersecurity-strategy.

[9] "London Conference on Cyberspace: Chair's statement," Government of the United Kingdom, accessed November 1, 2017, https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement; "Budapest Conference on Cybersecurity 2012," Budapest Conference on Cybersecurity, accessed November 1, 2017, https://web.archive.org/web/20130530035614/http:/www.cyberbudapest2012.hu/index; "Seoul Framework for and Commitment to Open and Secure Cyberspace," the Soul Conference on Cyberspace, accessed November 1, 2017, http://www.mofat.go.kr/english/visa/images/res/SeoulFramework.pdf; "Global Conference on Cyberspace 2015," GCCS 2015, accessed November 1, 2017, https://www.gccs2015.com/; "5th Global Conference on Cyberspace," GCCS 2017, accessed November 1, 2017, https://gccs2017.in/.

[10] Tian Shaohui, "International Strategy of Cooperation on Cyberspace," Xinhaunet, Janruary 3, 2017, http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm.

[11] "Sustainable Development Knowledge Platform," the United Nations, last accessed October 22, 2017, https://sustainabledevelopment.un.org/sdgs.

- Agree to an International Code of Conduct for Information Security, originally released in 2011 and updated in 2015; and
- Support capacity building initiatives to reduce the digital divide.[12]

China takes the position that there are no "general international rules in cyberspace that … govern the behavior" of states. Although Beijing has endorsed documents that reference the applicability of international law online, such as the G20 Antalya Communique or the 2013 UN GGE report, China asserts that existing law provides a general framework that should guide the creation of new rules specific to cyberspace.[13]

China sponsors annual conferences in Wuzhen as a means to promote China's interests in cyberspace, as well as promote Chinese technology companies.[14] Beijing views the Wuzhen process as a way to counterbalance the London process. Through Wuzhen, China emphasizes the importance it places on cyber sovereignty and promoting multilateral approaches to resolving differences between states.

1.5 **FRANCE**

France, like the United Kingdom and United States, stresses the applicability of international law to cyberspace and the need to develop norms. In its strategy, France argues that more dialogue is required to reach consensus on norms, that informal talks or discussions in non-traditional forums could lead to breakthroughs, and that capacity building is necessary to reduce the cyber threat to critical infrastructure. [15]

Unlike the United States and United Kingdom, France assesses that technological dependence "on a few monopolies" can pose a threat to its economic future. However, the strategy remains silent on whether Paris assesses that this dependence poses a strategic threat in the same vein that China and Russia infer that U.S. "dominance" in cyberspace is an inherent threat to cyber stability. France is also one of the few Western countries to explicitly address the threat of information operations, noting that the disruption TV5 Monde in 2015, though technically unsophisticated, undermines confidence in critical infrastructure.[16]

---

[12] The UN General Assembly, Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russia Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary General, (January 13, 2015), accessed October 22, 2017, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

[13] "G20 Leaders Communiqué," Group of Twenty, accessed October 22, 2017, http://www.mofa.go.jp/files/000111117.pdf; the UN General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/69/68 (June 24, 2013), accessed October 30, 2017, https://ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf.

[14] "World Internet Conference," Wuzhen Summit, accessed October 28, 2017, http://www.wuzhenwic.org/index.html.

[15] "La Stratégie nationale pour la sécurité du numérique : une réponse aux nouveaux enjeux des usages numériques," Agence nationale de la sécurité des systèmes d'information, accessed October 20, 2017, https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/.

[16] Gordon Coera, "How France's TV5 was almost destroyed by 'Russian hackers,'" BBC News, October 10, 2016, http://www.bbc.com/news/technology-37590375.

1.6 THE EUROPEAN UNION

The European Union's approach to cyber stability falls along the same lines as the United States, United Kingdom, and portions of the French approach. It advocates for the applicability of international law in cyberspace, the need of cyber norms, and the importance of confidence building measures to reduce strategic mistrust.[17] EU strategy documents place a heavy emphasis on the importance of a free and open online environment, where individuals' human rights offline are also upheld online.[18]

The Council of the European Union, which represents the heads of government/state of EU members, recently endorsed the use of a "cyber diplomatic toolbox," which signals to other actors how it will respond to cyber operations against it.[19] Although Council members recognize that each state has the sovereign authority to attribute and respond to a cyber incident, the EU is prepared to sanction an actor if requested to do so by a victim member state.

1.7 INDIA

India's approach to cyber issues straddles a middle ground between the US-UK-France-EU approach and the Russia-China approach. India advocates that states should seek agreement on common norms of behaviour and is hosting the London Process, but it may also be a party to the Shanghai Cooperation Organization's information security treaty through its ascension to the SCO in June 2017.[20] Recognizing that reaching consensus on norms may be challenging, India's 2016 submission to the UN Secretary General on information security issues suggests that states should prioritize confidence building measures as a way to build consensus toward norms.[21]

Unlike the United States and like-minded states, India has argued in favor of creating new bodies within multilateral institutions. One such body, which would foster discussions on cyber stability, would be hosted by the UN and is modeled on the Committee for the Peaceful Uses of Outer Space.[22]

To improve cyber stability, India advocates for cyber norms, confidence building measures, and capacity building efforts.

---

[17] "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," The European Commission, accessed October 20, 2017 http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.

[18] "Draft Council Conclusions on Cyber Policy," The Council of the European Union, February 11, 2015, http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

[19] "Cyber attacks: EU ready to respond with a range of measures, including sanctions," the Council of the European Union, accessed October 27,2017, http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.

[20] "Agreement between the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security," NATO Cooperative Cyber Defense Centre of Excellence, December 2, 2008, http://www.ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf; Kallol Bhattacherjee, "India, Pakistan become full members of SCO," *The Hindu,* June 9, 2017, http://www.thehindu.com/news/national/india-pakistan-become-full-members-of-shanghai-cooperation-organisation-sco/article18912600.ece.

[21] UN General Assembly, Resolution 70/237, Developments in the Field of Information and Telecommunications in the Context of International Security, S/RES/70, accessed October 24, 2017, https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/10/India.pdf.

[22] "The UN GGE on Cybersecurity: What is the UN's role?" the Council on Foreign Relations, last updated April 15, 2015, https://www.cfr.org/blog/un-gge-cybersecurity-what-uns-role.

1.8 **ANALYSIS**

Figure 1 identifies areas of potential agreement between states on the assumptions they make in their strategies, the threats they perceive, and the solutions to mitigating them.

For the most part, states agree that five criteria are necessary to improve international cyber stability: baseline rules (set by norms or treaty), dialogue (bilateral and multilateral), confidence building measures, law enforcement cooperation, and capacity building.

The primary fault-line between the Sino-Russian approach and that of the United States and like-minded countries is over the issue of a code of conduct or treaty. The latter are treaty averse for at least three reasons. First, states have yet to make a comprehensive assessment as to what specific provisions of existing international law apply to cyberspace. Without this, the United States and its allies argue it is premature to examine the feasibility of new law without identifying specific gaps in existing law. Second, before a treaty can be negotiated, states need a common understanding of what they are regulating. The definitional divide between the United States and Russia, for example, on information security might lead to calls for banning "information weapons" that would run into U.S. and EU concerns about regulating expression protected under international human rights law. Third, the nature of cyber tools makes it difficult, if not impossible to verify compliance with a treaty limiting their use. Malware and techniques used to undertake offensive cyber operations cannot be counted like tanks or missiles, thwarting attempts at verification—a staple of any arms control agreement.

SECTION 2: ASSESSMENT OF MULTILTERAL INITIATIVES

The diplomatic initiatives under consideration or recommended by multilateral organizations reflect the interests of their constituent members. Cyber stability-related initiatives at the North Atlantic Treaty Organization (NATO) or Group of Seven (G7) reflect the views of the United States, the United Kingdom, and France. Similarly, Shanghai Cooperation Organization (SCO) and BRICS initiatives reflect Russian and Chinese views.

Compromises that bridge the gap between the Russian-Chinese position and the United States and like-minded position tend to emerge in organizations with broader memberships, such as the United Nations (UN), Organization for Security and Cooperation in Europe (OSCE), and the Association for Southeast Asian Nations' Regional Forum (ASEAN RF).

2.1. THE UNITED NATIONS

There are three efforts at the United Nations to improve cyber stability.

First, the UN Group of Governmental Experts on Developments in the Field of Information and Communications Technologies in the Context of International Security (GGE) is the most high profile initiative. Since 2004, the Group has met five times, issuing consensus reports three times. The first consensus report recommended that states consider norms, confidence building measures, and capacity building initiatives to "reduce the risk of misperception" in cyberspace.[23] The second consensus report was the first time major powers explicitly acknowledged that "international law, in particular the Charter of the United Nations is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful, and accessible ICT environment."[24] It also encouraged the development regional confidence building measures. The third consensus report outlines voluntary peacetime norms states are encouraged to follow, such as:

- Not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
- Not intentionally damaging the critical infrastructure of another state using ICTs; and
- Responding to requests for assistance.[25]

[23] The UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/65/201 (July 30, 2010), accessed October 30, 2017, http://www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf.

[24] The UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 (June 24, 2013, accessed October 30, 2017, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

[25] The UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (July 22, 2015), accessed October 27,2017, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

The 2016-17 GGE failed to reach consensus. The United States argues it failed over states' unwillingness to explain how specific bodies of international law, such as the law of armed conflict (LOAC) or state responsibility, apply to cyberspace.[26] Cuba, echoing the views of Russia and China, argues that acknowledging LOAC would legitimize cyberspace as a domain for military conflict, giving state-sponsored cyber operations a green light.[27]

Second, the members of the SCO have circulated a draft international code of conduct for information security at the UN General Assembly.[28] The code proposes that countries voluntarily forego the "use of [ICTs] … to carry out activities which run counter to the task of maintaining international peace and security." For example, the code requests countries cooperate to combat "criminal and terrorist activities" using ICTs that incite "terrorism, separatism or extremism" and that countries not use ICTs to interfere in the internal affairs of states. Versions of the code have been floated at the UN since 2011, and has attracted some criticism for its perceived incompatibility with human rights law.[29] Given that it has yet to be introduced as a formal resolution, it is unlikely to have the support required for General Assembly adoption.

Third, the UN General Assembly adopted a resolution in 2003, calling on states to build a culture of cybersecurity by encouraging domestic stakeholders be aware of cybersecurity risks and to take steps to mitigate them.[30]

2.2 ORGANIZATION FOR SECURITY AND COOPERATION IN EUROPE

OSCE states have agreed to two series of voluntary CBMs to improve cyber stability. They encourage states to:

- exchange white papers, strategy documents and national views on cyber matters;
- hold talks "to reduce the risks of misperception … that may stem from the use of ICTs;"
- implement legislation that allows for the sharing of information related to the "terrorist or criminal use of ICTs;"

---

[26] Michele G. Markoff, "Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security," accessed October 30, 2017, https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm.

[27] "71 UNGA: Cuba at the final session of Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security," Cuba's Representative Office Abroad, accessed October 30, 2017, http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information.

[28] The UN General Assembly, Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, (A/69/723) January 13, 2015, accessed October 30, 2017, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

[29] The UN General Assembly, Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary General, A/66/359 (September 14, 2011), accessed October 30, 2017, http://www.un.org/ga/search/view_doc.asp?symbol=A%2F66%2F359&Submit=Search&Lang=E ; Alex Grigsby, "Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era?" Net Politics (blog), the Council on Foreign Relations, January 28, 2015, https://www.cfr.org/blog/will-china-and-russias-updated-code-conduct-get-more-traction-post-snowden-era; Sarah McKune, "An Analysis of the International Code for Conduct for Information Security," the Citizen Lab, September 28, 2015, https://citizenlab.ca/2015/09/international-code-of-conduct/.

[30] The UN General Assembly, Resolution 57/239, Creation of a global culture of cybersecurity, A/RES/47/239 (January 31, 2013), accessed October 22, 2017, https://www.oecd.org/sti/ieconomy/UN-security-resolution.pdf.

- nominate a national point of contact to facilitate dialogue between states on cyber matters;
- identify collaboration opportunities to improve the cybersecurity of critical infrastructure; and
- encourage the responsible disclosure of ICT vulnerabilities.[31]

According to the OSCE Secretariat, almost 90 percent of states have nominated a point of contact and shared their respective national cyber strategies and organizational mechanisms, which are available to other OSCE members through an information sharing platform called POLIS.[32]

The OSCE also operates a secure communications network, which states can use to formally inquire about another state's actions it perceives as threatening or a security risk. OSCE states have endorsed the use of the network for cyber-related inquiries, and have begun establishing the procedures states should follow when raising a cyber inquiry.

2.3 ASEAN REGIONAL FORUM

Efforts at improving cyber stability within the ASEAN region have been ongoing since at least 2010. In 2015, ARF Ministers agreed to a work plan to improve the security "in the use of ICTs" and in 2017, agreed to establish an Inter-Sessional Meeting on ICT security.[33] China, Australia, Singapore, the United States, South Korea, Malaysia, and others have held workshops to sensitise members to the importance of norms, CBMs and capacity building to improve cyber stability.

The ARF has focused its efforts on improving CERT-to-CERT collaboration, improving the ability of national CERTs to respond to incidents through exercises, and establishing a regional contact network to facilitate crisis communications. However, sustaining momentum on these projects has been difficult due to the absence of an ARF secretariat or sustained sources of funding, necessitating that each member state organize, fund, and sustain an initiative.

2.4 SHANGHAI COOPERATION ORGANIZATION

In addition to promoting their code of conduct at the United Nations, SCO members signed an agreement on "cooperation in the field of information security" in 2009.[34] The agreement outlines what its parties view as the primary threats in the information space (an almost identical reflection of the threats outlined in Russia's strategic documents),

---

[31] Decision No. 1202 OSCE Confidence Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies," Organization for Security and Co-operation in Europe, accessed October 25, 2017, http://www.osce.org/pc/227281?download=true.

[32] "OSCE Polis Home," OSCE Polis, last accessed October 25, 2017, https://polis.osce.org/home.

[33] "ASEAN Regional Forum Work Plan on Security and the Use of Information and Communication Technologies (ICTs)," ASEAN Regional Forum, accessed October 25, 2017, http://aseanregionalforum.asean.org/files/library/Plan%20of%20Action%20and%20Work%20Plans/ARF%20Work%20Plan%20on%20Security%20of%20and%20in%20the%20Use%20of%20Information%20and%20Communications%20Technologies.pdf; "Chairman's Statement of the 24th ASEAN Regional Forum: 'Partnering for Change, Engaging the World,'" ASEAN 2017, accessed October 25, 2017, http://www.asean2017.ph/wp-content/uploads/7.Chairmans-Statement-of-the-24th-ARF-FINAL.pdf.

[34] "Agreement between the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security," NATO Cooperative Cyber Defense Centre of Excellence.

and compels them to cooperate to mitigate them. To improve cyber stability, the document requires parties to, among other measures:

- "Act in the international information space" in a way that complies with "generally recognized principles and norms of international law;"
- Elaborate "collective measures regarding the development of norms of international law to curb the proliferation and use of information weapons;"
- Ensure the information security of "critical structures of the states of the parties;"
- Exchange white papers, share lessons learned, and hold regular talks on information security issues.

In 2015, China hosted a "joint online counter-terrorism exercise" to share best practices in preventing the use of the Internet for terrorism.[35] However, that was done under the SCO's Regional Anti-Terrorist Structure, not the information security agreement.

Very little is known about how this agreement is being implemented given the limited information available about it in the public domain. It could be viewed as a success, however, given that it has formed the basis for bilateral agreements Russia has signed with China, India, and South Africa (see section 3).

2.5 BRICS

In 2014, the BRICS created a working group of cyber experts under the leadership of their respective national security advisors to establish joint positions on cyber issues, and coordinate their positions in multilateral venues. Since 2014, BRICS leaders have:

- Advocated that "the use and development of ICTs through international cooperation and universally accepted norms and principles of international law is of paramount importance to ensure a peaceful, secure and open" Internet space;
- Agreed to prevent the use of the Internet "as a weapon;"
- Condemned acts of mass surveillance and the use of ICTs "to violate human rights and fundamental freedoms;"
- Called for a universally binding instrument to combat cybercrime;
- Emphasised the importance of the United Nations as a venue for cyber stability and Internet governance discussions; and
- Created a point-of-contact network among CERTs in BRICS countries.[36]

Although the BRICS communiqués reference the importance of states respecting "universal norms" and "principles of international law," none of them reprise the language contained in the 2013 UN GGE report that "international law, in particular the Charter of the United Nations is applicable and is essential to maintaining peace and stability." The 2013 GGE language is an unequivocal endorsement of the applicability of international law to cyberspace. The BRICS use of

[35] "SCO hosts first joint online counter-terrorism exercise in China," the Ministry of National Defense, the People's Republic of China, accessed October 30, 2017, http://eng.mod.gov.cn/Database/MOOTW/2015-10/15/content_4624404.htm.

[36] "The 6th BRICS Summit: Fortaleza Declaration," BRICS Information Centre, the University of Toronto, accessed October 31, 2017, http://www.brics.utoronto.ca/docs/140715-leaders.html.

language like "universal norms" and "principles of law" could be interpreted as a more muted endorsement of existing law, particularly given that Russia seeks a treaty and Moscow and Beijing promote the SCO code of conduct.

2.6 NATO

NATO's approach to cyber stability is one of norms and deterrence. NATO does this by publicly signalling the rules it believes is applicable to cyberspace (such as international law) and how it will interpret offensive cyber activity against it, with the hope that it will deter potential adversaries.

In 2014, NATO leaders agreed that international law applied to cyberspace, and that cyber defense was a "core task" of the transatlantic alliance.[37] NATO members also agreed that an offensive cyber operation against could trigger the collective self-defense provision under Article 5 of the North Atlantic treaty, and that such a decision could only be taken by the North Atlantic council, NATO's peak governing body.

2.7 GROUP OF 20

Cyber stability measures have made two appearances in G20 leaders' declarations. The first, and most consequential, was the Antalya Summit in 2015.[38] States agreed that they had a "special responsibility" to promote stability in cyberspace, and affirmed that "no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." This language is almost identical to the agreement the United States struck with China in 2015, creating a norm against economic espionage for commercial gain. Leaders also endorsed the applicability of international law to cyberspace, reprising the language used in the 2013 UN GGE report.

The second reference to cyber stability came in 2017, when leaders affirmed their commitment to ensuring a "secure ICT environment" and the "importance of collectively addressing issues of security in the use of ICTs."[39]

2.8 GROUP OF 8, THEN 7

The G8/7 has contributed to cyber stability in two ways. First, its Roma-Lyon Sub Group on High-Tech Crime maintains a 24-7 contact network for law enforcement to facilitate international collaboration on combating cybercrime.[40] The network is primarily used to request that a jurisdiction assist with accessing and preserving data for evidentiary purposes.

---

[37] "Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales," the North Atlantic Treaty Organization, accessed October 26, 2016, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[38] "G20 Leaders' Communiqué, Antalya Summit," the G20, accessed October 31, 2017, http://www.mofa.go.jp/files/000111117.pdf.

[39] "G20 Leader's Declaration: Shaping an Interconnected World," the G20, accessed October 31, 2017, https://www.g20.org/Content/EN/_Anlagen/G20/G20-leaders-declaration.pdf?__blob=publicationFile&v=11.

[40] Thomas Dougherty, "G7 24/7 Cybercrime Network," the Council of Europe, accessed October 31, 2017, https://rm.coe.int/1680303ce2.

Second, leaders or foreign ministers have addressed cyber stability in their annual communiqués, endorsing specific norms, CBMs, and capacity building efforts. In 2011, leaders expressed concern that the Internet could be used for "purposes that are inconsistent with international peace and security."[41] In 2013, foreign ministers affirmed that "international law is relevant in the digital world, as it is offline." Calling international law "relevant" (as opposed to applicable) was a compromise between Russia and the rest of the G8, and the statement was issued before the 2013 GGE report.[42]

Once Russia was expelled from the G8 in 2014, statements on cyber issues became more reflective of Western interests. The 2015 Foreign Ministers' statement reiterated the 2013 GGE report's language on the applicability of the law, the importance of capability building, and endorsed the Budapest Convention—something that would have been impossible with Russia still in the group. [43]

The 2016 leaders' communiqué included an annex enumerating steps to improve cyber stability.[44] The annex explicitly endorsed the notion that cyber activities could amount to a "use of force or armed attack within the meaning of the UN Charter" and that states could exercise their "inherent right of self defense" in response to an armed attack through cyberspace.

In 2017, G7 foreign ministers issued a Declaration on Responsible Behavior in Cyberspace.[45] The declaration reprises G7 text from 2015 and 2016, as well as the norms, CBMs, and capacity building recommendations from the 2013 and 2015 GGE reports. Unlike previous documents, it is the first to endorse the applicability of the law of state responsibility for cyberspace, endorses the use of countermeasures, and highlight that a state is "free to make its own determination" of attribution, within the confines of international law.

2.9 ORGANIZATION OF AMERICAN STATES

The OAS' primary contribution to cyber stability has been its capacity building efforts. Through its Inter-American Committee Against Terrorism (CICTE), the OAS has been training and assisting Latin American countries develop national cybersecurity strategies and build their incident response capabilities.

---

[41] "Deauville G8 Declaration: Renewed Commitment for Freedom and Democracy," European Union Archives, May 26, 2011, http://ec.europa.eu/archives/commission_2010-2014/president/news/speeches-statements/pdf/deauville-g8-declaration_en.pdf.

[42] "G8 Foreign Ministers Meeting Chair's Statement," G7 Information Centre, University of Toronto, April 12, 2012, http://www.g8.utoronto.ca/foreign/formin120412.html.

[43] "G7 Foreign Ministers' Meeting Communiqué," G7 Information Centre, University of Toronto, April 15, 2015, http://www.g8.utoronto.ca/foreign/formin150415.html; "Convention on Cybercrime," Council of Europe, November 23, 2001, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

[44] "G7 Principals and Actions on Cyber," G7 Information Centre, University of Toronto, May 27, 2016, http://www.g8.utoronto.ca/summit/2016shima/cyber.html.

[45] "G7 Declaration on Responsible States Behavior in Cyberspace," G7 Information Centre, University of Toronto, April 11, 2017, http://www.g8.utoronto.ca/foreign/170411-cyberspace.html.

In April 2017, CICTE adopted a resolution creating a working group to establish CBMs in the region.[46] The text of the resolution explicitly references the three UN GGE reports and their endorsement of CBMs as the impetus for creating the working group.

2.10 ANALYSIS

Figure 2 included in the Annex identifies areas of potential agreement between multilateral venues on norms, CBMs and capacity building.

States are most divided on the issue of norms or law for cyberspace. There is little overlap between the norms promoted by Russia/China-led organizations and those led by the United States and its allies. The only venue that brings both groups together is the UN GGE, making the norms agreed to in that group the most acceptable and likely to succeed. However, the absence of a 2017 consensus report and uncertainty about which part of the UN system will take up the cyber norms discussion in the absence of a renewed GGE mandate makes it difficult to foresee new norms emerging in the near future.

CBMs offer the most promising area of compromise given that the GGE, OSCE, ASEAN RF, SCO, and BRICS have all agreed to the following as important for cyber stability:

- Bilateral or regional talks;
- Exchanging white papers, strategy, and best practices;
- Point of contact networks and hotlines; and
- Law enforcement collaboration.

[46] "OAS to establish a working group on cooperation and confidence building measures in cyberspace," Organization of American States, April 10, 2017, http://us11.campaign-archive2.com/?u=353ff0663258ae5a775d460db&id=498d2344a8.

SECTION 3: ASSESSMENT OF BILATERAL DIALOGUES AND INITIATIVES

A number of countries have begun incorporating cyber issues into formal government-to-government dialogues, either as one topic among many in regular security talks or in separate, stand-alone tracks. In addition, think tanks have established Track 1.5 of Track 2 dialogues to encourage dialogue among potential rivals on cyber issues using non-official channels. These talks include the UK-China Track 1.5, the U.S.-China Track 2, the U.S.-Russia Track 2, the U.S.-India Track 1.5, the EU-China Track 2, and the Russian-led Garmisch Forum.[47]

The following section is not an attempt to list all of the ongoing talks, but to examine a sample of those that have resulted in specific outcomes where states agree to undertake certain activity, such as abide by a norm or establish a CBM.

3.1 THE U.S. – RUSSIA DIALOGUE

In 2013, Presidents Obama and Putin agreed to establish a standing working group on cyber issues as well as three CBMs: sharing technical information about malware or other malicious indicators between CERTs: using the Nuclear Risk Reduction Centers (NRRC) for formal inquires about "cybersecurity incidents of national concern;" and using the existing White House-Kremlin hotline to manage a cyber-related crisis should it occur. [48]

[47] "Sino- U.K. Tact 1.5 Dialogue on Cyber Security," Press Releases, Institute for Strategic Studies, last accessed October 31,2017, https://www.iiss.org/en/about%20us/press%20room/press%20releases/press%20releases/archive/2014-dd03/october-a29d/sino-uk-track-15-dialogue-on-cyber-security-1496; "Track 1.5 U.S.- China Cyber Security Dialogue," Center for Strategic and International Studies, accessed October 27, 2017, https://www.csis.org/programs/technology-policy-program/cyber-diplomacy-and-deterrence/track-15-dialogues/track-15-us-0; "First US-India Track 1.5 Cyber Dialogue held in Washington DC," Observer Research Foundation, last modified June 8, 2016, https://ssol.columbia.edu/cgi-bin/ssol/q18hKLbNH1QShCyAyXd2Ox/?p%.5Fr%.5Fid=DAZs5uO85Vzsj19HpgXgBR&p%.5Ft%.5Fid=1&tran%.5B1%.5D%.5Fentry=student&tran%.5B1%.5D%.5Ftran%.5Fname=sdar; "Sino-European Cyber Dialogue," the Hague Center for Strategic Studies, last modified December 8, 2016, https://hcss.nl/news/sino-european-cyber-dialogue-6secd; "Ninth International Forum "State, Civil Society and Business Partnership on International Information Security," Information Security Institute, last accessed October 27, 2017, http://www.iisi.msu.ru/.

[48] "Fact Sheet: U.S.-Russian Cooperation on Information and Communications Technology Security," Statements and Releases, the White House of President Barrack Obama, accessed October 31, 2017, https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol

The work of the standing working group was halted in 2014, but Russia and the United States have kept the lines of communications open, and some have sought to re-establish a formal cyber dialogue.[49] The use of the formal inquiry mechanism via the NRRC is only known to have occurred once, during the 2016 U.S. election when the White House warned Russia against further online influence operations. [50]

3.2 THE U.S. – CHINA DIALOGUE

In 2015, Presidents Obama and Xi agreed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[51] They also agreed to establish two dialogues, an experts group to discuss cyber norms and a ministerial-level group that meets biannually to "review the timeliness and quality of responses to requests for information or assistance with respect to malicious cyber activity." As part of the second dialogue, they agreed to establish a hotline should requests require escalation. The hotline was inaugurated in 2016. [52]

As a result of the agreement, private sector cybersecurity firms report that the level of Chinese cyber activity against private sector targets in the United States has declined.[53] There is no public information to indicate that the hotline has ever been used.

3.3 RUSSIA-CHINA, RUSSIA-INDIA, AND RUSSIA-SOUTH AFRICA AGREEMENTS

In 2015, Russia and China signed a bilateral agreement inspired by Russia's proposed information security convention and the SCO information security agreement.[54] The deal commits them to regular bilateral dialogues, establishing a point of contact to facilitate information exchanges, and cooperation on the creation and dissemination of cyber

---

[49] Evan Perez, "First on CNN: U.S. and Russia meet on cybersecurity," CNN, April 17, 2016, http://www.cnn.com/2016/04/17/politics/us-russia-meet-on-cybersecurity/; "Moscow in talks with U.S. to create cyber working group: RIA report," Reuters, July 20, 2017, https://www.reuters.com/article/us-russia-us-cyber-envoy/moscow-in-talks-with-u-s-to-create-cyber-working-group-ria-report-idUSKBN1A51MM.

[50] David Ignatius, "In our new Cold War, deterrence should come before détente," The Washington Post, November 15, 2016, https://www.washingtonpost.com/opinions/global-opinions/in-our-new-cold-war-deterrence-should-come-before-detente/2016/11/15/051f4a84-ab79-11e6-8b45-f8e493f06fcd_story.html?utm_term=.f629868589ee.

[51] "Fact Sheet: President Xi Jinping's State Visit to the United States," Statements and Releases, the White House of President Barack Obama, accessed November 1, 2017, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[52] "Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues," The United States Department of Justice, accessed November 1, 2017, https://www.justice.gov/opa/pr/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues.

[53] Adam Segal, "The U.S.-China Cyber Espionage Deal One Year Later," Net Politics (blog), the Council on Foreign Relations, https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later.

[54] "Agreement between the government of the Russian Federation and the government of the People's Republic of China on cooperation in the field of international information security," The Ministry of Foreign Affairs of the Russian Federation, accessed November 8, 2017, http://static.government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf.

norms. Article 4 of the agreement has been interpreted as prohibiting both countries from conducting cyber operations against each other, leaving some to label it as a non-aggression pact.[55]

There is little publicly-available information on the implementation of the agreement other than a joint statement issued a year later identifying each side's respective point of contact, and efforts to cooperate on technology to filter information online. [56]

Russia signed what is believed to be a similar deal with India in 2016 and with South Africa in 2017. [57] The texts of both deals have not been made public.

3.4 THE U.S. – INDIA FRAMEWORK

In 2016, the United States and India agreed to a framework document to guide their bilateral relationship.[58] Under the framework, both countries agree to cooperate on a range of measures, from law enforcement efforts against cyber crime to exchanging cybersecurity best practices, as well as promoting specific cyber norms recommended by the UN GGE and the G20. New Delhi and Washington have also explicitly agreed to "develop a shared understanding of international cyber stability, and destabilizing activity." The framework is valid for five years.

In addition to keeping their existing bilateral dialogues on cyber and ICT cooperation matters, the United States and India agreed to designate a point of contact for each specific area of cooperation outlined in the framework to facilitate its implementation.

---

[55] Elaine Korzak, "The Next Level for Russia-China Cyberspace Cooperation?" Net Politics (blog), the Council on Foreign Relations, August 20, 2016, https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation.

[56] "Twenty sentences to understand Sino-Russian Joint Declaration—the past and future of Sino-Russian relations are all here" (in Mandarin), Xinhuanet, June 27, 2017, http://news.xinhuanet.com/asia/2016-06/27/c_129092111.htm; Andrei Soldatov and Irina Borogan, "Putin brings China's Great Firewall to Russia in cybersecurity pact," the Guardian, November 29, 2016, https://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact.

[57] Arun Mohan Sukumar, "India and Russia sign cyber agreement, pushing the frontier for strategic cooperation," Digital Frontiers (blog), Observer Research Foundation, October 15, 2016, http://www.orfonline.org/expert-speaks/india-and-russia-cyber-agreement/.

[58] "Press release on signing a cooperation agreement between the Government of the Russian Federation and the Government of the Republic of South Africa on maintaining international information security," the Ministry of Foreign Affairs of the Russian Federation, accessed November 1, 2017, http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2854430.

SECTION 4: NON-STATE PROPOSALS

Non-state actors, such as research organizations and private companies, have also sought to shape the cyber stability debate. Their suggestions range from promoting new norms for state behavior to creating new organizations to assist with the challenge of publicly attributing cyber operations. This section will provide an overview of some of the more prominent proposals

4.1 CREATING AN ATTRIBUTION ORGANISATION

Some academics and Microsoft have made the argument that an independent attribution organization could improve cyber stability by having a group of geographically diverse experts review evidence, making the evidence available for peer review, and publishing its findings as appropriate.[59]

Microsoft sponsored a RAND corporation study that examined what a possible attribution organization could look like to ensure that its attribution determinations are evidence-based and credible. The study argued it should:

- Contain a mix of geographically representative technical and cyber policy experts, between 20 and 40 people in total, drawn from academia, technology companies, and research organizations;
- Not include state representatives or rely on information provided by states; and
- Conduct its activities transparently and publish its findings.[60]

The study suggests the creation of a Global Cyber Attribution Consortium built on these characteristics. Victims seeking a determination of attribution would approach the Consortium for its expertise. The Consortium would collect evidence, assess it against a publicly available framework of incidents and methods, make an attribution determination via majority vote, and communicate the finding, along with the necessary evidence, to the public. Once an attribution determination is made, it would be up to the victim state to determine a cause of action to hold the perpetrator accountable—the Consortium would have no enforcement role.

4.2 MICROSOFT'S NORMS AND THE DIGITAL GENEVA CONVENTION

Microsoft is arguably the most prominent ICT company active in the cyber stability debate, recognizing that its products are both the means by which state-sponsored offensive cyber operations are delivered and their target. Implicit in Microsoft's norms proposals is that states will continue conducting cyber operations against each other, and that

[59] Henry Farrell, "Promoting Norms for Cyberspace," the Council on Foreign Relations, last modified April 6, 2015, https://www.cfr.org/report/promoting-norms-cyberspace; Jan Neutze, "The role of cybernorms in preventing digital warfare," Microsoft EU Policy Blog, July 8, 2016, https://blogs.microsoft.com/eupolicy/2016/07/08/the-role-of-cybernorms-in-preventing-digital-warfare/.

[60] John S. Davis II et al.,"Stateless attribution: Towards International Accountability in Cyberspace," the RAND Cooperation, accessed November 1, 2017, https://www.rand.org/pubs/research_reports/RR2081.html.

norms are necessary to protect the company, its customers, and the ICT industry from the proliferation of offensive tools. The company has proposed a series of norms for states, each with a corresponding norm for the global ICT industry.[61] States should

- Not target global ICT companies to insert vulnerabilities in their products (and ICT companies should not permit states to adversely impact the security of ICT products);
- Have a clear policy on the handling of vulnerabilities that favors responsible disclosure instead of stockpiling or selling them (and ICT companies should adhere to coordinated disclosure practices for handling vulnerabilities);
- Exercise restraint in developing cyber weapons and ensure that any which are developed are limited, precise, and not reusable (and ICT companies should defend against and remediate the impact of such attacks);
- Not proliferate cyber weapons (and ICT companies should not traffic in software vulnerabilities for offensive purposes); and
- Assist the private sector to detect, contain, respond to, and recover from events in cyberspace (and ICT companies should assist states do the same).

Of these norms, only one can be said to have filtered into official diplomatic processes. The GGE, OSCE and G7 have proposed confidence building measures encouraging the responsible disclosure of computer vulnerabilities, similar to Microsoft's request that states set clear policies that favour vulnerability disclosure.

In 2017, Microsoft began making the argument for a digital Geneva convention that would codify its proposed norms in international law.[62] Unlike the Geneva Conventions, which regulate state activity during armed conflict, Microsoft argues that a digital Geneva convention would regulate state activity in cyberspace during peacetime and create an independent attribution organization.

4.3 TALLINN MANUAL

The Tallinn Manual process is an attempt to outline how existing international law applies in cyberspace. The 2013 and 2017 Manuals outline specific rules its authors believe states and non-state actors should follow in cyberspace to remain compliant with international law. Manual authors hope that a common interpretation of the law will improve cyber stability by clarifying the ground rules under which states should operate.

Russia and China view the Tallinn process skeptically. The Russian ambassador for cyber affairs criticized the first manual as a justification for the "bellicose interests of the West."[63] According to one account, these concerns are mirrored in China. [64] The 2017 manual was also criticized on the same grounds, with the Chinese expert who

[61] "From Articulation to Implementation: Enabling progress on cybersecurity norms," Microsoft, accessed November 1, 2017, https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf.

[62] Brad Smith, "The need for a Digital Geneva Convention," Microsoft on the Issues (blog), February 14, 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

[63] Tim Stevens, "Cyberweapons: an emerging global governance architecture," Palgrave Communications 3, January 10, 2017, https://www.nature.com/articles/palcomms2016102.

[64] Ashley Deeks, "Tallinn 2.0 and a Chinese View on the Tallinn Process," Lawfare (blog), May 31, 2015, https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process.

participated in its drafting quoted as saying it was "aligned with Western interests and values."[65] The Tallinn process also undermines Chinese and Russian interests—having detailed guidance on how states should interpret existing law in cyberspace undermines the argument new law is necessary.

4.5 PROPOSED NORM AGAINST UNDERMINING THE GLOBAL FINANCIAL SYSTEM

The Carnegie Endowment for International Peace (CEIP) has proposed a norm against manipulating the integrity of financial data.[66] Working on the assumption that no state has an interest in undermining faith in the global financial system, CEIP argues that states should not "conduct or knowingly support any activity that intentionally manipulates the integrity of financial institutions' data or algorithms whether they are stored or when in transit."

The norm was proposed in March 2017 and has not been incorporated in negotiated outcome documents or received formal endorsement by states.

[65] "Experts, have you heard of the Tallinn Manual?" (in Mandarin) Internet Dissemination Magazine, February, 22, 2017, http://china.huanqiu.com/mrwx/2017-02/10183186.html.

[66] Tim Maurer, Ariel Levite, and George Perkovich, "Towards a Global Norm Against Manipulating the Integrity of Financial Data," the Carnegie Endowment for International Peace, accessed November 1, 2017, http://carnegieendowment.org/2017/03/28/towards-global-norm-against-manipulating-integrity-of-financial-data-pub-68485.

CONCLUSION

Diplomatic efforts to improve cyberspace have focused on three areas: setting norms or law, CBMs, and capacity building.

Despite the considerable progress on the norms front, there still remains a large gap between the United States and its allies on one side, and Russia, China and their allies on the other. Prospects for a rapprochement seem dim for two reasons. First, the GGE has been the primary venue for the norms discussion, and it is unclear whether its mandate will be renewed as a result of its failure in issuing a 2017 consensus report. Second, Russia/China and the United States still view cyber threats in fundamentally different ways (e.g. cyber tools versus information weapons), making it difficult to establish and enforce common norms.

CBMs could offer a more promising avenue for cyber stability. CBMs do not require countries agree to a shared set of principles—instead, they foster cooperation despite the differences in principle because states recognize they have a shared interest in promoting stability.

There has been considerable work on CBMs bilaterally and in select multilateral venues, particularly on the issue of points of contacts and hotlines. However, there are a few areas where states, either in their stated cyber strategies or through multilateral venues, have explicitly expressed concern about a cyber policy issue but have not proposed a corresponding stability-related activity to address it. Within this context, more could be done in the following areas:

- Supply chain security. The challenge of mitigating the threat of backdoors being surreptitiously introduced in hardware or software has been referenced in successive GGE reports, the SCO information security agreement, the code of conduct, and national legislation in the United Kingdom, Russia, China, and others. It is also a critical concern for the private sector, whose products are often the target of these attempts. However, there is no specific CBM that has been developed to specifically address this common concern.
- Encouraging vulnerability disclosure policies. The 2015 GGE report, OSCE and private sector have endorsed the idea that countries develop vulnerability disclosure policies. Disclosing how state security agencies discover computer vulnerabilities and inform vendors could improve the stability of cyberspace by signaling to others that they are not stockpiling computer flaws for future use.[67] So far, the United States is the only country that has released any information on its vulnerabilities equities process.

Finally, aside from the national strategy documents of France, Russia, and China, very few cyber diplomatic initiatives deal with the issue of information operations, including the use of obtaining sensitive information about prominent persons and disclosing it to the public. Given the Russian and Chinese concern with "information attacks" and the United States' and France's recent experience with election campaign materials being disclosed, this might be an area where stability measures could prove fruitful.

[67] Alex Grigsby, "Disclosing Policies on Zero-Days as a Confidence-Building Measure," Net Politics (blog), the Council on Foreign Relations, November 18, 2014, https://www.cfr.org/blog/disclosing-policies-zero-days-confidence-building-measure.

ANNEXES

FIGURE 1 -- ASSUMPTIONS, THREATS AND SOLUTIONS EXPLICITLY IN STATES' CYBER-RELATED STRATEGIES

	Russia	China	United States	United Kingdom	France	European Union	India
Assumptions							
Cyberspace is unregulated	X	X					X
Norms are necessary to promote stability			X	X	X	X	
A new domain, such as cyberspace, requires new law	X	X					
The buildup of offensive cyber capabilities fuels a security dilemma	X	X			X		
The content of information online can be destabilizing	X	X					X
Perceived threats							
States using cyberspace or information operations to pursue	X	X	X	X	X	X	X

foreign policy objectives (includes espionage)							
Buildup of cyber tools for military purposes	X	X	X	X	X	X	X
One state being dominant in cyberspace, creates threats to the stability of the international system	X	X			X		
Terrorists' use of the Internet	X	X	X	X	X	X	X
Interference in the internal affairs of states or threats to sovereignty	X	X					
Cybercrime	X	X	X	X	X	X	X
Disruption of critical infrastructure	X	X	X	X	X	X	X
Misuse of ICTs/social media to inflame social tensions	X	X					X
Proposed solutions							
New international law applicable to cyberspace	X						
Affirmation that existing law applies to cyberspace	X		X	X	X	X	

A code of conduct	X	X					
Norms of responsible state behavior			X	X	X	X	X
Bilateral dialogue	X	X	X		X		
Confidence building measures	X		X		X	X	
Capacity building	X	X	X	X	X	X	
Law enforcement cooperation (bilateral or regional, not treaty-based)	X	X	X	X			
Deterrence, including public attribution and sanctions			X	X		X	

FIGURE 2 -- STABILITY-IMPROVING MEASURES REFERENCED IN MULTILATERAL INITIATIVES

	GGE	OSCE	ASEAN RF	SCO	BRICS	NATO	G20	G7	OAS
Rules/Norms/Law									
International law is applicable and essential to maintaining peace and stability on cyberspace	X					X	X	X	
States should use ICTs in accordance with principles				X	X				

of international law, particularly the political independence, territorial integrity and sovereign equality of states, non-interference in internal affairs of other states									
States should be prohibited from using the Internet as a weapon or using information weapons				X	X				
A universally-binding instrument is required to combat cybercrime					X				
States must meet their international obligations regarding internationally wrongful acts attributable to them	X							X	
States must not use proxies to commit international wrongful acts using ICTs	X							X	
States should respond to requests for assistance by another state whose critical infrastructure is subject to malicious ICT	X							X	

acts									
States should not knowingly allow internationally wrongful acts to be committed from their territory	X							X	
States should not conduct or knowingly harm CERTs	X							X	
States should not use CERTs to engage in malicious cyber activity	X							X	
States should not conduct or knowingly support activity that intentionally damages critical infrastructure	X			X (a version of this at A/69/723 PP 6)				X	
Sovereignty, and the principles that flow from it, apply to state conduct of ICT-related activities	X								
States should not conduct or support ICT-enabled theft of intellectual property with the intent of providing competitive advantages to companies or commercial sectors							X	X	
Call on states to endorse	NA							X	

and operationalize the GGE recommendations									
Cyber activities could amount to the use of force or armed attack, and potentially trigger the inherent right of self defense						X		X	
States victims of an internationally wrongful act may, in certain circumstances, resort to proportionate countermeasures								X	
States should take reasonable steps to ensure the integrity of the supply chain of ICT products	X			X				X	
Confidence Building Measures									
Bilateral or regional consultations	X	X	X	X	X				
Exchanging white papers, national strategy, doctrine, best practices, lessons learned	X	X	X	X	X			X (particularly how international law applies)	X

Developing new international law to curb proliferation and use of information weapons				X					
Establishing point-of-contact networks and hotlines, including procedures and templates on their use	X	X	X	X	X			X (law enforcement only)	
Fostering CERT-to-CERT collaboration	X		X		X				X
Developing a list of relevant terms and definitions	X	X	X						
Law enforcement collaboration	X	X (specific to terrorist use of the Internet)	X	X	X			X	
States should encourage responsible disclosure of computer vulnerabilities	X	X						X	
Table-top exercises	X		X						
Exchanging views of categories of critical infrastructure and national efforts to protect them	X	X		X					
Creating a mechanisms to classify ICT incidents in	X								

terms of scale and seriousness									
People-to-people exchanges (e.g. academic, military, law enforcement)	X			X					
Respond to requests for assistance	X			X				X	
Call on states to endorse and operationalize the GGE recommendations	NA							X	
Capacity Building									
Establishing and building the capabilities of national CERTs	X		X						X
Implement A/RES/64/211 (Global Culture of Cybersecurity)	X			X (a version of this in A/69/723 PP 9)					X
Training to assist developing countries keep abreast of international policy developments	X		X						X
Call on states to endorse and operationalize the GGE recommendations	NA							X	

AN ANALYTICAL REVIEW AND COMPARISON OF OPERATIVE MEASURES INCLUDED IN CYBER DIPLOMATIC INITIATIVES

Deborah Housen-Couriel, *Adv., LL.M., MPA-MC*

BRIEFING №2

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This Brief focuses on the analytical gaps with respect to the incorporation of measures into 84 contemporary cyber diplomatic initiatives; and the opportunities these gaps present for bolstering global cybersecurity and IPS of cyberspace. The initiatives studied are presented in Figure 1, and the accompanying analytical matrix is included in Appendix 1. Each initiative is categorized according to the type of initiating stakeholder, be it a state, international organization, intergovernmental group, non-governmental organization, academia, industry or private sector actor, law enforcement authority or other entity. Thus, in broadening the usual understanding of the term "diplomatic initiative", non-state initiatives have been included in the analysis to the extent that a reasonable basis for comparison and analysis was present. Initiatives that cross stakeholder boundaries at this first stage are relatively rare, and have been so noted in the analysis.

In the initiatives studied, 40 distinct operative measures have been identified and grouped for analysis into 27 topic clusters (for example, "Information sharing measures" and "Legislation, mutual legal assistance and legal training"). The topic clusters were not predetermined, but rather emerged from the research and analysis of the documents reviewed.

Key findings of the research include a listing of measures that are most commonly included in diplomatic initiatives across stakeholder groups. Moreover, the analysis revealed a "convergence of concept" around certain measures which different types of stakeholders have incorporated into initiatives. These are: information sharing in general, sharing of information around cyber threats, law enforcement cooperation, protection of critical infrastructure, mechanisms for cooperation with the private sector and civil society, arrangements for international cooperation, a mechanism for vulnerability disclosure, regular dialogue, the mandating of general legislative measures, training of cyber personnel, cyber education programs and conducting exercises and tabletops.

Additional analysis is required to elucidate whether the frequency of incorporation of these measures is due to their independent adoption in a variety of initiatives, or to redundancy in initiatives among similar stakeholders. Nonetheless, we propose in this Brief that this convergence of concept does indicate progress in the elucidation of the potential zones of agreement around measures for bolstering cybersecurity and at the international level.

The next stage of mapping, comparison and analysis for the development of global and national public policy with respect to IPS of cyberspace should address questions such as (a) the comparison of new initiatives to more mature ones; and (b) overlap or redundancy in stakeholders' incorporation of measures vs. cumulative and complementary take-up. Finally, to the end of influencing and leveraging future cyber diplomatic initiatives, a model for identifying proxies for impact and success of measures would deepen the understanding of which measures should be prioritized in public policy efforts.

SECTION 1: INTRODUCTION AND INITIAL FINDINGS RESULTING FROM THE GAP ANALYSIS OF CYBER DIPLOMATIC INITIATIVES

1.1 FRAMING THE NORMATIVE CHALLENGE

Diplomatic initiatives to advance global levels of cybersecurity have accelerated significantly over the past five years,[68] reflecting two key trends. The first is a deepened understanding on the part of decisionmakers that there is a steady increase in the vulnerabilities of national and trans-national computer systems and information assets to hostile acts in cyberspace. The second is the recognition that development of normative frameworks to govern state and non-state actor activity in cyberspace has become a critical issue at the global level, whether advanced by state or non-state actors.[69] A recent study has described this normative challenge as "one of the most pressing problems of global governance."[70]

The range of traditional legal and policy tools for development of such frameworks have included treaties, codes of conduct, agreements, memoranda, public declarations, national policies and the like: instruments that set transparent expectations and standards for responsible behavior of actors on the international plane and permit others to assess their intentions and actions. In the best of cases, it has been possible to conclude formal treaties that are binding on state signatories and inform policy and decision-making processes, as with the 2001 Council of Europe Convention on Cybercrime.[71] Despite criticism of the Convention at the level of its implementation and enforcement, it has been

[68] Of the 84 initiatives identified and analyzed in this Brief, 70 (83%) date from 2012 to the present.

[69] The normative challenges in this context have been explored by several scholars. See, for example, Kubo Macak, *From Cyber Norms to Cyber Rules: Re-engaging States as Lawmakers*, Leiden Journal of International Law, Vol. 30 (December 2017), pp. 877-899; and Martha Finnemore and Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, American Journal of International Law, Vol. 110, No. 3 (July 2016), pp. 425- 479; and Michael Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum*, Harvard Law School National Security Journal, Vol. 8, Issue 2 (2017).

[70] Finnemore and Hollis, *ibid*, at 429.

[71] Council of Europe, Convention on Cybercrime, ETS No.185, 2001.

effective in instituting common definitions of cyber-enabled criminal activity among its 56 state signatories and influencing such definitions in some regional treaties.[72]

Nonetheless, reaching formal agreement on binding norms governing conduct in cyberspace has proven difficult.[73] Beyond the challenges caused by the present fragmented international system and the political gaps that divide state and organizational actors,[74] cyberspace is presently characterized by several factors that impede the evolution of such binding norms. These include (a) rapid technological developments that introduce new individual and organizational activities in cyberspace, such as the Internet of Things;[75] (b) state and organizational behaviors that continue to lack transparency; (c) attribution challenges; (d) controversy about content online; and (e) the unprecedented uses and influences of social media. The widening gap between the need for normative clarity in cyberspace, on the one hand; and the possibilities of achieving consensus or agreement around norms, on the other, has changed expectations around what is achievable. This is due to both a lack of normative consensus among stakeholders and uncertainty around the current feasibility of such an undertaking at the global level.[76]

Thus, for example, the 2015 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - the last consensus report of the GGE Group - advocated "voluntary, non-binding norms of responsible State behavior" as a means to reduce risks to international peace, security and stability in cyberspace.[77] Moreover, specific measures, tools, methodologies and best practices that expressly avoid normative determinations and controversies may at present be more relevant to actors' national and global cybersecurity needs and requirements, given the present difficulties with achieving broad agreement around substantive norms.[78] Such measures, including CBMs, are of course not disconnected from normative implications - in fact, some actors explicitly attribute a normative dimension to them[79] - and may have important *de facto* effects that

---

[72] See, for instance, the African Union Convention on Cyber Security and Personal Data Protection, Article 29 and the Arab League Arab Convention on Combating Information Technology Offences, Articles 6-9.

[73] See James Lewis, *Sustaining Progress in International Negotiations on Cybersecurity, Center for Strategic and International Studies*, July 2017, p.4: "The dynamics of fragmentation in the international system limit the scope for global norms development." The challenges to achieving geopolitical agreement even around issues that diplomatic actors fully agree are beyond the scope of this Brief.

[74] See Alex Grigsby, *Overview of Cyber Diplomatic Initiatives*, GCSC, November 2017.

[75] Pew Research Center, *The Internet of Things Will Thrive by 2025*, May 2014.

[76] See references at note 2.

[77] A/70/174, 22 July 2015, at p. 7, < http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174>.

[78] The 2011 definition of cybersecurity in the framework of the non-binding standard of the International Telecommunication Union, ITU-T X.1500 ("Overview of cybersecurity") is notable in this context of normative neutrality. Cybersecurity is there defined, in part, as "The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets."

[79] See, for example, European Union Parliament, *Briefing: Cyber diplomacy confidence building measures*, October 2015. There, CBMs are categorized as part of the normative project, either as support structures for norm implementation or autonomously.

move the long-term normative process forward.[80] This proposition is supported by the initial results of the gap analysis of 84 initiatives conducted for the present Brief.[81]

1.2 METHODOLOGY

This study is based on a literature review[82] and analysis of publicly-available primary sources. While the listing of initiatives in Figure 1 does not claim to constitute a comprehensive listing of all contemporary cybersecurity-related initiatives, it aims to include a broad range of initiators and stakeholders such as standards bodies, law enforcement entities, NGOs and private sector organizations. The aim of this inclusive approach is to reflect the challenges posed by increasing diversity of international actors and to better draw out elements of commonality among current initiatives. Thus, the critical question posed regarding the inclusion or non-inclusion of a given initiative was the degree to which it incorporates measures, whether binding or voluntary, in addressing the IPS of cyberspace.

Nonetheless, the present scope did not permit an analysis of whether the frequency with which such measures are incorporated into several initiatives is due to redundancy and overlap (i.e., the same stakeholders incorporating it in several initiatives); or cumulative (i.e., reinforced in the initiatives of different stakeholders). This is an important methodological distinction in weighing the actual commonality of a given measure, and should be explored in further research and through the development of corresponding mapping tools.[83] Likewise, the actual impact of a measure on the practice of state and non-state actors and proxy measurements for its success in bolstering cybersecurity is a critical issue for policy development, as pointed out by scholars and other commentators, yet these remain at present open issues for further study.

The categorization and analysis of the 84 cyber diplomatic initiatives could have been approached from several perspectives. This Brief classifies initiatives by the type of initiating stakeholder (i.e., regional organization, law enforcement entity). The cross-reference of measures stemmed organically from the research, through comparison and analysis of the documents studied.

Finally, we note that the terms "operative measures" or "measures", as used in this Brief, refer collectively to those operative elements included in initiatives that may be designated as best practices, guidelines, recommendations, frameworks, or confidence building measures (CBM's). The current usage of these terms on the part of stakeholders is fluid, and, as discussed above, are likely to incorporate normative dimensions.[84]

Additional methodological challenges, limitations of scope and topics for further research are detailed in Part II below.

---

[80] In fact, there are varying understandings of the terminology used by the GGE and other bodies, and the degree to which CBMs are normative or procedural in nature. "The discussion about confidence-building measures in cyberspace is closely linked to the parallel debates about acceptable norms of state behaviour. While the focus on norms, both in the existing international law and non-binding political agreements, helps to establish international level of expectations about states' behaviour in cyberspace, development of CBMs provides practical tools to manage these expectations" (Patryk Pawlak, *Confidence Building Measures in Cyberspace: Current Debates and Trends*, in in Anna-Maria Osula and Henry Rõigas (Eds.), International Cyber Norms: Legal, Policy & Industry Perspectives, CCDCOE, 2016, pp.129– 153, at p. 133.)

[81] Three additional initiatives have been recently added to the analysis and remain to be will be fully integrated.

[82] Selected sources are included following Part V in the full version of the Brief.

[83] Nevertheless, Figure 1 contains the detailed data for *prima facie* evaluation of the degree of redundancy.

[84] See the discussion on this point in Finnemore and Hollis, note 2.

1.3 INITIAL FINDINGS OF THE GAP ANALYSIS

COMMON OPERATIVE MEASURES

The gap analysis that will be further elaborated herein revealed that the following operative measures are included in more than 25% of the total cyber diplomatic initiatives (21 out of the total 84). They are, in order of the frequency of their inclusion:[85]

Information sharing measures in general

- Exchange between stakeholders of information about strategies, policies, legislation, best practices, and cyber infrastructure capacity building

Mechanisms for international cooperation

- Cyber diplomacy projects, convening of conferences, task forces, learning exchanges, professional study sessions, dedicated websites

Mechanisms for government - private sector cooperation

- Closed industry roundtables convened by regulators, Information Sharing and Analysis Centers (ISACs), regulatory protections for the sharing of sensitive data between the private sector and the government and among private actors

Specific measures for transnational law enforcement cooperation and mutual legal assistance for cybercrime

- Agreed forensics procedures, standardized exchange of breach data in a timely manner, joint training of law enforcement officers, ongoing communications among cyber units in national police forces

Establishment of a specific national or organizational point of contact for information exchange

- Including a specific mandate or mention of points of contact established as CERTs, CSIRTs and FIRSTs

Technical standards are recommended or required

- Such as the ISO 27001 information technology security techniques series or the NIST Cybersecurity Framework

Creating a culture of cybersecurity or information security

- Through nationwide educational programs, advertising campaigns, transparency around legal and regulatory initiatives and platforms for public input into these

"Regular dialogue"

- Ongoing, regularly scheduled regional and bilateral meetings that address both a permanent common agenda and current issues. Such meetings may take place as "Track 2" and "Track 3" dialogues, as well

Threat sharing (in general)

- Although often not transparent, threat sharing mechanisms may include public and private actors, as well as national security entities

---

[85] The implications of the "frequency of inclusion" parameter are discussed in Section II below in the review of methodology. In general, it is difficult within the current scope of research to specify whether frequency of inclusion is redundant or cumulative, and this issue has been noted as a topic for further research.

Mechanisms for **government - third sector cooperation** (NGO's, academia, civil society, informal groups)

- Government financial support for NGO participation in international *fora*, investment in academic research programs and university degrees supporting cybersecurity, support for government outreach to the public through civil society activities for cybersecurity awareness and training

Developing common **terminology**

- Definition of cybercrimes at the level of formal agreements such as the Cybercrime Convention, cooperation on common terminology through standards bodies, glossaries collated through academic and professional joint efforts

Additional key findings are detailed in Part III.

MAPPING OF NORMATIVE ELEMENTS

Parallel to the analysis of the operative measures that are at the core of this Brief, normative elements have also been identified for each initiative and mapped out on a separate matrix, included in Appendix 2. This was done for the sake of completeness of the research, as there is significant overlap between operative and normative elements in several instances.[86] One example is Measure #6, "Ensuring technical interoperability of networks", which is ostensibly a technical task, yet has normative implications for global internet governance. Another is Norm #34 governing "the responsibility to report ICT vulnerabilities", which necessitates a technically-safe reporting mechanism. The solution to these overlaps was to include both measures and norms in the analysis, allowing some flexibility in their characterization.

Nevertheless, the core analysis of the Briefing remains focused on measures although some comparisons between the analysis of measures and norms have been addressed. Thus, the following normative elements were incorporated in more than 25% of the total cyber diplomatic initiatives (21 out of the total 84, see Appendix 2):[87]

1. Human rights, civil rights, and/or individual rights should be respected in cyberspace
2. Norms relating to internet/cyberspace governance in general
3. Protection of personal and private data
4. Norms specifying international cooperation

It is interesting to note, even from these two initial lists, that significantly more measures than norms (11 v. 4) are incorporated in the initiatives at the cutoff point of a 25% of the initiatives. This point will be further elaborated herein.

[86] Pawlak, note 13.

[87] See the explanation and reservations regarding the frequency parameter in note 18.

SECTION 2: SCOPE OF THE WORK, METHODOLOGY AND ISSUES FOR FUTURE RESEARCH

2.1 SCOPE

The Brief takes a broad and inclusive approach to the type of cyber diplomatic initiative included, by including a range of modes of agreement on operative measures. These include multilateral treaties and draft agreements (such as the Shanghai Cooperation Organization's Agreement on Cooperation in the Field of Information Security[88]); as well as less formal modes such as industry initiatives (including Microsoft's proposal for the establishment of an International Cyberattack Attribution Organization[89] and the CPMI-IOSC's Guidance on cyber resilience for financial market infrastructures[90]). In addition, some of the initiatives reviewed were not "international" by original intent, but have become so because of the degree of their *de facto* adoption by cyberspace actors in many states and organizations, such as the NIST Cybersecurity Framework.[91] The aim of this inclusive approach is to reflect the challenges posed by increasing diversity of international actors and, as discussed above, to better draw out elements of commonality among current initiatives. In sum, the critical question posed regarding the inclusion or non-inclusion of a given initiative was the degree to which it incorporates measures, whether binding or voluntary, in addressing the IPS of cyberspace.

The scope of the research, as originally prescribed, does not include evaluation of the actual impact of measures on cybersecurity policy, proxy parameters for evaluating their success, nor policy recommendations, although these are touched upon in the concluding Part V.

2.2 WORKING DEFINITION OF "CYBER DIPLOMATIC INITIATIVE"

We have used "cyber diplomatic initiative" to refer to any initiative that incorporates measures that are intended to boost cybersecurity on the international plane. The flexibility of this approach enables the inclusion of sources such as voluntary frameworks and measures, proposals from policy and academic experts, and industry guidelines, as

[88] The most recent version is available at https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf.

[89] See Microsoft, *Establishing an International Cyberattack Attribution Organization to strengthen trust online*, no date.

[90] Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions, Guidance on cyber resilience for financial market infrastructures, June 2016.

[91] The NIST Framework was developed in response to Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013 but see (regarding extensive international adoption) Evan D. Wolff, *The Global Uptake of the NIST Cybersecurity Framework*, February 2016.

explained above in Part I. The categorization by type of stakeholder may allow some conclusions to be drawn about the potential impact of each initiative on global cybersecurity. For instance, Initiative #3, the Additional Protocol to the Council of Europe Cybercrime Convention,[92] has the potential to impact signatory state behavior on the international plane differently from Initiative #63, the Oxford Global Cyber Security Capacity Centre's Cybersecurity Capacity Maturity Model for Nations. Yet as illustrated by the example of measure #4.8 for the establishment of cyber hotlines connecting the US, Russia and China (as well as MERIDIAN members[93]), caution should be exercised in drawing any definitive conclusions about the comparative impact of measures and norms based on the type of initiative or the stakeholders involved, in terms of effective compliance and overall impact on cybersecurity.[94]

METHODOLOGICAL CHALLENGES AND SCOPE LIMITATIONS

The listing of initiatives in Figure 1 has aimed to encompass all contemporary cybersecurity-related initiatives, yet does not claim to be comprehensive. Even during the Brief's drafting process several new initiatives were published. Due to limitations of time and scope it does not include, for instance, e-commerce frameworks. Several regimes relating to the protection of personal data have been included, however, because of their cybersecurity relevance.[95]

Three methodological challenges are a cause for caution in assessing the results of the gap analysis. The first concerns (a) the difficulty in accessing important initiatives, especially from Asian countries, either because they are not transparent online or because of language barriers.[96] This point has substantive implications regarding the measures and norms that are incorporated in the analysis and excluded from it, a limitation which will be discussed in the Conclusion. The second is (b) the overlapping nature of some measures, which may cause inconsistency in their categorization.[97] Finally, assessing measures by quantifying the degree of their inclusion in initiatives only provides part of the overall cybersecurity picture. One example is the inclusion of measure #4.8 "Cyber hotline for issues that may escalate" by only five initiatives out of the 84. Yet (c) the contribution of this single measure to global cybersecurity may be much greater than the inclusion of, for instance, measure #15 "Creating a culture of cybersecurity or information security", incorporated by 25 initiatives.

---

[92] Council of Europe, Additional Protocol to the Cybercrime Convention, ETS 189, 28 January 2003.

[93] A cyber hotline is also included in the OSCE measures (Decision 1202, 2016, #8).

[94] On this point, one international law scholar has observed: "Some non-obligatory international norms have produced important results, managing to obtain voluntary compliance, and even exceeding the original expectations of their supporters [...] International law tends to be effective whenever compliance is more or less automatic. This can happen either because there is no significant incentive to violate what has been agreed upon or there are reciprocal gains achieved by maintaining reliable standards." (Richard Falk, "'Voluntary' International Law and the Paris Agreement", *Global Justice in the 21st Century*, January 16, 2016),

[95] The EU General Data Protection Regulation, the African Union Convention on Cybersecurity and Personal Data Protection, and the APEC Privacy Framework have been included.

[96] One important example is China's recent regulatory initiative on cybersecurity and data protection. See Sara Xia, China Cybersecurity and Data Protection Laws: Change is Coming, China Law Blog, May 10, 2017.

[97] For instance, Norm #3 "Protection of CERTs and other cyber emergency responders" may be viewed by some as a measure without normative content. However, its grouping together with normative content in some initiatives determined its inclusion in the norms matrix.

ISSUES FOR FUTURE RESEARCH AND POLICY DEVELOPMENT THAT ARE BEYOND SCOPE

The research gave rise to some additional questions which are beyond the scope of this Brief, yet need attention to further the comparative analysis presented here. These include (a) initiatives addressing e-commerce; (b) the degree to which initiatives are implemented and enforced; (c) even when fully enforced - determination of their actual impact on cybersecurity; (d) measures that are relatively overlooked, such as research and development programs and security and privacy by design; and (e) sources of funding for the initiatives, their costs, and their financial sustainability. In addition, the data collected might be utilized to explore other research directions, including chronological patterns, the types of norms or measures preferred by a type of stakeholder, and the degree of cross-referencing among initiatives. The next stage of mapping, comparison and analysis for the development of global and national public policy with respect to cybersecurity and the IPS of cyberspace should address questions such as the comparison of new initiatives to more mature ones and overlap in stakeholders' incorporation of measures vs. cumulative and complementary take-up. A model for identifying proxies for impact and success of measures would deepen the understanding of which measures should be prioritized in public policy efforts.

SECTION 3: KEY FINDINGS WITH RESPECT TO CLASSIFICATION OF CYBER DIPLOMATIC INITIATIVES ACCORDING TO TYPE OF STAKEHOLDER

Figure 1 lists the initiatives reviewed and analyzed for this Brief.[98] We preface it with some key findings with respect to the types of stakeholders engaged with diplomatic cyber initiatives.

1. Consistent with the assumptions reviewed Part I above, **few multilateral treaties have so far been concluded to deal with cyber security**. Of the five included here, the SCO Code of Conduct (6 state parties) and the CoE Convention on Cybercrime (56 state parties) are the two core initiatives for cybersecurity. The ITU basic instruments (193 state parties) deal with the global governance of cyberspace infrastructure and some technical aspects of global communications, and the WTO GATS Agreement on Telecommunications (88 state parties) has only recently been linked to a cybersecurity context.[99] The multilaterals are strong on the adoption of measures promoting common cybersecurity terminology (#3); information sharing in general (#4.1); closing the digital divide (#18); common definitions of cybercrimes (#5.2); law enforcement cooperation (#5.3); and adoption of standards (#6).
2. There are **20 initiatives of regional organizations** – 24 when the OSCE 2016 initiatives are included (they have been separated out to highlight the organization's work on CBMs). This group of initiatives includes most regions of the world, and a robust range of measures, including vulnerability disclosure (in the EU /ENISA Good Practice Guide on Vulnerability Disclosure);[100] a strong level of incorporation of information sharing methods, including real-time, 24/7 sharing (#4.4); adoption of standards (#6); law enforcement cooperation (#5.3); R&D (#20) and mechanisms for governmental cooperation with the private and third sectors (#'s 9 and 10).

[98] There are some anomalies in the listing worth noting: the International Telecommunication Union's treaty documents appear under multilateral arrangements, while a resolution from that organization's plenipotentiary conference appears under the designation of Specialized Agency Conferences. The Wassenaar Arrangement is not categorized as a multilateral agreement as it is not considered a formal treaty by participants.

[99] See Chris Mirasola, U.S. Criticism of China's Cybersecurity Law and the Nexus of Data Privacy and Trade Law, Lawfare (blog), October 10.2017.

[100] ENISA, *Good Practice Guide on Vulnerability Disclosure*, January 2016.

3. At least four countries have published self-proclaimed "international" cybersecurity strategies: the US (2011), China (2017), the Netherlands (2017) and Australia (2017). Three out of the four have unanimously incorporated measures for law enforcement cooperation (#5.3) and general international sharing (#4.1). Other measures adopted by them include supply chain supervision (#12), threat sharing (#4.3), private sector engagement (#9) and technical standards (#6).[101]
4. It is evident to all observers that private sector actors have begun to engage intensively with cybersecurity at the global level. They have proposed at least eight initiatives in the years 2016-2017. Leaving aside their engagement with normative issues that in the past were in the exclusive purview of states (Microsoft's From Articulation to Implementation: Enabling progress on cybersecurity norms and Digital Geneva Convention are the prime examples; and ICANN's Draft Framework for Registry Operator to Respond to Security Threats may carve out a much more activist role for the private sector in coping with hostile activity in cyberspace). Some of the measures included in private sector initiatives are the establishment of mechanisms for communicating vulnerability disclosures (#4.5), the use of ISACs and FIRSTs (#'s 4.7 and 4.8), Microsoft's concept of establishing global attribution mechanisms (#5.4), cooperation arrangements between governments and the private sector and B2B (#'s 9 and 11), supply chain supervision (#12) and development of risk assessment mechanisms for increasing cybersecurity (#22).

In concluding this summary of some key cyber measures according to type of initiative stakeholders, three final examples involving three different types of stakeholders are salient, and significant to the processes taking place in the incorporation of measures at the global level. The 2015 GGE Report, the 2016 OSCE initiatives on CBMs;[102] and the 2017 bilateral agreement between India and the US indicate many identical measures. The US - India agreement includes 20 distinct measures.[103] It shares seven of these with the GGE and OSCE initiatives: information sharing in general (#4.1), sharing of information around cyber threats (#4.3), law enforcement cooperation (#5.3), protection of critical infrastructure (8.2), mechanisms for cooperation with the private sector and civil society (#'s 9 and 10), and arrangements for international cooperation (#19). At least two of these three actors have in common six more measures: a mechanism for vulnerability disclosure (#4.5), regular dialogue (#4.6), the mandating of general legislative measures (#5.1), training of cyber personnel (#13), cyber education programs (#14) and conducting exercises and tabletops (#17).

This "convergence of concept" around several measures to which different types of stakeholders have shown themselves willing to incorporate into initiatives constitutes, we propose, progress in elucidating the potential zones of agreement for measures at the international level.

The initiatives reviewed and analyzed are presented in the following table. The key number for the measure as it appears in the analytical table in Appendix 1 is indicated in green.

[101] The Netherlands international strategy takes a slightly different approach.

[102] See the OSCE's *Efforts Related to Reducing the Risks of Conflict Stemming from the Use of ICTs* and Decision No. 1202 on Confidence-Building Measures.

[103] It would be interesting to compare this 2017 initiative with bilateral agreements concluded by each party with other countries, and to follow its use in the future as a possible template for a bilateral accord on measures.

Figure 1: DIPLOMATIC CYBER INITIATIVES BY STAKEHOLDER	Key (#) and Description *Initiatives are listed in reverse chronological order within each category.*	Year
STATE-TO-STATE Multilateral treaties		
	1Shanghai Cooperation Organization, International Code of Conduct for Information Security	2015
	2International Telecommunication Union, Constitution, Convention and Administrative Regulations (Radio Regulations and Telecom Regulations (Melbourne) (Dubai)	2014 (RR 2016, ITR 1988, 2012)
	3Council of Europe, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems	2003
	4Council of Europe, Convention on Cybercrime	2001
	5WTO, General Agreement on Trade in Goods and Services (Annex on Telecommunications)	1997
Regional		
	6African Union, Internet Infrastructure Security Guidelines for Africa: A joint initiative of the Internet Society and the Commission of the African Union ("Recommendations")	2017
	7EU, Proposal for an EU Regulation on strengthening ENISA	2017
	8EU, Code of Conduct for Cloud Services Providers, v.1.7	2017
	9EU, Joint Communication, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU	2017
	10 OAS, Inter-American Committee Against Terrorism, Working Group on Cooperation and Confidence-Building Measures in Cyberspace	2017
	11 ASEAN, Chairman's Statement (para's 23 and 32) and ASEAN Cyber Capacity Programme	2017
	12 Ibero-American General Secretariat, Special Communication on Cooperation	2016

	on Cybersecurity	
	13EU, Network Security Directive	2016
	14EU, General Protection of Data Regulation	2016
	15Council of Europe, Internet Governance - Council of Europe Strategy 2016-2019	2016
	16NATO, Warsaw Summit Communique re article 5 applicability in cyberspace	2016
	17 ASEAN, Regional Forum Work Plan on Security of and in the Use of ICTs	2015
	18APEC Telecommunications and Information Working Group Strategic Action Plan 2016-2020	2015
	19 APEC Cross Border Privacy Rules (CBPR) system and Privacy Framework	2015
	20EU/ENISA, Good Practice Guide on Vulnerability Disclosure	2015
	21African Union, Convention on Cyber Security and Personal Data Protection	2014
	22EU, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace	2013
	23League of Arab States/ Gulf Cooperation Council, Arab Convention on Combating Information Technology Offences	2010
	24UN Economic Commission for Africa , African Regional Action Plan on the Knowledge Economy (ARAPKE)	2005
	25OAS, Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: a Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity	2004
	26UN Economic Commission for Africa, African Information Society Initiative	1996
Bilateral		
	27 US-India	2017
	28China-EU cybersecurity agreements / Joint Summit 2012	2015
	29 China-Russia Information Security Agreement	2015
	30China-US Agreement	2015
	31 US- Russia	2015
	31.5 China-Japan-Korea Joint MoU on CSIRT with National Responsibility	2011
UNILATERAL STATE INITIATIVE WITH INTENT TO APPLY ON THE		

INTERNATIONAL PLANE		
	32China, International Strategy of Cooperation on Cyberspace	2017
	32.1 Netherlands Building Digital Bridges- International Cyber Strategy	2017
	33 Australia, International Cyber Engagement Strategy	2017
	34US, International Strategy for Cyberspace	2011
INTERNATIONAL ORGANIZATIONS United Nations Security Council, General Assembly and GGE		
	35Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE)	2015
	36 Security Council Resolution 2178 (pp. 2-3)	2014
	37GGE 2013	2013
	38GGE 2010	2010
	39UNGA Resolution 57/239: Creation of a global culture of cybersecurity	2003
Specialized agency conferences		
	40ITU, World Telecommunication Development Conference (Dubai, 2014) Resolution 45 – Mechanisms for Enhancing Cooperation on Cybersecurity, Including Countering and Combating Spam	2014
	41 ITU, Global Cybersecurity Agenda	2007
	42ITU, World Summit on the Information Society, Tunis Commitments	2005
Standards organizations		
	43US NIST, Framework for Improving Critical Infrastructure Cybersecurity 1.1	2017

	44 US NIST-NICE Cybersecurity Workforce Framework	2017
	45 US NIST, Guide to Cyber Threat Information Sharing	2016
	46 ISO 27001 -Information technology security techniques information security management systems – requirements	2013
	47 ISO 29147, Vulnerability disclosure to vendors	2014
	48 ISO 27032, Guidelines for Cybersecurity	2012
	49 ITU-T, X.1500 Cybersecurity information exchange – Overview of cybersecurity	2011
OSCE (Note: the OSCE is a region organization, categorized separately because of its engagement with CBMs.)		
	50 OSCE, Minsk Declaration	2017
	51 OSCE, Ministerial Council Decision 5/16, Efforts Related to Reducing The Risks of Conflict Stemming from the Use of ICTs	2016
	52 OSCE, Decision No. 1202 on Confidence-Building Measures to Reduce the R Conflict Stemming from the Use of ICTs	2016
	53 OSCE, Permanent Council Decision No. 1106	2013
INTERGOVERNMENTAL DECLARATIONS		
	54 BRICS, Leaders Xiamen Declaration	2017
	55 G20, Statement on Countering Terrorism	2017
	56 G7, Declaration on Responsible States Behavior in Cyberspace	2017
	57 G7, Principles and Actions on Cyber	2016
	58 BRICS, ICT Development Agenda and Action Plan	2016
	59 G20, Antalya Summit Leaders Communique	2015
	60 G7, Foreign Ministers' Meeting Communiqué	2015
NON-GOVERNMENTAL		

ORGANIZATIONS AND ACADEMIC INSTITUTIONS		
	61Carnegie Endowment, Toward A Global Norm Against Manipulating the Integrity of Financial Data	2017
	62CCDCOE, Tallinn Manual 2.0	2017
	63 Oxford Global Cyber Security Capacity Centre, Cybersecurity Capacity Maturity Model for Nations	2017
	64Carnegie Endowment (Europe), Governing Cyberspace: A Road Map for Transatlantic Cyberpolicy Leadership (pp. 74-75)	2016
	65Freedom Online Coalition, Tallinn Agenda for Freedom Online	2014
	66Netmundial, Multistakeholder Statement	2014
	67Stanford University, Draft International Convention to Enhance Protection from Cyber Crime and Terrorism	2001
INDUSTRY AND SECTORAL ORGANIZATIONS		
	68Facebook, Building Global Community	2017
	70Google, Digital Security & Due Process: Modernizing Cross-Border Government Access Standards for the Cloud Era	2017
	71Global Internet Forum to Counter Terrorism	2017
	72Microsoft/RAND, International Cyberattack Attribution Organization	2017
	73Microsoft, Digital Geneva Convention	2017
	74 ICANN, Draft Framework for Registry Operator to Respond to Security Threats	2017
	75Microsoft, From Articulation to Implementation: Enabling progress on cybersecurity norms	2016
	76Board of the International Organization of Securities Commissions, Guidance on cyber resilience for financial market infrastructures	2016
	77US Securities and Exchange Commission, Cybersecurity Guidance	2015
	78 ICANN, Montevideo Statement on the Future of Internet Cooperation	2013
LAW ENFORCEMENT		

AGENCIES		
	79Interpol, Global Cybercrime Strategy	2017
	80Europol, European Cybercrime Center (EC3), Joint Cybercrime Action Taskforce	2014
OTHER		
	81Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies	2017
	81.5 Meridian Process for Critical Information Infrastructure Protection	2005
	82Computer Emergency Response Team (CERT / CSIRT)	No date
	83 Information Sharing Analysis Centers	No date
	84 PCH, INOC-DBA	2002

SECTION 4: SELECTED OUTCOMES OF THE GAP ANALYSIS OF THE MATRIX WITH RESPECT TO THE MEASURES INCORPORATED INTO INITIATIVES

Some of the key outcomes are as follows:[104]

MEASURES THAT WERE INCORPORATED IN INITIATIVES

More than a quarter of the initiatives across the stakeholder categories (21/84) incorporated the following measures:

KEY #	OPERATIVE MEASURE	NUMBER OF INITIATIVES INCOR-PORATING THE MEASURE (OUT OF 84 TOTAL)
4.1	Information sharing measures in general (information about strategies, policies, legislation, best practices, capacity building)	43

[104] This summary of outcomes is intended to address the concern of one of the reviewers regarding the quantity of data in the graphic representation of the gap analysis. While the summary highlights key outcomes, others are inherent in the chart provided in Appendix 1. The methodological issue of the frequency parameter is addressed in Part II above.

19	Mechanisms for international cooperation (conferences, task forces, cyber diplomacy, learning exchanges, dedicated websites)	35
9	Mechanisms for government - private sector cooperation	31
5.3	Specific mechanisms for transnational law enforcement cooperation and mutual legal assistance for cybercrime	30
4.2	Establishment of a specific national or organizational point of contact for information exchange (including mandate or suggestion of CERT, CSIRT specifically)	29
6	Technical standards recommended or required	27
15	Creating a culture of cybersecurity or information security	25
4.6	"Regular dialogue"	23
4.3	Threat sharing (in general)	23
10	Mechanisms for government - third sector cooperation (NGO's, academia, civil society, informal groups)	22
3	Developing common terminology	21
8.2	Mechanisms for protecting critical infrastructure and essential services	19
4.4	Real-time, 24/7 exchange	18
18	Closing the digital divide	15
14	Cyber education programs	14
12	Supply chain supervision	13
5.1	General cybersecurity legislative measures are mandated	12
2	Publication of a cybersecurity strategy, policy and/or incident response plan required or recommended	11
20	Research and development (R&D) mechanisms mandated	11
4.5	Mechanisms should be established for communicating vulnerability disclosures	10
23	Publication of statistics, metrics and indicators mandated or recommended	10
11	Mechanisms for B2B cooperation	9
13	Development, training and certification of cybersecurity personnel	9
17	Conducting cyber simulation exercises and tabletops	9
8.1	Common CI (critical infrastructure) terminology	8
22	Development of risk assessment mechanisms for increasing cybersecurity, including insurance risk assessment	7
24	Ensuring technical interoperability of networks	7
7	Certification of professionals, products or services recommended or required	7
1	Specification of government institutions or entities responsible for cyber governance	6
4.7	Information Sharing and Analysis Centers (ISACs) mandated or suggested	6

21	Security / privacy by design for products, systems and services is recommended	6
5.5	Programs to educate and train national legislators and other legal/regulatory personnel on cybersecurity	6
27	Promotion of gender, youth and other diversity cyberspace workforce / engagement	5
5.2	Common definitions of cybercrimes	5
26	Promotion of e-governance	3
4.9	Cyber hotline for issues that may escalate	5
5.4	Mechanism for attribution of hostile cyber activities	2
16	Developing cybersecurity leadership	2
25	Utilize generic identity certificates (digital certification) for user authentication	2
4.8	FIRSTs mandated or suggested	1

SOME ADDITIONAL GAPS IDENTIFIED FROM THE ANALYSIS

Several additional gaps stem from the analysis of initiatives carried out in this Brief. These are listed below, and may serve as a basis for the development of policy recommendations in future iterations of the research on which the Brief is based.

- It is relatively acceptable to actors to agree to general arrangements for information sharing (#4.1 – 43 initiatives – it is the leading agreed-upon measure), and even to specify a national or organizational point of contact (#4.2 – 29 initiatives) but they are less willing to commit to a 24/7, real-time exchange of cybersecurity-related information (#4.4 – 18 initiatives).
- There appears to be a high degree of readiness to cooperate around mutual legal aid and support in coping with cybercrime (#5.3 - 30 initiatives). Yet support for such cooperation by collaborating on common definitions of cybercrimes (#5.2 – 5 initiatives) and by training legislators and judges (#5.5 – 6 initiatives) is less common.
- Attribution is a key issue for many aspects of cybersecurity and law enforcement regarding cybercrimes. Only Microsoft has been willing to propose a mechanism for advancing technical means attribution (#5.4 – 2 initiatives). The novelty of the proposal, as well as its challenge to the *status quo* of non-transparency for many activities in cyberspace, are probably strong contributing factors.
- Arrangements for government cooperation with the private sector (#9 –31 initiatives) and civil society (#10 – 22 initiatives) are relatively highly prioritized. Yet such arrangements are often plagued by lack of trust and efficiency.[105] This is an "external" gap (i.e., it is not evident from the analytical matrix), and it is somewhat surprising that 7 out of 10 private sector actors include this element in their initiatives.
- Finally, there are two measures that appear, *prima facie*, to be relatively low cost/high gain modes of bolstering cybersecurity, yet are not readily included in initiatives: research and development programs (#20 –11 initiatives) and instituting recommendations regarding security and privacy by design (#21 – 6 initiatives). The reasons for their non-inclusion are unclear, and are important to pursue through further research in terms of their feasibility and potential impact on cybersecurity.

[105] See, for instance, Andrew Nolan, *Cybersecurity and Information Sharing: Legal Challenges and Solutions*, Congressional Research Service, March 16, 2015.

CONCLUSION – TOWARDS A BASELINE OF MEASURES FOR STABILITY IN CYBERSPACE - NEXT STEPS

This Brief has focused on the analytical gaps identified with respect to the incorporation of measures into current cyber diplomatic initiatives; and the opportunities these gaps may present for bolstering global cybersecurity. Some of the key gaps have been identified above, and some of the opportunities that might be leveraged by future cyber diplomatic initiatives are discussed below.

STATE AND NON-STATE ACTORS ARE CLEARLY MOVING AHEAD WITH DIPLOMATIC INITIATIVES FOR INCREASING THE STABILITY OF CYBERSPACE.

Returning to the support referred to at the outset that was expressed by the 2015 GGE Report for "voluntary, non-binding norms of responsible State behavior", including CBMs and other measures: in the intervening two years state and non-state actors alike have moved ahead in precisely this direction. We have noted above that of the 84 initiatives identified and analyzed in this Brief, 83% date from 2012 to the present, and 53 of them – 63% - date from 2015 on. This is a remarkable indication of the current interest in moving forward with the normative and practical challenges of cyberspace.

A recent example of this continued interest and commitment, which contains many of the measures reviewed in this Brief, is the April 2017 G7 Declaration on Responsible States Behavior in Cyberspace. The G7 Declaration interweaves both norms and operative measures in a document that clearly presents the intent of its signatories, countries that are relatively advanced in their utilization of cyberspace and representing some of the world's strongest economies: [106] The approach of this recent cyber diplomatic initiative is worth noting:

> *We are committed to promoting a strategic framework for conflict prevention, cooperation and stability in cyberspace, consisting of the recognition of the applicability of existing international law to State behavior in cyberspace, the promotion of voluntary, non-binding norms of responsible State behavior during peacetime, and the development and the implementation of practical cyber confidence building measures (CBMs) between States....*[107]

Future diplomatic initiatives at the global, regional and domestic levels should to be able to build on this and similar flexible approaches.[108]

---

[106] The member countries are Canada, France, Germany, Italy, Japan, the United Kingdom and the United States.

[107] At p. 2 of the Declaration.

[108] On the importance of flexibility of approach and the importance of the process of norm-building, see also Finnemore and Hollis, note 2.

TWO POINTS OF CAUTION

Nevertheless, we offer two points of caution regarding the diplomatic initiatives reviewed in this Brief. First, like-minded countries that negotiate these initiatives may be in fact echoing one another, yet excluding many others: an unreasonable proposition in such a globally-connected context as cyberspace. One example of this is the potential redundancy, reiteration and cross-referencing in the initiatives analyzed here to the 2015 GGE Report, as opposed to a potential cumulative normative effect through incorporation in more separate initiatives. Initiatives of the G7, G20, and OAS refer to the Report; yet Russia, China[109] and the BRICS countries as a group, significant players in cyberspace, do not. Some of the normative dissonance does penetrate the mutual language barriers, yet there is an urgent need to learn firsthand about the cybersecurity needs of those countries that have agreements, protocols, policies, rules, guidelines and CBMs in languages or formats that are not currently accessible. This constraint is also an acknowledged methodological shortcoming of the present Brief.

Secondly, the metrics relevant to measuring the impact and success of cybersecurity norms and measures, even when consistently implemented by actors, are still evolving.[110] It is critical for cybersecurity initiatives and the policy processes that accompany them to incorporate more transparent data regarding the relevant cost-benefit analyses, to include the public more effectively in the discussion around these costs and benefits, and to elucidate parameters and proxies for impact and success of measures.

NEXT STEPS

Some of the initial findings of this Brief's gap analysis include a "convergence of concept" around several measures and CBMs to which different types of stakeholders have shown themselves willing to incorporate into initiatives. These measures are detailed in the analytical matrix and the accompanying analysis in Parts III and IV. To the extent that they provide a baseline from which diverse stakeholders might proceed to develop new potential zones of agreement, it is proposed that a good starting point would be those measures that have been identified in this Brief as the most frequently adopted by diplomatic initiatives. Additional analysis is required to elucidate whether the frequency of incorporation of these measures is due to their independent adoption in a variety of initiatives, or to redundancy in initiatives among similar stakeholders. Nonetheless, we propose in this Brief that this convergence of concept does indicate progress in the elucidation of the potential zones of agreement around measures for bolstering cybersecurity and at the international level.

These gaps identified remain very broad and generalized at this early stage of the research, making it a challenge to formulate a sense of the next steps needed for the formation of policy. Certainly, additional metrics need to be developed for better understanding the relationships among the diplomatic initiatives studied, as well as their potential impact.

Thus, the next stage of mapping, comparison and analysis for the development of global and national public policy with respect to IPS of cyberspace should address questions such as (a) the comparison of new initiatives to more mature ones; and (b) overlap or redundancy in stakeholders' incorporation of measures vs. cumulative and complementary take-up. Finally, to the end of influencing and leveraging future cyber diplomatic initiatives, a model for identifying proxies for impact and success of measures would deepen the understanding of which measures should be prioritized in public policy efforts.

---

[109] Except for the 2015 agreement with the US, which clearly referenced that year's GGE Report.

[110] See, for example, the evaluations and metrics used in Melissa Hathaway et al, *Cyber Readiness Index 2.0*, Potomac Institute, 2015.

SELECTED BIBLIOGRAPHY

Martha Finnemore and Duncan B. Hollis, Constructing Norms for Global Cybersecurity, American Journal of International Law, Vol. 110, No. 3 (July 2016), pp. 425- 479.

Melissa Hathaway, Getting Beyond Norms: When Violating the Agreement Becomes Customary Practice, Centre for International Governance Innovation, 2017.

Camino Kavanaugh, Tim Maurer, Eneken Tikk-Ringas, Baseline Review: ICT-Related Processes and Events, Implications for International and Regional Security, ICT4Peace Foundation, 2014.

James Lewis, Sustaining Progress in International Negotiations on Cybersecurity, Center for Strategic and International Studies, July 2017.

Paul Nicholas, What are confidence building measures (CBMs) and how can they improve cybersecurity?, Microsoft, 2017.

Anna-Maria Osula and Henry Rõigas (Eds.), International Cyber Norms Legal, Policy & Industry Perspectives, CCDCOE, 2016.

Vladimir Radunovic, Towards a secure cyberspace via regional cooperation, DiploFoundation, 2017.

APPENDIX 1

ANALYTICAL MATRIX REPRESENTING MEASURES IN CYBER DIPLOMATIC INITIATIVES ACCORDING TO TYPE OF STAKEHOLDER

*Please note that the number key for identifying initiatives appears in Figure 1.

ANALYTICAL MATRIX COMPARING CYBER INITIATIVES: OPERATIVE MEASURES														
INITIATIVES (KEY TO #'s BELOW) A. OPERATIVE MEASURES ▼		STATE-TO-STATE			UNILATERALSTATE ON INTN'L PLANE	INTERNATIONAL ORGANIZATIONS				INTERGOVERN-MENTAL DECLARATIONS	NON-GOVERNMENTAL ORGANIZATIONS	INDUSTRY AND PRIVATE SECTOR	LAW ENFORCEMENT AGENCIES	OTHER
Tools and mechanisms, including CBM's, agreed upon or proposed by state or non-state actors to address IPS of cyber-space ("the how")		MULTILATERAL	REGIONAL	BILATERAL		UN	SPECIALIZED AGENCIE	STANDARDS	OTHER					
1	Specification of government institutions or entities responsible for cyber governance	2	7,13, 14,21, 22											
2	Publication of a cybersecurity strategy, policy and/or incident response plan required or recommended		13,21, 24,26				40,41	46		58	63	76,77		
3	Developing common terminology	2,3, 4,5	7,8, 13,14, 15,19,			38		45,48, 49	52,53				79	81,82

			21,23											
4	Information sharing measures													
4.1	In general (strategies, policies, information about legislation, best practices, capacity building)	1,2, 4	6,7, 8,9, 11,13 14,16, 17,18, 20,21, 22,24, 25	27,28, 29,30	32,33, 34	35,37, 38,39	40	43,45, 46,47, 48,49	50,52, 53	58	63,64, 66	71,76	79	81,82 83,84
4.2	Establishment of a specific national or organizational point of contact for information exchange (including mandate or suggestion of CERT, CSIRT specifically)	4	6,7, 9,13, 14,18, 19,20, 21,22, 23,25 ,	30,31	33,34	35,37		45,47, 49	52,53	57		70,74		82,83
4.3	Threat sharing (in general)	4	6,7,9, 13,16, 20	27,28, 30,31		35		45,47, 49	52	56,57	75	71	79,80	82,83
4.4	Real-time, 24/7 exchange	4	7, 13, 17,20, 23,25,	28,31	33	35		45,49					79,80	82,83, 84
4.5	Mechanisms should be established for communicating vulnerability disclosures		20			35		45,49	52	56	63	73,75, 76		
4.6	"Regular dialogue"	4	6,7, 9,11, 13,16, 17,18	27,28 30,31	32	35,37		45			66	71	79	81,82, 83
4.7	ISACs mandated		7					43,45				76,77		83

	or suggested													
4.8	FIRSTs mandated or suggested											75		
4.9	Cyber hotline for issues that may escalate	2.5		30,31					52					84
5	Legislation, mutual legal assistance and legal training													
5.1	General cybersecurity legislative measures are mandated	4	6,21, 22,23, 24,25	27			40		52		63		79	
5.2	Common definitions of cybercrimes	3,4	21,23								67			
5.3	Specific mechanisms for transnational law enforcement cooperation and mutual legal assistance for cybercrime	3,4	9,17, 19,21, 23,25	27,30	32,33, 34	35,37	40		52	56,57, 58, 60,61	63,67	70,74, 75	79	82,83
5.4	Mechanism for attribution of hostile cyber activities											72,75		
5.5	Programs to educate and train national legislators and other legal/regulatory personnel on cybersecurity		24	27	34						63	70	79	
6	Technical standards recommended or required	2,5	6,7, 8,9, 11,13, 14,20, 22,25, 26	27	33,34		41	44,45, 49		58	63,66	76		81,82 83
7	Certification of		7,8,	27				44,49						

	professionals, products or services recommended or required		9, 14											
8	Critical infrastructure and essential services													
8.1	Common CI terminology	2,4	21					43			63,67			82,83
8.2	Mechanisms for protecting critical infrastructure and essential services	7	6,13, 22	27		35,37		43	52	56,58	63,67	72,73, 74,75, 76		82,83
9	Mechanisms for government - private sector cooperation	5	13,16 18,19, 21,22, 24,25, 26	27	33,34		42	43,45, 47	52	55,56, 57,60	66	71,72, 73,74, 75,76, 78		82,83
10	Mechanisms for government - third sector cooperation (NGO's, academia, civil society, informal groups)	5	6,15, 16,18, 21,22, 24,26	27	34	35,37	42		52	56,57	66	71,72, 78		82,83
11	Mechanisms for B2B cooperation			27						58		71,72, 73,76, 78		82,83
12	Supply chain supervision		7	27	34			43,46, 47		58	63	75,76, 77	79	81
13	Development, training and certification of cybersecurity personnel		6,7	27		35		45,46, 48			63	76		
14	Cyber education programs		7,9, 13,15, 18, 21,22, 24,26	27		35,37			58		63			

15	Creating a culture of cybersecurity or information security	1	6,7, 9, 15, 18, 21,22, 24			35,38, 39	40,41, 42	43,45, 46,48			63,66	73,76		82,83
16	Developing cybersecurity leadership		21					46						
17	Conducting cyber simulation exercises and tabletops		7,16 18,22	27		35,37						76,77		
18	Closing the digital divide	1,2, 5	18,22, 24		32,33	35,37	40,42			57,59	66			
19	Mechanisms for international cooperation (conferences, task forces, cyber diplomacy, learning exchanges, dedicated websites)	2,4	6,7, 9, 10, 11, 12,13, 14,15, 16,17, 18,19, 22,25	27,30, 31	32,33, 34	35,37			52,53	56,58	63,66		79	81,82 83
20	Research and development (R&D) mechanisms mandated		7,9, 13,17, 18,22	27		37				57,58		71		
21	Security / privacy by design for products, systems and services is recommended		13,14		33	39				57		76		
22	Development of risk assessment mechanisms for increasing cybersecurity, including insurance risk assessment		22					43	46,48		63	76,77		
23	Publication of statistics, metrics and indicators mandated or		7,22,25 26				41	43				76	79	81,82

	recommended													
24	Ensuring technical interoperability of networks			27	34			45,49			65,66	78		
25	Utilize generic identity certificates (digital certification) for user authentication						41,42							
26	Promotion of e-governance									58	63,65			
27	Promotion of gender, youth and other diversity cyberspace workforce / engagement	26		27						58	65,66			

ANALYTICAL MATRIX REPRESENTING NORMS IN CYBER DIPLOMATIC INITIATIVES ACCORDING TO TYPE OF STAKEHOLDER

The norms most frequently incorporated, in descending order, are as follows:

*Please note that the number key for identifying matrix initiatives appears in Figure 1 above.

RANKING OF NORMATIVE ELEMENTS IN THE INITIATIVES ANALYZED		
KEY #	NORM	NUMBER OF INITIATIVES INCORPORATING THE NORM (OUT OF 84 TOTAL)
28.11	Human rights, civil rights, and/or individual rights should be respected in cyberspace	30
32	Norms relating to internet/cyberspace governance in general	28
36.1	Protection of personal and private data	25
37	Norms specifying international cooperation	26
28.1	UN Charter applies in cyberspace	18
31	Norms relating to critical infrastructure protection	17

28.2	International law applies in cyberspace	16
28.12	Endorsement of 2015 UNGGE norms	15
30.1	Prohibition of the use of cyberspace by non-State actors for terrorist and other criminal purposes (see also 2.2)	15
35.1	Responsibility to ensure the integrity of the ICT supply chain	15
36.3	Intellectual property protections	13
28.4	Other "international norms", "universally recognized norms" or "standards" apply in cyberspace (rather than "international law")	9
28.7	The principle of state sovereignty applies in cyberspace	8
28.3	"International rule of law" applies in cyberspace"	5
30.3	Terrorist content should be criminalized / removable	5
30.4	Child pornography or abuse online should be criminalized / removable	5
28.8	Self-defense / collective self-defense against other countries' use of force in cyberspace is permissible	5
29.2	State must not allow their territories to be used for wrongful acts in cyberspace	4
33	Protection of CERTs and other cyber emergency responders	4
36.2	Financial data protections when separate from 36.1)	4
34	Norms governing responsibility to report ICT vulnerabilities	3
35.2	Prevention of the proliferation of malicious ICT tools and techniques	3
28.10	Countermeasures are permissible	3
29.1	"Internationally wrongful acts" using ICT are forbidden in cyberspace	3
29.3	ICT should not be used for purposes that harm international security	3
30.2	Information should be prohibited that is inciteful or inflames hatred on ethnic, racial or religious grounds	3
28.9	Cyberattacks against critical infrastructure are be equivalent to aggression	1
28.5	The promotion of voluntary norms of responsible state behavior in cyberspace	1
28.7	Appropriate norms of state behavior in cyberspace within the international community need to be identified and promoted	1
29.4	Private sector companies should not be targeted	1

FULL ANALYTICAL MATRIX FOR NORMS

ANALYTICAL MATRIX COMPARING CYBER INITIATIVES: NORMS

A. INITIATIVES ► (KEY TO #'s BELOW) B. NORMS ▼		STATE-TO-STATE			UNILATERAL STATE ON INTN'L PLANE	INTERNATIONAL ORGANIZATIONS				INTERGOVERNMENTAL DECLARATIONS	NON-GOVERNMENTAL ORGANIZATION AND ACADEMIC INSTITUTIONS	INDUSTRY AND PRIVATE SECTOR	LAW ENFORCEMENT AGENCIES	OTHER
Normative elements agreed upon or proposed by state or non-state actors to address IPS of cyber-space ("the what")		MULTILATERAL	REGIONAL	BILATERAL		UN	SPECIALIZED AGENCIES	STANDARDS	OTHERS					
28	Applicability of international law norms to state and non-state actor activity in cyberspace													
28.1	UN Charter applies in cyber-space	1	12, 16	27	32	35,37	42		51,52, 53	55,56, 57, 59, 60	62	75		
28.2	International law applies in cyberspace		16, 22	27	33	35,37	42		51,52, 53	55,56, 57, 59, 60	62			
28.3	"International rule of law" applies in cyberspace"				32,34		42			55		70		
28.4	Other "international norms", "universally recognized norms" or "standards" apply in cyberspace (rather than "international law")	1, 2	12, 16		32,33, 34	35					62			
28.5	The promotion of voluntary norms of responsible state behavior in			27										

	cyberspace													
28.7	Appropriate norms of state behavior in cyberspace within the inter national community need to be identified and promoted			30										
28.7	The principle of state sovereignty applies in cyberspace		12, 23	29	32,33	35,37					62			
28.8	Self-defense / collective self-defense against other countries' use of force in cyberspace is permissible		16		34					56,57	62			
28.9	Cyberattacks against critical infrastructure are equivalent to aggression								50					
28.10	Countermeasures are permissible				33					56	62			
28.11	Human rights, civil rights, and/or individual rights should be respected in cyberspace	1, 3, 4,	14, 15, 16, 22	27	32,33, 34	35,36,37	40,42		51,52, 53	55,56, 57, 60	62,63, 65,66, 67	70, 71		
28.12	Endorsement of 2015 UNGGE norms *version unclear		10, 12, 17	27 * 30, 31	33	35			51	56,57, 59, 60		73, 75		
29	Explicit prohibitions derived from applicability of international law norms to state and non-state actor activity in cyberspace													
29.1	"Internationally wrongful acts"	2			32						62			

	using ICT are forbidden in cyberspace													
29.2	State must not allow their territories to be used for wrongful acts in cyberspace					35, 37				56	62			
29.3	ICT should not be used for pur-poses that harm international security	1			32	35								
29.4	Private sector companies should not be targeted											73		
30	Norms relating to cybercrime and cyberterrorism													
30.1	Prohibition of the use of cyberspace by non-State actors for terrorist and other criminal purposes (see also 2.2)	1	21, 23		32,34	36, 37	42			55,56	62,67	71	79,80	
30.2	Information should be prohibited that is inciteful or inflames hatred on ethnic, racial or religious grounds	1, 3	21											
30.3	Terrorist content should be criminalized / removable	4	21, 23		34							71		
30.4	Child pornography and abuse online should be criminalized / removable		23							55	63	74	80	
31	Norms relating to critical infrastructure protection	1	6, 13, 21	27		35		43	50,52	56	62,67	73, 75, 76		82,83

32	Norms relating to internet/ cyberspace governance in general	1, 2	15	27	32,33, 34	35,3 7			52,53	54,55, 56, 57	64,65, 67	68, 71, 73, 74, 75, 78	70,79	82,8 3
33	Protection of CERTs and other cyber emergency responders			27		35				56		75		
34	Norms governing responsibility to report ICT vul- nerabilities		20					47				73		
35	Protection of the ICT supply chain													
35.1	Responsibility to ensure the integrity of the ICT supply chain	1	6,9	27	33,34	35,3 7		43,4 7		56		75,7 6, 77		81
35.2	Prevention of the proliferation of malicious ICT tools and techniques					35						73		81
36	Norms governing the protection of types of data													
36.1	Protection of personal and private data		8,1 3, 14, 19, 21, 22		32,33, 34	39		43,4 5, 46,4 7		56, 57, 59, 60	63,64, 66,67	70,7 1, 74		
36.2	Financial data protections (when separate from 36.1)		14							61		76,7 7		
36.3	Intellectual property protections	4	20	27, 30	32,33, 34			45,4 6		56,57, 59	63			
37	Norms specifying international cooperation	1, 2, 4, 5	9,1 0 15, 20, 22, 25	27	32,33, 34	35,3 7				55,56	62	73,7 4, 75	70,79	82,8 3

PROTECTING THE PUBLIC CORE OF THE INTERNET

Ms. Joanna Kulesza, *University of Lodz*

Mr. Rolf H. Weber, *University of Zürich*

MEMO №1

TABLE OF CONTENTS

INTRODUCTION

Internet governance, once a purely technical exercise, that later evolved to cover nearly all Internet-related activities, is now being perceived as one of many tools to enforce national policies and local laws. States reach out to operators providing core Internet services, expecting them to assist with issues of national security, crime prevention or anti-terrorist measures. This increasing trend shows a misconception of the way the network operates, putting at risk its fundamental end-to-end principle: design within the infrastructure of the network becomes subject to policy constraints that should be dealt with at the end nodes. If Internet infrastructures are to be tweaked and used for the purposes of national security, copyright protection, curtailing free speech according to local standards or surveilling local citizens, risks of damaging the global network as it is now known are caused. What has long been referred to as "cyberbalkanization" – the creation of numerous smaller networks, disconnected, reflective of local legal and cultural values –might lead to the end of global communications. This report aims to identify the risks posed to core Internet operations by the growing expectations from local governments and different groups of interest. The authors assess and develop the most appropriate means and venues that could address the growing need to secure Internet functions and stability of its core infrastructures. They look at existing venues for Internet governance related debates and international law mechanism to address the challenge of protecting the Internet's core.

METHODOLOGY

Based on the review of academic writing and public policies, the report answers the question on the fundamental properties constituting the "public core" of the Internet and on the best means to protect them. The study sets its findings against international law rules governing certain global goods, attempting to identify the most effective ways of protecting the network's core, derived from existing international law and practice. The authors argue that the recognized principles of international law, in particular those on 1) state responsibility, 2) due diligence and 3) international liability,[111] can be applied to cyberspace and its most fundamental subsets. They look at various existing venues where Internet governance related issues are being discussed and assess their relevance for addressing Internet's security challenges. Following the current trend in academic debates on Internet governance, they recognize the need for a versatile approach. Many international fora, such as the International Telecommunications Union (ITU), the Internet Governance Forum (IGF) or the Internet Corporation for Assigned Names and Numbers (ICANN) offer possibilities to address the security and stability issues relevant for Internet governance. The authors recommend coordination of the respective individual efforts, paving the way for an international customary compromise, possibly leading to a more tangible contractual framework.

The first section of the report briefly covers the phenomenon of Internet governance and describes its multistakeholder approach. The authors emphasize the fundamental role of three groups of stakeholders: states, business (including the technical community) and civil society in the process of Internet standard-setting and policy-making. Then they move on to discuss the notion of Internet's "public core". The authors link this need of protecting Internet's "critical resources" to the well known concepts of critical infrastructure protection and discuss the latest developments in relevant international policies. The following section discusses the way states and private parties deal with managing critical infrastructures and avoid threats. Drawing analogies to international law, the authors refer to e.g. environmental law and international trade law as proofs of the changing face of international law and policy making, pertinent also to Internet governance and cybersecurity. The current model of international law and policy making shifts from state-centered to more distributed and informal forms, just to point to environmental law or international trade specifics, strongly relying on private parties input. This is relevant also for international telecommunications and Internet governance, as discussed in more detail below. The authors recommend applying the lessons learned from other areas of law, in particular those dealing with the environment and global trade for Internet governance, with due concern for the necessary, accompanying political tension.

[111] Any summary of the pertaining academic debate on the interrelationship between "state responsibility" and "international liability" reaches far beyond the ambit of this report. For an excellent reiteration of the points of contention see: A. E. Boyle, Liability for Injurious Consequences of Acts. Not Prohibited By International Law: a Necessary Distinction?, 39 The International and Comparative Law Quarterly 1990, 1-26.

SECTION 1: INTERNET GOVERNANCE AND THE MULTISTAKEHOLDER APPROACH

1.1 TRADITIONAL CONCEPTS AND DEVELOPMENTS

Originally, "governing" the Internet referred to the performance of purely technical administration of online services and was done by academics. Yet as the commercial, social and political potential of the Internet grew, the term has become all-encompassing, covering:

> *34. (...) the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet. (Tunis Agenda 2005)*

Once "managing" the Internet found its way onto the international diplomatic agenda, it covered all issues relevant to the reliable and stable operation of the network:

> *29. The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organisations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism. (Tunis Agenda 2005)*

as well as the roles of various stakeholders:

> *35. We reaffirm that the management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international Organisations. In this respect it is recognised that:*
>
> *Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues;*
>
> *The private sector has had and should continue to have an important role in the development of the Internet, both in the technical and economic fields;*
>
> *Civil society has also played an important role on Internet matters, especially at community level, and should continue to play such a role;*
>
> *Intergovernmental Organisations have had and should continue to have a facilitating role in the coordination of Internet-related public policy issues;*
>
> *International Organisations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies. (Tunis Agenda 2005, emphasis added)*

This all-encompassing definition has been fundamental to the multistakeholder approach to Internet governance (also known as the multistakeholderism principle), representing the joint management of Internet resources by three groups: states, business and civil society "in their respective roles".[112] The last group – the civil society – seems most complex and with that the most challenging to define. The following paragraph refers to particular sub-groups within the Internet governance community:

> *36. We recognize the valuable contribution by the academic and technical communities within those stakeholder groups mentioned in paragraph 35 to the evolution, functioning and development of the Internet. (Tunis Agenda 2005, emphasis added)*

This comprehensive build-up of the IG community has been recognized by various international fora that include e.g. the Council of Europe (CoE). In their 2011 Declaration on Internet governance principles the CoE Committee of Ministers refers indirectly to "multi-stakeholder governance" of the network:

> *The development and implementation of Internet governance arrangements should ensure, in an open, transparent and accountable manner, the full participation of governments, the private sector, civil society, the technical community and users, taking into account their specific roles and responsibilities. (CoE 2011)*

Also the NETMundial initiative reiterated the principle of multistakeholderism at the very top of its list, defining it as:

> *the full participation of governments, the private sector, civil society, the technical community, academia and the users in their respective roles and responsibilities. (NETMundial principles 2014)*

Another noteworthy attempt at identifying the principles behind the multistakeholder governance model specific to Internet are the UNESCO Internet Universality R-O-A-M Principles, focused on a "human-Rights based, Open, Accessible Internet governed by Multi-stakeholder participation".[113] While focusing on Internet accessibility and reflective of UNESCO's work on measuring media freedom, the Principles also strongly reflect the multistakeholder nature of online governance.

The 10 years period after the WSIS summit (2005-2015) fostered debates on making the ambiguous notion of "Internet governance" more specific. In particular defining the "respective roles" of states, business and civil society proved challenging. Some authors emphasized the role of private actors in national and international policy making.[114] Others called for linking Internet governance with the framework of international human rights law, viewing the network as a global enabler for free speech, right to assembly and other human rights, following the path set by media law, relying on freedom of expression guarantees as the baseline of state commitment to the free flow of information online.[115]

---

[112] For a detailed discussion on multistakeholderism see: J. Kulesza, International Internet Law, Routledge 2012, 138-139; R. Radu, J. M. Chenou, R. H. Weber (eds.), The Evolution of Global Internet Governance: Principles and Policies in the Making, Springer Science & Business Media 2014, 79-141; R.H. Weber, Legal foundations of multistakeholder decision-making, 135 Zeitschrift für Schweizerisches Recht (2016), 247-267.

[113] UNESCO, Principles for governing the Internet, a comparative analysis, UNESCO Publishing 2016, available at: http://unesdoc.unesco.org/images/0023/002344/234435e.pdf.

[114] See e.g. L. A. Bygrave, Internet Governance by Contract, OUP 2015.

[115] R. Balleste, Internet Governance: Origins, Current Issues, and Future Possibilities, Rowman and Littlefield 2015.

Another group of discussants argued for a return to the initial, technical, narrow perception of the term,[116] and so e.g. Broeders relies on the evolving two-tier approach to the notion of Internet governance, when he argues:[117]

> *The first is governance of the Internet's infrastructure, i.e. the governance of the core infrastructure and protocols of the Internet. It is this public core that drives the Internet's development. The collective infrastructure takes precedence in this form of governance. The second form is governance using the Internet's infrastructure. In this case, the Internet becomes a tool in the battle to control online content and behaviour. The issues vary from protecting copyright and intellectual property to government censorship and surveillance of citizens. (Broeders 2015:10)*

1.2 NOTIONS OF "PUBLIC CORE" AND "GLOBAL GOOD"

The aforementioned distinction is fundamental to the concept of the "public core of the Internet" and the policy proposal to consider it a "global good", both discussed in that same paper and focal to this report.[118] It follows a current trend in cybersecurity debates, focused on redefining Internet governance to better reflect current policy needs and sees many authors offer novel approaches to the distribution of competence among stakeholders. Savage and McConnell recommend "simplifying Internet governance (IG) by partitioning it into issues that can be addressed by existing international agencies and those that cannot".[119] They suggest modifying the way international agencies dealing with Internet governance related issues operate so as to reflect the multistakeholder model specific to ICANN. The international forums to be considered as possibly addressing the issues relevant to addressing the Internet's core are: 1) International Telecommunications Union (ITU) – an intergovernmental organization within the ambit of the United Nations, which, despite having taken steps towards multistakeholderism, still lacks the recognition from civil society or business; 2) the Internet Governance Forum (IGF) – run under UN auspices for over a decade the IGF was never designed to actively attend to pertinent policy issues or serve as a platform for diplomatic negotiations, hence still enjoys little interest from states, perceived more as a talk shop formula for civil society; and 3) the Internet Corporation for Assigned Names and Numbers (ICANN), the current paradigm of multistakeholderism, yet, unlike the ITU, ill-suited for binding intergovernmental negotiations.

As the issue of telecommunication and information systems security rises on national and international policy agendas, more venues, traditionally used for international security debates, come into play. Among state-led actions targeting cybersecurity challenges one should note the North Atlantic Treaty Organization (NATO) - the most significant intergovernmental organization focusing on armed conflicts and international peace. In 2016NATO officially recognized cyberspace as the fifth warfare domain and confirmed that a cyberattack on any of its allies will be considered an act of

---

[116] D. Broeders, The public core of the Internet, AUP 2015; D. Broeders, Defining the protection of the 'Public core of the internet' as a national interest, 190 ORF Issue brief 2017; L. DeNardis, Protocol Politics. The Globalisation of Internet Governance, MIT Press 2009.

[117] For a comprehensive discussion on trends in Internet governance discourse see generally: R. Radu, J. M. Chenou, R. H. Weber (eds.), The Evolution of Global Internet Governance: Principles and Policies in the Making, Springer Science & Business Media 2014. For an analysis of different approaches to Internet governance see: D. Sylvan, Global Internet Governance: Governance without Governors, idem 23-37.

[118] For a comprehensive analysis of policies and trends in governance of global public goods see also: N. Kirsch, The Decay of Consent: International Law in an Age of Global Public Goods, 108 American Journal of International Law 2014, 1-40.

[119] J. E. Savage, B. McConnell, Exploring Multi-Stakeholder Internet Governance, EastWest Institute 2015, 2.

war.[120] Another outcome of NATO's cybersecurity focus was the Tallinn Manual (with its two editions thus far), offering a first every study of international law applicable to cyberspace.

The NATO model is purely governmental and in no way resembles the paradigmatic multistakeholder model of Internet governance. NATO's cybersecurity focus followed over a decade of state-lead efforts in the Internet governance domain, initiated with the ITU WSIS process and culminated in 2012 with the World Conference on International Telecommunications (WCIT-12) in Dubai. Both: NATO and ITU enjoy a strong US presence, which proved highly significant in the light of the "Snowden revelations". The 2013 disclosure of long-lasting US surveillance targeting global communications cast a shadow over White House international policies, raising serious concerns as to the trustworthiness of US leadership, also with regard to the Internet governance. As a counterbalance to US-led efforts in governing the global network, Brazil initiated the NetMundial Initiative (NMI), another intergovernmental forum debating Internet governance, cybersecurity and human rights.[121]

While Internet governance is eagerly discussed by governments, the current IG landscape was originally designed as the effect of bottom-up governance models, rooted strongly in the technical community, just to mention the Internet Society (ISOC) or the Internet Engineering Task Force (IETF) with its "Requests for Comments" (RfCs), community-developed common standards voluntarily followed by its members: Internet service providers or software developers. While "security by design" remains a common paradigm within both: ISOC and IETF,[122] there is no connection to be made between this extra-legal, community based rule-making approach and the hard norm setting model of e.g. NATO. Despite the efforts from ICANN, ISOC, and the IGF, the pertaining lack of effective exchange of information relevant to international cybersecurity holds crucial relevance for developing any successful international cybersecurity policies and must be addressed by any future model of global cybersecurity protection. There can be no effective cybersecurity policy developed solely at governmental level, without strong presence of the technical community and vigilant input from civil society. This is particularly relevant to a highly technical issue that is the protection of Internet's fundamental functions and resources, referred to as the Internet's core.

1.3 CRITICAL INTERNET INFRASTRUCTURE AND "PUBLIC CORE" OF THE INTERNET

The concept behind Internet's public core is a functional one – it aims to ensure an open and reliable Internet, free from third party influence, regardless of reasons or interests behind it. As Broeders argues:

> *In order to protect the Internet as a global public good there is a need to establish and disseminate an international standard stipulating that the Internet's public core – its main protocols and infrastructure, which are a global public good – must be safeguarded against intervention by governments. (Broeders; 2015:13)*

One of the few international attempts to directly address the issue of Internet's core at the policy level is CoE's 2009 report on "Internet governance and Critical Internet Resources".[123] It identified "Critical Internet Resources" (CIRs) that

---

[120] NATO Warsaw Security Summit Communique, para. 70-71, available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[121] For more details about the initiative see: http://netmundial.org/ .

[122] See e.g.: E. Rescorla, Guidelines for Writing RFC Text on Security Considerations, 3552 Request for Comments 2003 available at: https://tools.ietf.org/html/rfc3552.

[123] Council of Europe, Internet governance and critical internet resources a report prepared by the Council of Europe Secretariat Media and Information Society Division, Directorate General of Human Rights and Legal Affairs, Council of Europe 2009.

require particular care from the international community to ensure the free and reliable flow of information online. According to the CoE, CIRs include:

- *root servers;*
- *Domain Name System;*
- *Internet Protocol;*
- *Internet "backbone structures", including Internet Exchange Points (IXPs) (CoE 2009: 13-15).*

It emphasized also the need to secure universal broadband access and network neutrality and linked the need to protect CIRs with the existing critical resources dogmatic:

> *Internet is a critical resource. In order to make it sustainable, robust, secure and stable, it is necessary to protect it in the same way that other critical common resources are protected. (CoE 2009: 23)*

Another helpful guideline on identifying the Internet's core comes from ISOC, which in its 2005 Comments on the Chair's Internet Governance Paper identified "Infrastructure and management of critical Internet resources" among the "public policy issues relevant to Internet Governance".[124] It named IP addressing, DNS and the secure operation of RIRs as crucial elements of the Internet's ecosystem:

> *47. We seek to ensure [balanced] equitable access to IP addressing resources and commend the establishment and evolution of the Regional Internet Registry system that has responsibility for this important role. (...)*
>
> *48. We recognise the valuable role that ICANN and its supporting organizations have played in the management of the Domain Name Space.*

These two documents illustrate well the basis for existing compromise on the need to protect fundamental Internet functions reflected in national policies and community based technical standards.[125] While other elements might be considered crucial for the network's operation, as for late 2017 the consensus on critical Internet resources amounts to a short list and includes: 1) Internet backbone networks, 2) DNS servers, 3) Internet Exchange Points (IXPs) and 4) TLD related services (registries and registrars). While a progressive, open, catalogue of critical Internet resources is to be identified through dialogue and diplomacy, the international need for its legal and organizational protection is beyond doubt. These four resources are to be perceived as "Internet's public core", whose security and stability is indispensable for the reliable operation of the network.

One of the starting points for a discussion on protecting the Internet's core has been the political concept of "global public good". Although not perfectly aligned to the needs of Internet governance and the network's architecture, it deserves a closer look. A complementary concept of "critical infrastructures" and their protection will serve as another point of reference. The idea of "Internet's core" as a "global public good" can therefore be perceived as a derivative of two policy concepts:

- the ambiguous notion of "global public goods", generated by the era of globalization, derived from the economic writings of Paul Samuelson on "public goods". It refers to all 1) globally available goods that are 2) non-rivalrous (consumption does not influence the quantity available to others) and 3) non-excludable (their use cannot be

[124] Internet Society, Comments on the Chair's Internet Governance Paper, 2005, p. 4.

[125] For a thorough study on national documents and technical standards regarding cybersecurity and critical Internet resources see e.g.: D. Broeders 2017.

prevented). The examples of global public goods range from those referring to knowledge to the common heritage of mankind[126] and

- critical infrastructure protection as provided by existing national regimes and international cooperation programs, such as the European Programme for Critical Infrastructure Protection (EPCIP), securing networks fundamental to the daily operation of any modern day society, including but not limited to water and energy supply, public transport, health and emergency services.

This is not to imply that either of those concepts offers readymade solutions for protecting the public core of the Internet. It is rather to indicate the network of reference for further research, attempting to identify those areas of existing international relations, law and policy, which can be relevant for Internet governance at a time of increasing threats to national security and international peace. As the table below shows, each of the two approaches offers different benefits and originates in a different cognitive setting. While "(global) public goods" are a genuinely political notion to discuss shared values and commodities, lacking legal enforceability, they are rarely subject to international law debate, focused instead on shared spaces, common heritage or critical infrastructures.

Tab. 1. Comparison of relevant reference frameworks.

	NON-ENFORCEABLE POLICY CONCEPTS	ENFORCEABLE NORMS RECOGNIZED WITHIN INTERNATIONAL LAW (OF PEACE)
global public goods	x	
global commons (Ostrom's „common pool resource"; „imperfect public good")	x	
international spaces and shared resources		x
critical infrastructure protection		x

The following sections of this report look at critical infrastructure protection and other international law analogies, seeking to identify existing solutions that can be imported to the protection of Internet's critical infrastructures and their protection as a "global public good" in term of ongoing policy debates.

[126] The discussion on "globally public goods" reaches far beyond the scope of this study. For an introduction to the discussion on the issue see e.g.: I. Kaul, P. Conceição, K. Le Goulven, R. Mendoza (eds.), Providing Global Public Goods: Managing Globalization, Oxford 2002; N. Kirsch: The Decay of Consent: International Law in an Age of Global Public Goods, 108 American Journal of International Law 2014, 1-40.

SECTION 2: MANAGING CRITICAL INFRASTRUCTURES AND AVOIDING THREATS

The Tallinn Manual defines critical infrastructure (CI) as all systems and assets, physical and virtual, within a nation-state's jurisdiction that "are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety or the environment."[127] It also defines "cyber infrastructure" covering "communications, storage, and computing resources upon which computer systems operate".[128] This handbook based on NATO CCD COE sponsored research, designed as a non-binding, draft set of cyber norms at a time of war, stipulates in Rule 81:

> *Attacking, destroying, removing or rendering useless objects indispensable to the survival of the civilian population by means of cyber operations is prohibited. [Tallinn Manual 2013: 226]*

Referring to the law on armed conflict the experts behind the Tallinn Manual agreed that this provision covered "objects indispensable to the survival of the civilian population" that include: foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works. They clearly indicate that neither the Internet as such nor its infrastructure fall within the ambit of the existing customary law behind the proposed rule. They do note however:

> *Cyber infrastructure indispensable to the functioning of electrical generators, irrigation works and installations, drinking water installations and food production facilities could, depending on circumstances, qualify. (Tallinn Manual 2013: 227)*[129]

These observations are to be considered only with reference to a time of war, as per Art. 54(2) Additional Protocol I, since the first edition of the Tallinn Manual discussed international humanitarian law and its applicability to cyber conflicts, while observing that thus far possibly only the Stuxnet malware incident (2010) amounted to an "armed attack" in terms of international law, and that also not without controversy among the involved experts. With that in mind the discussion on an "armed attack" in cyberspace and its legal consequences remains beyond the ambit of this report, as for this study the legal qualification of critical Internet infrastructures at the time of war is of little significance. As already stated no cyber conflict has yet been considered an armed conflict as per international law. This is why rather than a reference to the law of war, one referring to the time of peace should be made.

At the time of peace, networks providing vital resources to national communities are managed as part of national civil defense programmes. One of the more recent examples of international cooperation on protecting critical infrastructure and computer networks is the EU Directive on Security of Network and Information Systems (NIS Directive), adopted by the European Parliament on 6 July 2016. It builds upon prior European cooperation framed

---

[127] M.N. Schmitt (ed.), TheTallinn Manual, CUP 2013, 258.

[128] Idem.

[129] For a detailed discussion on criteria allowing to recognize infrastructures as critical see the cited source: M.N. Schmitt (ed.) 2013, 227 ff.

within the 2008 Directive on European Critical Infrastructures (DirECI).[130] Annexed to the NIS Directive are non-exclusive lists of networks considered crucial to the security of the European Union. As the list below indicates, the EU recognizes "digital infrastructures" as part of critical infrastructures and implements uniform measures of protection to all categories named below:

1. Energy
    a. Electricity, including: 1) Electricity undertakings;[131] 2) Distribution system operators; 3) Transmission system operators
    b. Oil, including: 1) Operators of oil transmission pipelines; 2) Operators of oil production, refining and treatment facilities, storage and transmission
    c. Gas, including: 1) Supply undertakings; 2) Distribution system operators; 3) Transmission system operators; 4) Storage system operators; 5) LNG system operators; 6) Natural gas undertakings; 7) Operators of natural gas refining and treatment facilities
2. Transport
    a. Air transport, including: 1) Air carriers; 2) Airport managing bodies; 3) Traffic management control operators providing air traffic control (ATC) services
    b. Rail transport including: 1) Infrastructure managers; 2) Railway undertakings, including operators of service facilities
    c. Water transport including: 1) Inland, sea and coastal passenger and freight water transport companies; 2) Managing bodies of ports; 3) Operators of vessel traffic services
    d. Road transport including: 1) Road authorities; 2) Operators of Intelligent Transport Systems
3. Banking
    a. Credit institutions
    b. Financial market infrastructures including: 1) Operators of trading venues; 2) Central counterparties (CCPs)
4. Health sector
    a. Health care settings (including hospitals and private clinics)
    b. Healthcare providers
5. Drinking water supply and distribution, including suppliers and distributors of water intended for human consumption
6. Digital Infrastructure including: 1) IXPs; 2) DNS service providers; 3) TLD name registries.

The examples above indicate all kinds of infrastructure that should be considered crucial within the 480 million consumers EU market. All those systems are to share the same level of protection as required from their operators, including e.g. security due diligence measures and risk assessments. While other services or networks might be

[130] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[131] All terms are defined according to the relevant provisions of EU law, as specified in Annex II to the NIS Directive.

considered critical by different states or regions (just to mention the US including election infrastructures in its critical infrastructures list), the EU law serves as a relevant point of view for the discourse on international (as opposed to national) approaches to CI protection. This latest development in EU cybersecurity policy is interesting for two reasons. First, it lists "digital infrastructure" together with services well-recognized as parts of national critical infrastructures, such as water supply or transportation. It therefore represents a well deliberated policy decision by the EU states to use the existing resilience network, represented by e.g. the EPCIP, for key Internet resources: IXPs, DNS operators and TLD registries.

Interestingly, the EU debate on the NIS Directive was prolonged not only due to the controversy surrounding accounting for "digital infrastructures" as critical networks, but also because obligations similar to those imposed on critical infrastructure operators were to be applicable also to "digital services" offered within the "digital marketplace", to online search engines and all cloud computing services (NIS Directive, Annex III).[132] As the final EU policy decision confirms, the use of well-known legal methods and cooperation mechanisms for critical infrastructure protection with regard to the Internet backbone is well justified. This is so despite the fact that imposing obligatory cybersecurity audits and/or insurance on all e-commerce services operating within the EU, not just digital infrastructures operators, is bound to raise practical concerns, ones to be faced in 2018 at latest, as this is when the Directive comes into force. The way EU deals with this practical challenge to CI protection, including parts of what is to be considered the public core of the Internet, will offer a valuable lesson to other world regions and set a precedent for further international cooperation in the field.

Secondly, for the practical outcome of this study it is important to note that one of the world's biggest economies decided to take the critical infrastructure protection route for securing Internet's operation. The EU example is non-exhaustive and other states consider different CI sectors and approaches, but EU recognition of Internet's protocols and key services as a part of civilian critical infrastructure protection must be noted. Should the European example prove effective and other countries chose to follow it, this policy line cannot be disregarded in the discussion on the Internet's core as a "global public good" and effective means of protecting it. This is to imply that what has been defined above as "Internet's public core" can be easily referred to with the existing legal framework for critical infrastructure protection, adapted to the needs of the global network. While the national or regional lists for critical infrastructure differ, the tools and means for their protection remain similar and always include a high standard of professional due care on behalf of its operators. Those are to be considered when a framework for protecting the Internet's public core is discussed.

[132] For an overview see: R.H. Weber, E. Studer, Cybersecurity in the Internet of Things: Legal aspects, 32 Computer Law &Security Review 2016, 715, 723-726.

SECTION 3: LESSONS LEARNT FROM INTERNATIONAL LAW

International cooperation on critical infrastructure protection is not the only analogy to be drawn from existing legal frameworks. Also, for example, the concept of shared spaces, explored by all in a uniform, non-harmful way is not new to the international community, international relations and international law. Areas of international law that can be used for reference with regard to protecting the core of the Internet include:

- law of the sea
- air law
- space law
- diplomatic and consular law
- international human rights law
- international telecommunication law133
- environmental law
- law on international liability
- law of treaties
- international trade law
- antiterrorist laws and policies
- international sports law and policies
- Global Administrative Law (GAL)

While each of these legal regimes offers interesting insights that can be useful to Internet governance, the limited scope of this study encourages a concise and general conclusion, one derived from all those areas of international law and relations.[134] The Tallinn Manual 2.0 indicates that there are overarching international law principles relevant to all those specified regimes: 1) sovereignty, 2) jurisdiction, 3) state responsibility, and 4) due diligence. While the notion of 1) sovereignty and 2) the matrix of jurisdictional principles remains an unresolved challenge for Internet governance and critical infrastructures protection, subject to enhanced debate and still far from consensus, the two other principles of international law: 3) state responsibility and 4) due diligence can be easily applied to the biggest international open network and its key components – Internet's public core.

The law on state responsibility is perceived as a secondary regime, applicable to all other specified international law rules, imposing obligations upon states.[135] Once an international obligation of a state is breached – be it an obligation of conduct or one of result – the consequences provided for in the law of state responsibility entail.[136] The principle of due diligence implies state's duty to act with due care in following its obligation of conduct and preventing a violation of international law.[137] Indications of what is meant as "due care" in particular circumstances are to be derived from the law and practice within individual areas of international relations: environmental law, oil transportation, energy production etc. It is therefore only with reference to e.g. the law of the sea that a standard of due diligence for protecting maritime resources can be established.

---

[133] Those are discussed in more detail in the Tallinn Manual 2.0, M.N. Schmitt (ed), CUP 2017, 179-298.

[134] For a detailed study on the relevance of the international law duty of prevention reflected in all those regimes to the ongoing cybersecurity debates see: J. Kulesza, Due diligence in international law, BRILL 2016, 221-258.

[135] For a detailed discussion on state responsibility, international liability and due diligence see: J. Kulesza 2016.

[136] This is not to imply the law on state responsibility is unambiguous or a binding character of the 2001 ILC Articles on state responsibility for internationally wrongful acts. This phrasing refers to the general applicability of recognized customary norms on state responsibility for a acts prohibited by international law.

[137] See: J. Kulesza 2016.

Analogically, a due diligence standard for protecting Internet's public core could serve as a point of reference for state's responsibility for an omission resulting in transboundary harm, e.g. a malfunction in a foreign power plant caused by a cyberattack generated from that state's territory. Effectively, the existing community standards with regard to good business practice within each of the sectors named above as Internet's core (root zone operation, IXP operation, DNS and TLD management) could be referred to by both: the victim state in filing its claims and the adjudicating court as based on the international law principle of due diligence. Due diligence appears in all the regimes named above, and is also relevant, as argued by Heintschel von Heinegg,[138] for e.g. the law on neutrality in armed conflicts, which "is, in principle, applicable to cyberspace". He goes on to argue that:

> *(...) governments should closely cooperate in a continuing effort to arrive at an operable consensus that takes into consideration global interoperability, network stability, reliable access and cybersecurity due diligence. (Heintschel von Heinegg 2013: 34-35).*

Looking at individual regimes particular mechanisms for identifying necessary efforts to protect individual resources can be easily identified. They are usually the result of consensus on the object of protection, at times facilitated by specialized bodies (e.g. the International Maritime Organisation). Similar mechanism could be applied to cyberspace, its fundamental resources and procedures necessary to protect them.

Seeking similarities between Internet governance with regard to protecting the Internet's public core and other areas of international law, the need to identify a central arena for focused debates becomes apparent. Within the Internet governance landscape it is ICANN that is arguably the most representative forum for a multistakeholder debate, yet, as already discussed above, not only is it one of many venues for IG related debates, but, more significantly, as per its design it lacks the power to set internationally binding obligations, other than those imposed by its contracts upon contracted parties – operators of generic Top Level Domains (gTLDs)[139] and the five Regional Internet Registries (RIRs).[140]

By its design ICANN lacks the necessary international recognition to ensure an effective diplomatic dialogue and the following, binding international obligations. The role of the Governmental Advisory Committee (GAC), although increasing, remains advisory. ICANN's Root Server System Advisory Committee (RRSAC) and Security and Stability Advisory Committee (SSAC) together with its Security, Stability and Resiliency Framework (SSR), while offering a possible avenue to pursue the purpose of protecting the Internet's core, remain a primarily technology focused fora, with little involvement from governments and civil society. The recently formed GAC Public Safety Working Group lacks the needed multistakeholder representation, operating as a temporary, internal GAC structure for pursuing dialogue between governments, law enforcement and the technical community, with a strong representation from the United States governmental sector. While either of these venues might be modified to have an enhanced impact and offer a versatile platform for further discussion on protecting Internet's public core, their current position falls short of a truly representative and influential international forum.

If international legal methods are to be applied to secure the Internet's core, significant action on the part of states, more than on the part of other stakeholders, must be taken, as it is the states who are directly bound by international law and in the position to secure enforcement of agreed international principles and codes of conduct. The traditional

---

[138] W. Heintschel von Heinegg, Territorial Sovereignty and Neutrality in Cyberspace, 89 International Legal Studies 2013, 34-35.

[139] It's worth noting that country-code Top Level Domain registrars are under no contractual obligation with ICANN.

[140] Those include: AFRINIC for Africa, APNIC for Asia-Pacific, ARIN for North America, LACNIC for Latin America and the Caribbean and RIPE NCC for Europe.

international law approach is to operate on state level through international treaties and customs, entailing state duties that are to be later implemented against private actors through national laws and regulations. This traditional model of international law making per its design fails to directly address duties of private parties. Instead it is focused on the duties of states, both positive and negative, with the latter resulting in state responsibility for omissions in securing particular duties to be met by private parties, as is the case with environmental law or protection of aliens and diplomatic staff, required from states within their territories.

This well-recognized model of state responsibility for the negligence of its bodies (legislative, judicial or executive) can be applied to Internet's public core, obliging states to introduce particular duties vis-a-vis operators of individual services (DNS) or infrastructures (root zone). The discussion on the need for a relevant Internet treaty, precising these duties has been present in academic debates and political dialogues for decades, yet has thus far been futile due to lack of political incentives or the pertaining threats of political oversight over the network.[141]

2018 could be the year when the discussion on a cybersecurity framework convention becomes more tangible, with a contractual regime for cyberspace building upon the lessons of the failed negotiations within the UN Global Committee on Governmental Experts (UN GGE) and enhanced regional cooperation.[142] A strong influence for this debate was also the 2017 Microsoft president suggestion on a "digital Geneva Convention" – a formal treaty requiring states to refrain from military uses of cyberspace.[143] The strong criticism of this proposal coming from academic and policy circles, primarily in Europe and the US indicates that a time for any hard law on cyberpeace is not ripe, but the reoccurrence of the issue and the vibrant debate also indicates that the idea remains appealing.

Another possibility would be to offer a novel approach to traditional international treaty making by including particular private operators as signatories to a "cybersecurity framework convention". This would allow to apply the existing international law mechanisms of state responsibility vis-a-vis states as well as to codify the rules of international liability with regard to Internet's public core. Should ICANN and, optionally, the five RIRs enter an international cybersecurity treaty, they would obtain a framework of reference for designing contractual compliance with network operators (short of ccTLD registrars who, as noted above, are not ICANN contracted parties). It would be directly through contracts with private parties that ICANN and RIRs could demand a particular standard of care in securing the network's core services and infrastructures.[144] This would discard the need for harmonizing roughly two hundred national laws on securing Internet's public core, yet would require a novel, flexible approach to traditional international law-making.

The concept of Global Administrative Law (GAL), discussed below, might provide for a broader perspective on this issue.

---

[141] M. Mueller et al., The Internet and Global Governance: Principles and Norms for a New Regime, 13 Global Governance 2007, 237-252; J. Kulesza, Towards and Internet Framework Convention: the State of Play, in: N. Lavranos, R. Kok (eds), Hague Yearbook of International Law 2013, 84-115; B. Smith, A Digital Geneva Convention to protect cyberspace, 2017, available at: https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace.

[142] V. Radunovic, Towards a secure cyberspace via regional co-operation, Diplo Foundation 2017, available at: https://www.diplomacy.edu//sites/default/files/Diplo-Towards_a_secure_cyberspace-GGE.pdf.

[143] J. Leyden, Microsoft president says the world needs a digital Geneva Convention, The Register, Nov. 10th, 2017, available at: https://www.theregister.co.uk/2017/11/10/microsoft_president_calls_for_digital_geneva_convention/.

[144] The concept of ICANN contractual framework as a constitutional order for Internet governance has been discussed in: R. H. Weber, R. S. Gunnarson, A Constitutional Solution for Internet Governance, 18 Columbia Science and Technology Law Review 2012, 1-71.

SECTION 4: GOVERNING THE CORE VS THE MULTISTAKEHOLDER CHALLENGE

The academic discourse on various governance models[145] has put Internet governance into a broader context of GAL, drawing analogies to contracts, laws, regulations and principles within sports law, trade law or human rights law, reflecting the complex, comprehensive institutional settings.[146] Kingsbury, Kirsch and Stewart identified five types of global administration:

1. administration by formal international organizations;
2. administration based on collective action by transnational networks of cooperative arrangements between national regulatory officials;
3. distributed administration conducted by national regulators under treaty, network, or other cooperative regimes;
4. administration by hybrid intergovernmental–private arrangements;
5. administration by private institutions with regulatory functions.

They locate ICANN and its multistakeholder model of governance within the fourth category: the hybrid intergovernmental-private administration, next to e.g. the Codex Alimentarius Commission (CAC), which operates based on consensus and adopts standards on food safety. While their original observations echo the GAC enhancement process of 2002, they remain even more relevant for the internationalized ICANN oversight following the IANA functions transition in 2016. Its decisions, similarly to those within ICANN, are made with a significant participation of private actors, working together with state representatives. It produces standards that have a "quasi-mandatory effect" as per the SPS Agreement under WTO law. As the cited authors observe:

> *The involvement of state actors, subject to national and international public law constraints, alongside private actors who are not, and who may indeed have conflicting duties such as commercial confidentiality, threatens a very uneven and potentially disruptive set of controls. (Kingsbury, Krisch, Stewart 2005)*

The GAL concept remains disputed, with some academics arguing it is more of an idealistic attempt at categorizing certain factual cooperation models that an actual policy or regulation trend. It offers however some interesting insights

[145] For a recent overview see R.H. Weber, Elements of a Legal Framework for Cyberspace, 26 Swiss Review of International and European Law 2016, 195-215.

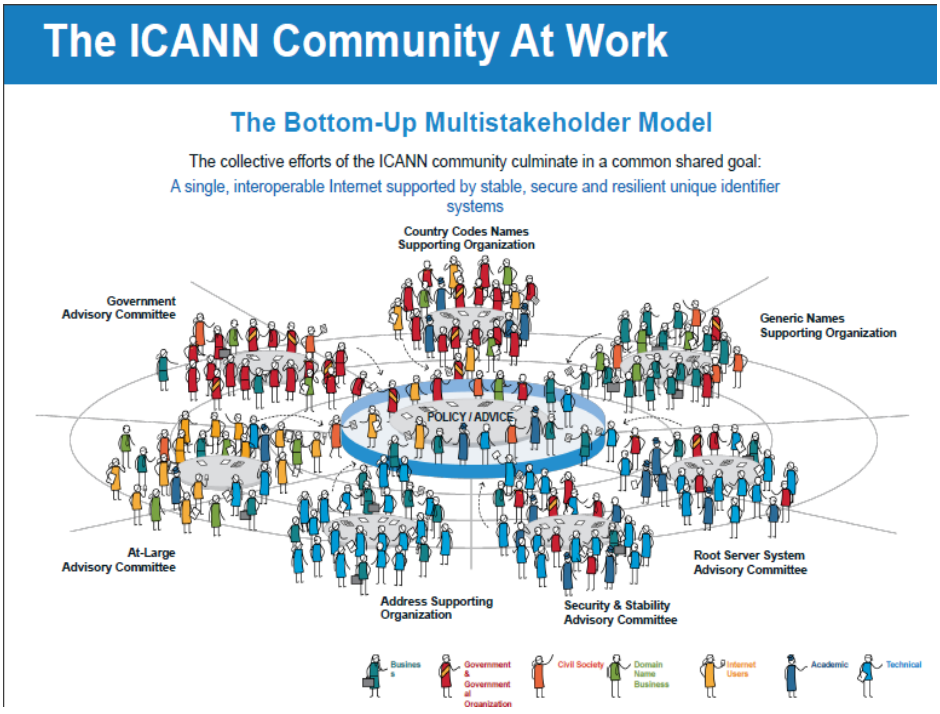
[146] B. Kingsbury, N Krisch, R.B. Stewart, The Emergence of Global Administrative Law, 17 New York University Public Law and Legal Theory Working Papers 2005, available at: http://lsr.nellco.org/nyu_plltwp/17. See also: R. B. Hall, T. J. Biersteker (eds), The Emergence Of Private Authority In Global Governance, CUP 2002.

into the Internet governance domain and options for administering the Internet's public core. Kirsch uses it as the background for a discussion on the changing models of governing "global public goods".[147] As he argues:

> *The dynamics of multilateral treaty-making, including the decline in recent decades, take a similar form across issue areas, whether these areas are dominated by club goods, like trade, or public goods, like the environment. (Kirsch 2014: 37)*

Also Broeders locates the need to protect Internet's universality, interoperability and accessibility within the category of "non-excludable" and "non-rivalrous", "global public goods" that "provide benefits to everyone in the world", to be attained only through targeted, public-private cooperation. While the shared use remains a valid argument, the two traits indicated as fundamental to the Internet as a global good – non-exclusion and non-rivalry – do not hold true.[148] These observations alone imply that the global public goods dogmatic applies only partially to Internet governance and administering the network's core (see Table 1above). This is not to imply, however, that international law has nothing to offer to solve this challenge – the link to club goods, administered within contractual international regimes like environmental law, may prove helpful.[149] As the case of environmental law, antiterrorist law or trade law and policies proves, administering a public resource can be done with the help of informal, polycentric regimes.

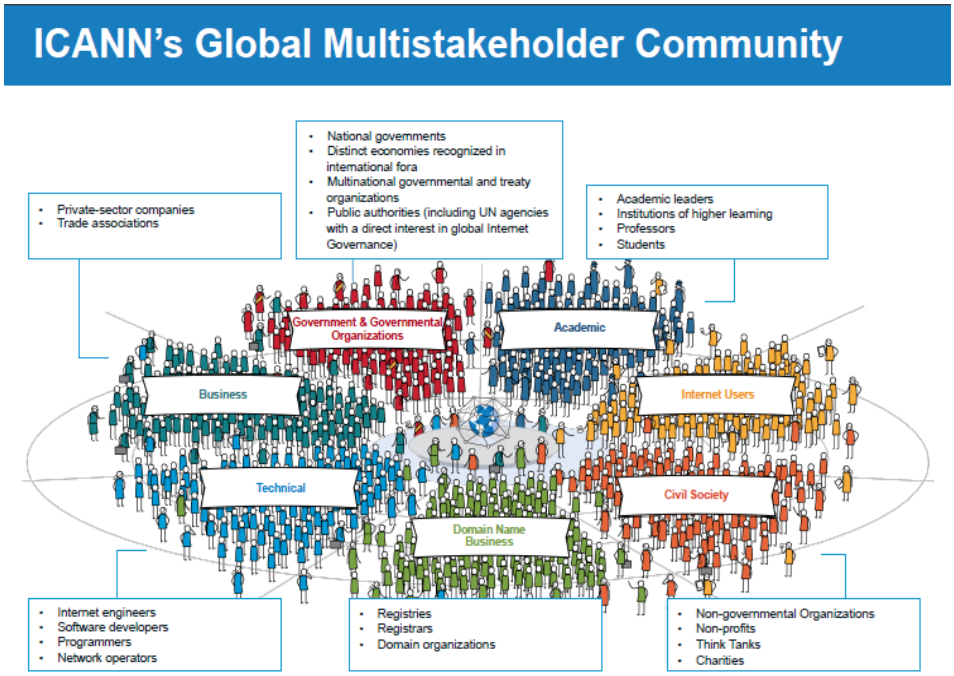
Thus far ICANN remains the contemporary paradigm multistakeholder governance model. The following graphics accurately depict its community and the way the "respective" roles of its members are performed:



[147] N. Kirsch, The Decay of Consent: International Law in an Age of Global Public Goods', 108 American Journal of International Law 2014, 1-40.

[148] D. Broeders 2015, 19-20.

[149] N. Kirsch 2015, 4.



Source: ICANN Engagement Update, Champika Wijayatunga, 2015.

The constitution and evolution of ICANN follows the policy trend of "presence and prominence of informal institutions and norms in global governance",[150] yet as discussed above it fails to address the needs of international law-making, one that could be used to implement effective protection of Internet's public core. The same observation applies however to all for a and organizations named in Section 1 of this report – none of them ideally meet the needs of multistakeholder Internet governance and effective international law-making. Below is their brief comparison:

Table 2 Comparison of fora debating various elements of protecting Internet's public core

ORGANIZATION/CHARACTERISTICS	ICANN	ITU	IGF	NMI	ISOC	IETF	NATO
multistakeholder	X		X	X			
bottom-up model of governance	X		X	X	X	X	
standard setting	X	X				X	
operates based on contractual compliance	X						
governmental		X		X			X
sets internationally enforceable obligations for states		X					X

[150] N. Kirsch 2015, 29.

In this context ICANN meets the needs of the dialogue on protecting the Internet's public core in many aspects, yet fails the most significant prerequisite – the power to introduce internationally enforceable norms or duties. That is rightfully so as the corporation was designed to avoid all political conflict. While "public interest" has been discussed within ICANN, in the context of "public interest commitments" in registrar accreditation agreements, any direct references thereto have been rejected by the community as a possible incentive for undesired governmental oversight.

Current Internet governance landscape fails to offer an ideal venue for discussing means of protecting Internet's public core. Contemporary debates on the issue are distributed among various fora, ranging from the dispersed ISOC community to the highly organized NATO. While there exists an international law framework to be referred to, one relying on state responsibility and due diligence, the precise reiteration of its applicability to Internet's key resources has not yet been addressed in a coordinated manner.

SECTION 5: RECOMMENDATIONS AND FORESIGHT – GOVERNING SHARED INTERNET RESOURCES

There seems to be little debate on the need to protect the stability and security of the Internet's "public core" seen as its protocols and standards. As explained above, the short list of Internet's core resources includes 1) Internet backbone networks, 2) DNS servers, 3) IXPs and 4) TLD related services (registries and registrars). Legal tools to govern Internet's public core can be derived from general international law, in particular the principles of due diligence and state responsibility. With reference to existing practice within other areas of international law, a cybersecurity due diligence standard can be identified based on good business practice, benchmarking and exchange of information. Other areas of international law allow to anticipate direct next steps in the evolution of this area of international relations. Those will likely include 1) cybersecurity audits for all critical Internet infrastructures operators, and 2) testing the preparedness of the organizations managing the infrastructure against best available practices.

Other areas of international law, in particular maritime oil transportation and nuclear energy production indicate the need to account for mandatory insurance of all such operators. It is therefore to be anticipated that similar obligations will be introduced also for critical Internet infrastructure operators. Uniform, universal standards of protection for all networks and services recognized as fundamental to the global networks' stable and reliable operation are to be identified through 1) international cooperation, 2) exchange of good practices, and 3) benchmarking. States must facilitate the creation and support the maintenance of international forum/fora for cybersecurity practice and experience exchange, either within existing specialized organizations (dealing with e.g. energy supply or air transportation) or within a separate, Internet-focused venue.

The multistakeholder model of Internet governance does not offer any leeway for the transposition of international obligations and norms on protecting the Internet's core onto national laws, regulations and sanctions for any protection of this global asset to be effective. This might prove the most challenging item on the agenda, as the experience of e.g. international environmental law has shown. While there is a broad international consensus on the need to protect the natural environment and a series of international agreements to detail this consensus, effective enforcement of environmental standards remains low. It is however likely that the Internet's multistakeholder model, as defined in the Tunis Agenda, with its unique distribution of power and authority will help to better enforce private obligations among various actors. As discussed in detail above, the international community can consider one of the two following scenarios:

1. traditional international law making through a treaty (e.g. a cybersecurity framework convention) effective against all signatories, necessitating its transposition onto national laws;
2. a novel approach to international law-making, inclusive of non-state actors, in particular open to ICANN and RIRs, who could use the conventional framework as a point of departure for their contractual compliance mechanisms, operating through good business practice and confidence building measures (CBMs).

From among the existing venues useful for enhancing the Internet stability and security debate, ICANN seems best equipped to fuel the discussion on technical standards for protecting the Internet's core. Yet by its very design it lacks effective tools to make any technical compromise internationally binding. With that in mind it can serve as a discussion platform, but not a diplomatic venue for advancing intergovernmental dialogue in its traditional sense. Contemporary international landscape lacks one venue where pertaining issues of protecting Internet's key resources can be discussed. It is therefore to be recommended for the existing venues to continue their work, aiming to ensure a coherent approach to cybersecurity. As has been the case with the law of the sea or, more recently, environmental law, the principles shared among those dispersed initiatives may serve as a foundation for a comprehensive customary framework, later to be transposed onto an international, contractual compromise, generated through common practice, benchmarking good practices and comprehensive confidence building measures.

BIBLIOGRAPHY

Balleste, R., Internet Governance: Origins, Current Issues, and Future Possibilities, Rowman and Littlefield 2015.

Boyle, A. E., Liability for Injurious Consequences of Acts. Not Prohibited By International Law: A. Necessary Distinction?, The International and Comparative Law Quarterly Vol. 39, No. 1 (Jan., 1990), pp. 1-26.

Broeders, D., Defining the protection of the 'Public core of the internet' as a national interest, ORF Issue brief 190, 2017;

Broeders, D., The public core of the Internet, AUP 2015;

Bygrave, L., A. Internet Governance by Contract, OUP 2015.

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Council of Europe, Internet governance and critical internet resources a report prepared by the Council of Europe Secretariat Media and Information Society Division Directorate General of Human Rights and Legal Affairs Council of Europe, April 2009.

DeNardis, L., Protocol Politics. The Globalisation of Internet Governance, MIT Press 2009.

Hall, R. B.,Biersteker, T. J. (eds) The Emergence Of Private Authority In Global Governance, CUP 2002.

Heintschel von Heinegg, W., Territorial Sovereignty and Neutrality in Cyberspace,, 89 International Legal Studies 123, 2013, 34-35.

Internet Society, Comments on the Chair's Internet Governance Paper, 2005, p. 4.

Kaul I., Conceição P., Le Goulven K., Mendoza R. (eds.), Providing Global Public Goods: Managing Globalization, Oxford 2002.

Kingsbury, B., Krisch, N. Stewart, R.B., The Emergence of Global Administrative Law, 17 New York University Public Law and Legal Theory Working Papers 2005, available at: http://lsr.nellco.org/nyu_plltwp/17.

Kirsch, N.,The Decay of Consent: International Law in an Age of Global Public Goods, 108 American Journal of International Law (2014), 1-40.

Kulesza, J., International Internet Law, Routledge 2012

Kulesza, J.,Towards and Internet Framework Convention: the State of Play, in: N. Lavranos, R. Kok (eds), Hague Yearbook of International Law 2013, 84-115;

Kulesza, J., Due diligence in international law, BRILL 2016.

Mueller M. et al., The Internet and Global Governance: Principles and Norms for a New Regime, 13 Global Governance 2007, 237 – 252;

NATO Warsaw Security Summit Communique, para. 70 – 71, available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

Radu, R. Chenou, J. M., Weber R. H. (eds.), The Evolution of Global Internet Governance: Principles and Policies in the Making, Springer Science & Business Media, 2014, 79-141.

Radunovic, V., Towards a secure cyberspace via regional co-operation, Diplo Foundation 2017, available at: https://www.diplomacy.edu//sites/default/files/Diplo-Towards_a_secure_cyberspace-GGE.pdf.

Rescorla, E., Guidelines for Writing RFC Text on Security Considerations, Request for Comments: 3552, 2003 available at: https://tools.ietf.org/html/rfc3552.

Savage, J. E., McConnell, B., Exploring Multi-Stakeholder Internet Governance, EastWest Institute 2015, 2.

Schmitt M.N. (ed.), Tallinn Manual 2.0, CUP 2017, 179-298.

Schmitt M.N. (ed.), The Tallinn Manual, CUP 2013, 258.

Smith, B., A Digital Geneva Convention to protect cyberspace, 2017, available at: https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace.

Weber, R.H., Legal foundations of multistakeholder decision-making, 135 Zeitschrift für Schweizerisches Recht (2016), 247-267.

Weber, R.H., Elements of a Legal Framework for Cyberspace, 26 Swiss Review of International and European Law (2016), 195-215.

Weber, R. H., Gunnarson, R. S., A Constitutional Solution for Internet Governance, 18 Columbia Science and Technology Law Review 2012, pp. 1-71.

Weber R.H., Studer E., Cybersecurity in the Internet of Things: Legal aspects, 32 Computer Law & Security Review (2016), 715, 715-728.

PROTECTING THE CORE

Mr. Oluwafemi Osho, *Federal University of Technology, Minna, Nigeria*

Dr. Joseph A. Ojeniyi, *Federal University of Technology, Minna, Nigeria*

Dr. Shafi'l M. Abdulhamid, *Federal University of Technology, Minna, Nigeria*

BRIEFING №3

TABLE OF CONTENTS

SUMMARY

The Internet is a global network consisting of autonomous and interconnected computer networks. At its core are backbone protocols and infrastructures. Over the years, the Internet has become target of inappropriate behaviors by both state and non-state actors. It has been increasingly subjected to significant threats and disruption. This briefing presents a summary of the most significant risks to the stability and security of the Internet, and the existing mechanisms to mitigate them. The methodology combines the use of extensive literature survey and perception of relevant communities that manage the core infrastructure of the Internet. It suggests that the loss or degradation of the core systems that provide basic Internet services is bound to have severe consequences on the functionality of the Internet. Consequently, it becomes pertinent that the core Internet infrastructures should be safeguarded against threats and interventions that exploit, undermine or target them.

SECTION 1: INTRODUCTION

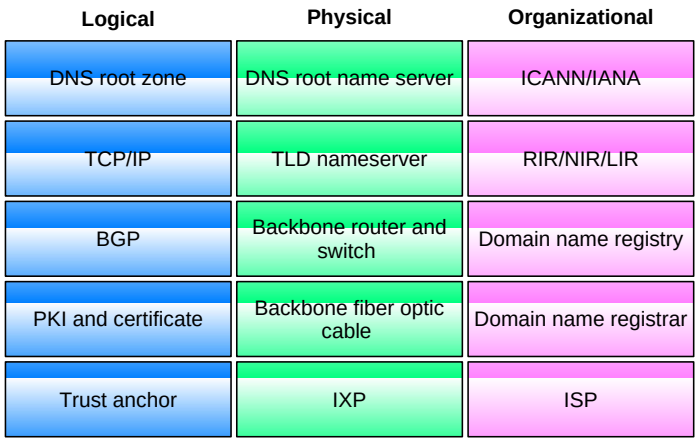
The Internet is a global network consisting of autonomous and interconnected computer networks. Over the years, significant evolution has been recorded in the technological, operations and management, social, and commercialization aspects of the Internet (Leiner et al. 2009). Essentially, it provides communication and information services (Maier and Wildberger 1994), supporting device to device, user to user, and user to device communication, and serving as a repository of information. Regular services provided by the Internet, under the two main categories, include, but not limited to, electronic mails, telnet, mailing list, chat, newsgroup, World Wide Web (WWW), file transfer protocol (FTP), and Gopher/WAIS/Archie/Veronica.

The success of the Internet, to a large extent, has been due to the trust its users have placed on its availability, consistency, and integrity. At the root of this trust are core values of accessibility, universality, operational stability, reliability, security, resiliency, and global interoperability expected by users (ICANN 2014b; Broeders 2015a; Internet Society 2017a).

1.1 THE CORE OF THE INTERNET

At the core of the Internet are protocols and infrastructures. These are consisted in systems that make up the logical, physical, and organizational infrastructure, which provide core naming and forwarding functions (Broeders 2017), ensuring the functionality and integrity of the Internet. These key protocols and infrastructures include (as shown in Figure 1), among other things, DNS root zone; DNS root server; TLD name servers; communication protocols: TCP/IP; routing protocols (e.g. BGP); PKI and certificates; routing facilities: core routers and switches, backbone fiber cables, Communication satellite; service providers: ISPs, IXPs; Internet administration/maintenance: ICANN/IANA; Internet registration: RIRs, domain name registry and registrars; and Internet standards developer: IETF (Hall 2000; Lévy-Bencheton et al. 2015; Bush et al. 2010; US GAO 2006; Internet Society 2017b; Biddle 2012).

Figure 1. Some Internet core protocols and infrastructure



However, over the years, the Internet has become target of inappropriate behaviors by both state and non-state actors. Its stability and security are continually subjected to significant threats and disruptions. In the past, Internet governance used to be the business of the technical community. Today, however, states are getting much more involved. Governance of the Internet has become more of governance using the Internet (Broeders 2015a).

1.2 RESEARCH OBJECTIVES

This research aims to present a summary of the most significant risks of global Internet disruption to the stability and security of the Internet and the corresponding mitigation measures. To achieve this aim, the specific objectives are to:

i. Present a formal definition and taxonomy of disruption of Internet services.

ii. Present significant risks to the core of the Internet.

iii. Present existing techniques and recommended good practices for mitigating the risks.

iv. Propose recommendations to enhance stability and security of the Internet.

1.3 RESEARCH STRUCTURE

The rest of the brief is organized as follows: chapter two focuses on defining and categorizing disruption to regular Internet services. The most significant risks to the core of the Internet are presented in chapter three. Chapter four discusses the risk mitigation mechanisms. Some recommendations towards enhancing stability and security of the Internet are presented in chapter five. The research concludes highlighting the implications of the foregoing on the definition of the public core of the Internet.

1.4 RESEARCH METHODOLOGY

This brief combines the use of extensive literature survey and perception of relevant community that manages the core infrastructure of the Internet. The research items were collated from relevant reports and literatures. The views of the expert were captured via email survey. Specifically, different questions sought their opinions on definition of disruption of Internet services; different threats, their respective level of impact and likelihood of occurrence; and level of effectiveness of existing risk mitigation techniques and recommended good practices. However, due to high variability in the perception of the experts on the aspects of threats and mitigation, only their views on Internet service disruption definition were considered.

SECTION 2: DISRUPTION OF INTERNET SERVICES

This chapter defines the concept of Internet disruption and identifies different forms of disruption – both conventional and non-conventional. To formulate a definition for Internet services disruption, survey respondents were asked, via an open-ended question, to define the term "significant disruption of regular Internet services" on a national or regional scale. From the responses, most frequently occurring terms were identified. These formed the basis of the proposed definition.

2.1 DEFINITION OF DISRUPTION OF REGULAR INTERNET SERVICES

Disruption of the Internet, at the very least, impinges on its capacity to provide needed services. However, its scope (in terms of users affected), scale (magnitude of effect), and period (amount of time) must be significant.

From the foregoing, the following definition of Internet disruption is proposed:

> A security breach that affects significant number of users, over a significant amount of time, causing significant impediment, interruption or retardation of access to, free flow of information through, or services provided by, the Internet.

2.2 TAXONOMY OF INTERNET DISRUPTION

The Internet was designed as a decentralized system, with its contents unregulated, and access to it unmonitored (Amichai-Hamburger 2013). By nature it is meant to be open, distributed and interconnected (Maurer et al. 2014). These properties are essential for the Internet to continuously guarantee the confidentiality, integrity, and availability of users' information, and consequently maintain its indispensability in the foreseeable future. Therefore, any behavior or activity that negatively impacts these characteristics can be categorized as disruptive to the Internet.

One potential impact of Internet disruption is countermining the functionality and integrity of the Internet (Broeders 2015a). Some of the consequences are reduced users' confidence in the Internet and Internet usage. Reports have shown that existing users already are increasingly becoming concerned about their privacy and security (Kende 2016).

Broadly speaking, regular Internet services can be disrupted by either undermining/exploiting or attacking core Internet protocols and infrastructures. As a result of these, different forms of disruption can be identified, viz. national or sub-national (mobile) Internet shutdown (West 2016), national or sub-national Internet censorship/filtering, throttling (Deloitte 2016; Aydin 2016), and Internet balkanization (Kumar 2001; Van Alstyne and Brynjolfsson 1996; Flew 2017; Maurer et al. 2014; Chander and Le 2014; Chander and Le 2015). Each of these disruptions requires different techniques, activities or behaviors to undermine, exploit or attack core Internet protocols and/or infrastructures. Figure 2 presents identified types of Internet service disruption, with the corresponding mechanisms used.

Table 1 highlights the different types of Internet service disruption, technique employed, what is disrupted, who disrupts, and the incentives and disincentives for disrupting these services

Figure 2. A taxonomy of Internet services disruption

(MOBILE) INTERNET SHUTDOWN

This involves the temporary shutting down of the entire Internet or mobile Internet, and may cover the entire or certain regions of a country. A typical example is the shutting down by the Egyptian government, in 2011, of the entire Internet for a period of 5 days, to stifle protest (West 2016).

Techniques used by state actors include shutting down telecommunication infrastructures or BGP session, powering down core devices, or changing the routing tables ("digital kill") (Wolchover 2011; Decraene et al. 2011; Van Beijnum 2011). These would normally target core devices like routers, switches, and telecommunication infrastructures. Non-state actors, on their own part, target fiber cables, and employ DDoS and other cyber attacks against the core devices (Sigholm 2013).

Apart from separating Internet users from their online acquaintances, Internet shutdowns negatively impact economic activities (West 2016). The economic impact has been estimated at an average of $23.6 million per 10 million population for a highly Internet-connected country (Deloitte 2016).

INTERNET CENSORSHIP/FILTERING

Internet censorship simply implies the control or stifling of contents on the Internet. This behavior is commonly employed by authoritarian governments, who enlist the service of service providers, to control the information accessible on the Internet (Leberknight et al. 2010; Broeders 2015b). The censorship could be applied nationally or limited to specific regions. Core Internet assets targeted includes gateway, domain name and web servers, and core routers.

To censor the Internet, techniques commonly employed are DNS tampering, HTTP proxy filtering, IP blocking/filtering, keyword filtering, URL filtering (Terman 2012; Faris and Villeneuve 2008; Leberknight et al. 2010; Dutton et al. 2011); DDoS, web defacement, and other cyberattacks against websites and contents (Noman 2011; Colarik and Ball 2016; Schmidt and Cohen 2014). A case study of the use of DDoS to enforce censorship is the use of 'the Great Canon' by government of China (Essers 2015).

THROTTLING

Throttling can be described as disruptions implemented through reductions in speed of the entire or specific services of the Internet. This significantly elongates the average time it takes a user to access a resource on the Internet. In some cases, certain services on the Internet may be rendered unusable once the speed is reduced below a particular level (Deloitte 2016).

Regrettably, this form of disruption is increasingly gaining preference, due to its less detectability, among state actors who try to limit free flow of information (Kelley 2017). In 2017, to curtail the spread of rumours, the Indian government requested Telecom companies to downgrade 3G and 4G services to 2G speeds (Shashidhar 2017).

Slowing down of the Internet can be implemented on core routers and servers, and other broadband infrastructure by regulating the rate of flow of packet to a certain quality level. This technique is known as traffic (or packet) shaping. It exists in the form of bandwidth throttling and rate limiting, depending on whether the regulation affect data transfer in or out of the network (TechTarget Network 2010).

INTERNET FRAGMENTATION

Internet fragmentation, also referred to as Internet balkanization (Maurer and Morgus 2014; Ma et al. 2010) or splintering the Internet (The Economist 2010), is the creation of "parallel Internets that would be run as distinct, private, and autonomous universes." (Kumar 2001). Three forms of fragmentation have been proposed: technical, governmental, and commercial fragmentation (Drake, Cerf, and Kleinwachter 2016). This brief focuses on the governmental fragmentation, which essentially centers on Internet border controls established to keep data in (Chander and Le 2014). To actualize this, different recommendations have been tabled, viz. creation of national email, localization of data storage and routing, and construction of new undersea cables (Maurer et al. 2014).

Fragmenting the Internet, for instance towards Internet/data nationalism, could require interfering with routing protocols (Broeders 2015b). This distorts the Internet's architecture. Localized e-mail and data storage and routing, among other things, impose geographical boundaries on traffic. This undermines the open and interconnected structure of the Internet (Maurer et al. 2014).

INCENTIVES/DISINCENTIVES FOR DISRUPTING

A close observation of the different case scenarios of disruption of Internet services reveals that authoritarian and repressive state actors disrupt mostly by undermining or exploiting core Internet protocols and infrastructures. On the other, non-state entities, perhaps due to lack of direct access to or control over those core infrastructures, primarily disrupt using attacking against the infrastructures.

Both state and non-state actors have their respective reasons for disrupting the Internet. The incentives and disincentives for state actors to disrupt the Internet fall broadly under three categories: politics and power, social norms and morals, and security concerns. Thus, it is not uncommon to find governments citing national security, prevention of election fraud, false information during elections or examination cheating, maintenance of public order, preservation of social norms and morals, economic interests, or copyright protection in order to shut down, censor or throttle the Internet (Aydin 2016; Broeders 2015a; West 2016; Faris and Villeneuve 2008). For repressive governments, Internet censorship is another veritable instrument for political oppression and suppression (Schmidt and Cohen 2014).

In the case of Internet fragmentation, the incentives are similar. Apart from national security, others are technological sovereignty, protection against foreign surveillance, and of privacy and data (Maurer et al. 2014; Drake, Cerf, and Kleinwachter 2016).

On the other hand, for non-state actors, their motives differ. Attacking Internet infrastructure, websites, or contents are motivated by economic/financial gain, revenge, grievance, sabotage, need for political or social change, propagation of propaganda, or patriotism (Sigholm 2013).

2.3 OTHER INTERNET "MISUSE" THAT DISRUPT

There are other activities that constitute a covert disruption of Internet services. They comprise of Internet abuse or misuse. In essence, these equally erode users' trust and affect how they use the Internet.

One of these is Internet surveillance. It requires exploiting core Internet protocols (Broeders 2015b) and infrastructure. Techniques used include bulk collection, illegal wiretapping, and packet sniffing. While it does not directly impinge on accessibility, it countermines confidentiality and integrity of data. When Internet users become aware that their conversations are under surveillance by the government, their willingness to express themselves freely and socially interact online might be stifled.

Table 1. Disruption techniques and actors, disrupted assets, and motivations for disrupting Internet services

Type	Technique	Asset targeted	Actor	Incentive/ Disincentive
National or sub-national (mobile) Internet shutdown	Shutting down mobile telecommunication infrastructure	telecommunication infrastructure	Governments, ISPs	National security, election fraud, false information during elections, public order, examination cheating prevention
	"Turning off," e.g. powering down or unplugging interconnection infrastructures or network disconnection	Servers, core routers, network switches		
	"Digital kill," e.g. changing routing tables	Core routers		
	BGP session shutdown	BGP peering links, border router		
	Disruption of fiber cables	Undersea and land cables	Terrorists	Propaganda, protest, revenge, sabotage, political or social change, patriotism, economic/financial gain, grievance
	DDoS or other cyber attacks against the infrastructure of the Internet	Servers, core routers	Hackers, hacktivists, cyber terrorists	

Type	Technique	Asset targeted	Actor	Incentive/ Disincentive
National or sub-national Internet censorship/filtering	IP blocking/filtering	Domain name, web servers, and core routers	▪ Government, ISPs ▪ Hackers, hacktivists, cyber terrorists	▪ National security, social norms and morals, economic interests, copyright protection, political oppression and suppression. ▪ Propaganda, protest, revenge, sabotage, political or social change, patriotism, economic/financial gain, grievance
	DNS tampering/poisoning and hijacking			
	HTTP proxy filtering			
	URL filtering			
	Automatic connection reset			
	Keyword filtering			
	Portal censorship			
	Port number blacklisting			
	DDoS or other cyber attacks against specific sites or contents			
Throttling	Traffic (or packet) shaping: bandwidth throttling and rate limiting	Core routers, servers, broadband infrastructure	Governments, ISPs	National security
Internet fragmentation	National e-mail	Servers, core routers, fiber cables	Governments, ISPs	National security, Technological sovereignty, foreign surveillance prevention, privacy and data protection
	Localization of data storage and routing			
	undersea cables			

SECTION 3: RISKS TO THE STABILITY AND SECURITY OF THE INTERNET

Extending the ICANN's security, stability and resiliency (SSR) framework definition (ICANN 2013) to the entire Internet, stability can be said to be the capacity of the Internet to function as expected. This implies constancy in its character (performance). Security of the Internet, on the other hand, entails protection of the Internet against attacks and misuse. This guarantees confidentiality, integrity, and availability of users' information.

This chapter presents threats to the core Internet infrastructure that negatively impact the stability and security of the Internet. It also identifies systems whose loss or degradation is likely to have severe impact on the Internet.

To identify the threats, relevant published materials were collated. The threats are sectionalized under different categories, viz. deliberate shutdowns; censorship; fragmentation; DNS threats; routing threats; certificate threats; physical attack/disaster; and error, malfunction, and compromise.

3.1 RISK MODEL

According to ISO/IEC 27005 (ISO 2011), information security risk is defined as:

"Potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization."

Table 2 contains different threats to the Internet core, the asset targeted and real-life incidences (Lévy-Bencheton et al. 2015; ICANN 2014a; Piscitello 2016; Turner, Polk, and Barker 2012).

In addition to popular threat, new threats are emerging. An example is the BGP MITM attack. Even though its possibility has been demonstrated since 2009 (Hepner and Zmijewski 2009), it was not until 2013 that these attacks were actually discovered (Alaettinoglu 2015). Another emerging threat is domain shadowing (Team RiskIQ 2016; ICANN 2016). Criminals use stolen or phished registrant's credentials and create large number of unauthorized subdomains, which are used for malicious activities.

3.2 "SINGLE POINT OF FAILURE"

The ISO guide (ISO 2011) described risk as "often characterized by reference to potential events and consequences, or a combination of these." One of the potential events with Internet infrastructure is their loss (which may be due to theft or attack) or degradation. This potentially could constitute a single point of failure.

A single point of failure (SPOF) is a component of a system which, if it fails, causes the entire system to stop functioning (Dooley 2009). To categorize a core Internet infrastructure as, potentially, a single point of failure, if lost or degraded, different perspectives could be considered. One perspective is to assess the criticality of such system to the stable and secure functioning of the Internet. It considers the questions: Can the Internet cope without the system? Are there alternative systems that perform the same functions? If a system is one alternative among systems that perform a

particular function or set of functions, the loss or degradation of that system cannot be expected to cause as much damage to the Internet as when such function or set of functions are performed solely by a single system.

If this yardstick is used, the loss or degradation of any of the infrastructures used to provide or support basic Internet communication and information services could, in theory, constitute a single point of failure. These include the DNS root zone, DNS root name server, TCP/IP, BGP, TLD nameservers, backbone routers, and the companies (as a whole) that manage core infrastructures of the Internet. If the DNS fails, there would be no way to find IP address. Consequently, Internet services become inaccessible (Cooper 2016). In the same vein, "killing" the BGP renders impossible routing of information. And needless to say, destruction of the entire organizations that manage those core infrastructures would inevitably lead to the destruction of the infrastructures too.

The other perspective considers the likelihood of loss or degradation of a system – the effort, cost or time required to cause the loss or degradation – in determining whether a system could be categorized as a single point of failure. Going by this perspective, it will be tempting to conclude that it is near impossible to have any single point of failure. This is due to the existing resiliency level of the Internet. However, considering the increasing acquisition and proliferation of cyberweapons, especially by state actors (Dévai 2016; Hughes and Colarik 2016), the possibility of successfully bringing down a core system, regardless of its level of resiliency, might not be as remote as it is currently believed. Evidences attest to this possibility. Already, some actors (most probably state actors) seem to be mooting the idea of taking down the entire Internet (Paganini 2016; Schneier 2016). Schneier reported about calibrated attacks targeted against organizations that manage core infrastructures of the Internet. The attacks were aimed at determining the limit of their defenses. Another evidence: a group of researchers introduced a DDoS attack, termed Coordinated Cross Plane Session Termination (CXPST), capable of targeting all core routers on the Internet (Schuchard et al. 2010; Mohan 2011).

Table 2. Threat categories, types, assets targeted and real-life scenarios

Threat Category	Threat	Asset Targeted	Case Study
Deliberate shutdowns	Shutting down mobile telecommunication infrastructure	Telecommunication infrastructure	There were more than 50 Internet shutdowns in 2016 alone (Kamen 2017).
	"Turning off," e.g. powering down or unplugging interconnection infrastructures or network disconnection	Servers, core routers, network switches	
	"Digital kill," e.g. changing routing tables	Core routers	
	BGP session shutdown	BGP peering links, border router	
Censorship	IP blocking/filtering	Domain name and web servers, core routers	Iran is ranked 1st in terms of Internet censorship. In China, using a 4-level filtering process, government block more than 1 to 4 sites accessible via search engines (Gaille 2017).
	HTTP proxy filtering		
	URL filtering		
	Automatic connection reset		
	Keyword filtering		
	Portal censorship		
	Port number blacklisting		
	Traffic (or packet) shaping: bandwidth throttling and rate limiting	Core routers, servers, broadband infrastructure	Iran in 2009 (Anderson 2013) and 2013 (Aryan, Aryan, and Halderman 2013).
Fragmentation	National e-mail	Servers, core routers, fiber cables	Iran launched its own Youtube; Turkey intends to build a domestic search engine and email service (Clark et al. 2017).
	Localization of data storage and routing		

Threat Category	Threat	Asset Targeted	Case Study
DNS threats	Brute-force attack	Root zone KSK	
	Substitution attack	Root zone KSK	
	Pre-image attack	Root zone KSK	
	Domain shadowing attack	Domain registrant credentials	Use of Angler Exploit Kit (Biasini 2015).
	DNS cache poisoning attack	DNS resolvers	Google Malaysian domain hit with DNS cache poisoning attack (Previous Contributors 2013)
	DNS hijacking attack	DNS server	Wikileaks site hacked via its DNS (Greenberg 2017).
	"Exploit to own" DoS attack	Name servers	Attacker could execute arbitrary code (Manion 2003).
	DDoS attack	Core servers	All 13 DNS root servers targeted (Roberts 2002)
	DNS amplification attack	Servers, end-user nodes	An attacker sends at least 20Gbps against an end-user's system 24 hours a day (Prince 2012).
	Malware	Core servers	Malware-based DDoS attack against Dyn servers (Woolf 2016)
	Domain registration hijacking attack	Registration account, Name servers	PANIX became a victim of domain hijacking (SSAC 2005).
	DNS response modification	DNS resolver	

Threat Category	Threat	Asset Targeted	Case Study
Routing Threats	BGP route leak	Autonomous systems	Misconfigured router caused Internet service degradation (Madory 2017)
	BGP (prefix) hijacking attack	Autonomous systems	Tens of prefixes originated from Rostelecom (Toonk 2017)
	BGP MITM attack	Autonomous systems	Traffic for major networks directed to an ISP in France (Toonk 2013)
Certificate threats	Impersonation	Certificates	
	Registration Authority compromise	Certificates	
	Certificate Authority system compromise	Certificates, Certificate revocation lists (CRLs)	DigiNotar CA breach (Hoogstraaten et al. 2012).
	CA Signing key compromise	CA signing key, certificates, CRLs	
Physical attack/disaster	Vandalism/theft/loss	Undersea and land cables and other core infrastructure	Fiber cables in California attacked (T. Hughes 2015)
	Natural/Environmental disaster	Core physical infrastructure	Under-sea cable damaged by powerful earthquakes off the coast of Taiwan (Lemon 2006).
Error, malfunction, compromise	Root/TLD operator errors	Root/TLD infrastructure	
	Hardware failure	Core physical infrastructure	
	Registration services failure/compromise	Services	
	Service provider failure/operation disruption	Hardware, software, services	

SECTION 4: MITIGATING RISKS TO THE STABILITY AND SECURITY OF THE INTERNET

This chapter focuses on highlighting some of the existing techniques and recommended best practices for mitigating risks to the core of the Internet.

A number of the threats to the Internet, often employed by authoritarian or repressive state actors, are not direct attacks. Core Internet infrastructure are exploited or undermined. These equally destabilize and undermine the security of the Internet. For these threats, there are no formal recommended good practices. However, Internet users have devised different informal methods of dealing with them. One of these threats is censorship. Tools commonly used to bypass censorship include Virtual Private Networks (VPNs), custom DNS servers, web-based proxies, Tor browser, and SSH tunnels (Hoffman 2016). In 2014, an Android-based app, DNSet, was used by Turkish citizens to bypass censorship during the first months. The application enabled users who did not have administrative rights on their devices to alter, without difficulty, the DNS server imposed by 3G/4G providers (Di Florio et al. 2014).

For threats like deliberate shutdown and Internet fragmentation, there are no technical countermeasures to mitigate them. new methods might be required to moderate them.

Some of the existing recommendations for mitigating threats that target core infrastructure are presented in Table 3 (Internet Society, n.d.; Lévy-Bencheton et al. 2015; Conrad 2016; IANA 2016; US-CERT 2013; Xu 2017; Manion 2003; SSAC 2005; SSAC 2008; Turner, Polk, and Barker 2012; Lewis 2017; Qamar 2014; Khanse 2015).

4.1 GAPS

Despite the array of techniques and mechanisms available to prevent and mitigate many of the threats to the core infrastructure of the Internet, there are issues that require attention. One of these is root zone KSK rollover. It was meant to take place on October 11, 2017, but had to be postponed. Some implementation and configuration bugs associated with RFC 5011, the mechanism which enables validators to automatically update their trust anchors, were discovered (Wessels 2017).

Another issue is the limitation of the DNSSEC. It essentially addresses the aspect of integrity. Other aspects of information security, including confidentiality of the information inside the DNS and availability needs to be addressed. Much efforts are still required to ensure the network layer of the infrastructure are protected (Marsan 2010).

Equally worthy of further attention are the emerging threats. While a number of mitigation mechanisms have already been proposed (Huston 2013; Oti, Bansah, and Adegboyega 2016), more research is needed to address issues that might arise during their implementation.

Table 3. Risk mitigation techniques and good practices

Threats	Mitigation Technique/Good Practices
DNS Threats	
Brute-force attack	Periodic changing of the root zone-signing cryptographic keys.
Substitution attack	Distribute the public component of a Trust Anchor in a secure fashion.
Pre-image attack	Implement a sufficiently resistant cryptographic hash function in conjunction with the signing algorithm during the time in which the signature is valid.
Domain shadowing attack	Check IP addresses against a reputation-based blacklist if it resolves to multiple names or IP addresses.
	Adopt heuristic behavioral analysis to identify potentially malicious network connections requiring further inverstigation.
DNS cache poisoning attack	Adopt DNS open resolver configuration.
	Deploy DNSSEC for securing DNS clients origin authentication of DNS data, authenticated denial of existence and data integrity.
	Utilize developed patches commonly adopted against Kaminsky Cache Poisoning.
	Restrict zone transfers to reduce load on systems and network.
DNS hijacking attack	Apply DNSSEC.
	Use good security software capable of preventing DNS-Changing malware.
"Exploit to own" DoS attack	Upgrade or apply vendor-specified patch.
	Restart dynamically linked processes and recompile statistically linked libraries.

Threats	Mitigation Technique/Good Practices
DDoS attack	Apply BCP38 to mitigate DDoS attacks via IP Source Address Spoofing.
	Adopt source IP address verification at the edge of Internet infrastructure.
	Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure
	Disable open recursion on name servers and only accept DNS queries from trusted sources.
	Manufacturers and configurators of network equipment should take steps to secure all devices, e.g. keep them up-to-date by patching flaws.
DNS amplification attack	ISP should reject any DNS traffic with spoofed addresses.
	Disable recursion on authoritative name servers.
	Restrict recursion to only authorized clients.
Malware	Use strong anti-malware software and also update your system and software periodically.
Domain registration hijacking attack	Registries should implement Registrar-Lock and EPP authInfo according to specification.
	Resellers and registrants should be provided with Best Common Practices by registries and registrars that describe appropriate use and assignment of EPP authInfo codes and risks of misuse.
	An emergency action channel should be provided by registrars.
DNS response modification	Inquiry should be made by registrants about the treatment of their unregistered subdomains by entrusted agents.
	Organization for which accurate NXDomain reporting is essential for operational stability should opt for entrusted agents that guarantee non-modification of DNS responses in its terms of service.
Routing Threats	
BGP route leak	Announce routes more preferable than leaked route to counter illegitimate routes.

Threats	Mitigation Technique/Good Practices
BGP route leak	Entirely change prefix via modifying DNS records.
	Route Origin Authorizations (ROAs) should be published in the various RIRs.
BGP (prefix) hijacking attack	Apply cryptographic resource certification (RPKI) for the purpose of AS origin validation.
	Establish an Appropriate Use Policy (AUP) to promote rules to secure peering.
	Utilize resource information from databases such as IRR, APNIC, ARIN, and RIPE.
	Utilize prefix filtering and automation of prefix filters.
	Utilize prefix filters to facilitate validation of routing information on global scale.
	Utilize third-party BGP prefix hijacking detection service from which you receive notifications (please, note that this mitigation is under debate).
BGP MITM attack	Periodic changing of the cryptographic keys used to sign the root zone.
Certificate Threats	
Impersonation	RAs must ensure adoption of best practices for vetting certificate requests as documented in the certificate policies (CPs) associated with the CAs served by the RA.
RA compromise	RAs must implement security best practices.
CA system compromise	CAs must perform regular third-party audits and reviews.
	CAs must implement mechanisms for tracking and detection and perform regular manual operational sanity checks.
	CAs must revoke issued fraudulent certificates, when detected, and inform victim organizations and all potential relying parties.
CA signing key compromise	In the event of a signing key theft, CAs must revoke all certificates issued by the compromised CA and all necessary parties notified that they would require new certificates.

SECTION 5: ENHANCING THE STABILITY AND SECURITY OF THE INTERNET

Previous chapters have discussed essentially various risks to the stability and security of the Internet and some of the existing strategies to mitigate them. The capacity of the Internet to sustain its underlying values of universality, interoperability, and accessibility is firmly hinged on continuous guarantee of the functionality and integrity of its core components (Broeders 2015a; Broeders 2015b).

This chapter proposes some measures essential towards improving the stability and security of the Internet.

- More efforts are required in the area of detection or/and mitigation of threats including BGP MITM, root zone KSK brute-force, and domain shadowing attacks. Existing solutions need further reviews. For instance, while it is certain the root zone KSK rollover is essential to mitigate brute-force attack against the KSK, further research could be commissioned towards identifying potential implementation and configuration issues.
- The size and scale of recent cyberattacks are pointing to increasing involvement of state actors. When this is placed side by side the increasing critical role the Internet is likely to play in national development in the years ahead, the need for states to categorize security of the Internet as a national security issue, more than ever before, cannot be overemphasized. Hence, states should identify all core Internet infrastructures within their boundaries as critical national infrastructure (CNI). While some states, including UK (CPNI 2017) and US (DHS 2017), have included communication sector or/and IT sector as CNIs, others, like Nigeria (Adepetun 2016; Onwuanumba 2017), are yet to.

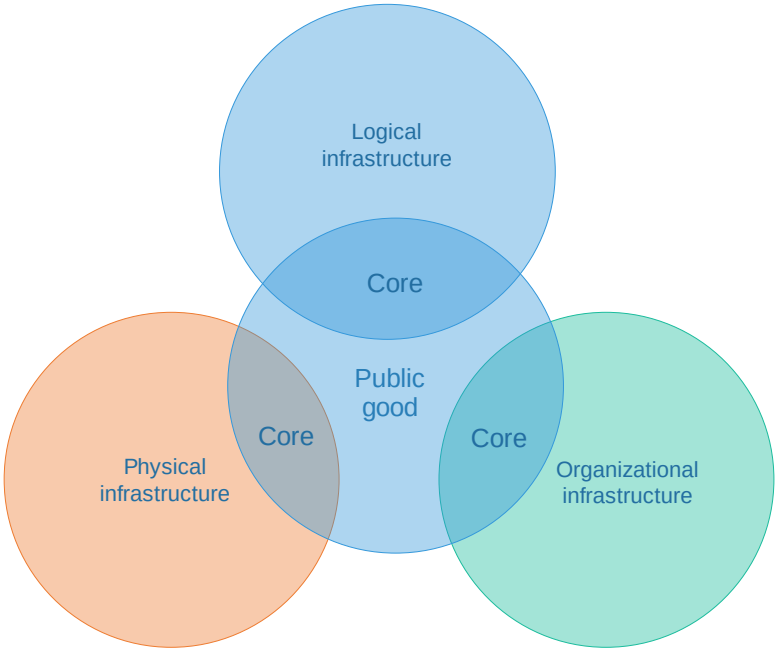
CONCLUSION: IMPLICATIONS FOR THE "PUBLIC CORE" OF THE INTERNET

This brief identifies the various categories of Internet disruption and risks which threaten the core infrastructure of the Internet. Existing risk mitigation mechanisms and good practices are explored; while some gaps, requiring urgent attention, are identified. Lastly, some measures essential to enhance the stability and security of the Internet are proposed.

Using criticality to the stability and security of the Internet as a basis, this brief argues that the systems that support basic information and communication services on the Internet could, if lost or degrade, in theory, constitute single points of failure. These include the DNS root zone, DNS root name server, TCP/IP, BGP, TLD nameservers, backbone routers, and the companies that manage core infrastructures.

The future of the Internet rests primarily on its capacity to consistently guarantee the values of confidentiality, integrity, and availability. The arguments of this brief underline the urgent need for the core infrastructures of the Internet to be protected from belligerent state and non-state actors who undermine, exploit, and target them. This supports existing studies (e.g. Broeders 2015a), which recommend the designation of core Internet protocols and infrastructures as a global public good (as presented in Figure 3). The Internet affords many benefits to everyone. Hence, the core of its existence and survival should not be jeopardized.

Figure 3. The Internet core as a global public good



BIBLIOGRAPHY

Adepetun, Adeyemi. 2016. "For Telecoms Operators, the Challenge of Infrastructure Vandalism Is Sour Pill." The Guardian, April 12. https://guardian.ng/features/for-telecoms-operators-the-challenge-of-infrastructure-vandalism-is-sour-pill/.

Alaettinoglu, Cengiz. 2015. "BGP Security: No Quick Fix." Network Computing. https://www.networkcomputing.com/networking/bgp-security-no-quick-fix/1303232068.

Amichai-Hamburger, Yair, ed. 2013. The Social Net: Understanding Our Online Behavior. Oxford: Oxford University Press.

Anderson, Collin. 2013. "Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran." arXiv Preprint arXiv:1306.4361, 1–31. http://arxiv.org/abs/1306.4361.

Aryan, Simurgh, Homa Aryan, and J. Alex Halderman. 2013. "Internet Censorship in Iran : A First Look." 3rd USENIX Workshop on Free and Open Communications on the Internet, no. August: 8.

Aydin, Deniz Duru. 2016. "Five Excuses Governments (Ab)use to Justify Internet Shutdowns." DW Akademie. http://www.dw.com/en/five-excuses-governments-abuse-to-justify-internet-shutdowns/a-36135649.

Biasini, Nick. 2015. "Threat Spotlight: Angler Lurking in the Domain Shadows." Cisco Blogs. https://blogs.cisco.com/security/talos/angler-domain-shadowing.

Biddle, Sam. 2012. "How to Destroy the Internet." Gizmodo. http://gizmodo.com/5912383/how-to-destroy-the-internet.

Broeders, Dennis. 2015a. The Public Core of the Internet: An International Agenda for Internet Governance. WRR-Policy Brief. The Hague: WRR.

———. 2015b. The Public Core of the Internet: An International Agenda for Internet Governance. Amsterdam: Amsterdam University Press.

———. 2017. "Defining the Protection of 'the Public Core of the Internet' as a National Interest." New Delhi. http://cf.orfonline.org/wp-content/uploads/2017/07/ORF_IssueBrief_190_PublicCore.pdf.

Bush, R, D Karrenberg, M Kosters, and R Plzak. 2010. "Root Name Server Operational Requirements." https://tools.ietf.org/pdf/rfc2870.pdf.

Chander, Anupam, and Uyen P Le. 2014. "Breaking the Web: Data Localization vs. the Global Internet." Emory Law Journal, Forthcoming; UC Davis Legal Studies Research Paper No. 378., no. April: 1–50. doi:http://dx.doi.org/10.2139/ssrn.2407858.

———. 2015. "Data Nationalism." Emory Law Journal 64 (3): 677–739. law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf.

Clark, By Justin, Rob Faris, Ryan Morrison-westphal, Helmi Noman, Casey Tilton, and Jonathan Zittrain. 2017. "The Shifting Landscape of Global Internet Censorship." Cambridge, Massachusetts. https://thenetmonitor.org/research/2017-global-internet-censorship#results.

Colarik, Andrew, and Rhys Ball. 2016. "Anonymous Versus ISIS: The Role of Non-State Actors in Self-Defense." Global Security and Intelligence Studies 2 (1): 4. doi:10.18278/gsis.2.1.3.

Conrad, David. 2016. "DNSSEC: Rolling the Root Zone Key Signing Key." ICANN Blog. https://www.icann.org/news/blog/dnssec-rolling-the-root-zone-key-signing-key.

Cooper, David. 2016. "Why Is DNS Important?" Quora. https://www.quora.com/Why-is-DNS-important.

CPNI. 2017. "Critical National Infrastructure." Accessed December 1. https://www.cpni.gov.uk/critical-national-infrastructure-0.

Decraene, P, P Francois, C Pelsser, Z Ahmad, A. J Elizondo Armengol, and T Takeda. 2011. "Requirements for the Graceful Shutdown of BGP Sessions." https://tools.ietf.org/html/rfc6198.

Deloitte. 2016. "The Economic Impact of Disruptions to Internet Connectivity A Report for Facebook." http://globalnetworkinitiative.org/sites/default/files/The-Economic-Impact-of-Disruptions-to-Internet-Connectivity-Deloitte.pdf.

Dévai, Dóra. 2016. "Proliferation of Offensive Cyber Weapons. Strategic Implications and Non-Proliferation Assumptions." AARMS 15 (1): 61–73.

DHS. 2017. "Critical Infrastructure Sectors." Accessed December 1. https://www.dhs.gov/critical-infrastructure-sectors#.

Di Florio, Andrea, Nino Vincenzo Verde, Antonio Villani, Domenico Vitali, and Luigi Vincenzo Mancini. 2014. "Bypassing Censorship: A Proven Tool against the Recent Internet Censorship in Turkey." In 2014 IEEE International Symposium on Software Reliability Engineering Workshops, ISSREW 2014, 389–94. doi:10.1109/ISSREW.2014.93.

Dooley, Kevin. 2009. Designing Large-Scale LANs. O'Reilly Media.

Drake, William J., Vinton G. Cerf, and Wolfgang Kleinwachter. 2016. "Internet Fragmentation: An Overview." Future of the Internet Initiative White Paper. http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

Dutton, William H, Anna Dopatka, Michael Hills, Ginette Law, and Victoria Nash. 2011. "Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet." Paris.

Essers, Loek. 2015. "The 'Great Cannon' of China Enforces Internet Censorship." Computerworld. https://www.computerworld.com/article/2908504/the-great-cannon-of-china-enforces-internet-censorship.html.

Faris, Robert, and Nart Villeneuve. 2008. "Measuring Global Internet Filtering." Access Denied: The Practice and Policy of Global Internet Filtering 5: 1–24. https://opennet.net/sites/opennet.net/files/Deibert_02_Ch01_005-028.pdf.

Flew, Terry. 2017. "When Governments Want to Splinter the Internet." Khaleej Times, August 4. http://www.khaleejtimes.com/opinion-editorial/when-governments-want-to-splinter-the-internet.

Gaille, Brandon. 2017. "33 Amazing Internet Censorship Statistics." Brandon Gaille. https://brandongaille.com/32-amazing-internet-censorship-statistics/.

Greenberg, Andy. 2017. "Hacker Lexicon: What Is DNS Hijacking?" Wired. https://www.wired.com/story/what-is-dns-hijacking/.

Hall, Eric A. 2000. Internet Core Protocols: The Definitive Guide. Edited by Mike Loukides. First. California: O'Reilly & Associates.

Hepner, Clint, and Earl Zmijewski. 2009. "Defending Against BGP Man-In-The-Middle Attacks." In Talk at BlackHat. Arlington, Virginia. https://www.blackhat.com/presentations/bh-dc-09/Zmijewski/BlackHat-DC-09-Zmijewski-Defend-BGP-MITM.pdf.

Hoffman, Chris. 2016. "5 Ways to Bypass Internet Censorship and Filtering." How-To Geeks. https://www.howtogeek.com/167418/5-ways-to-bypass-internet-censorship-and-filtering/.

Hoogstraaten, Hans, Ronald Prins, Daniël Niggebrugge, Danny Heppener, Frank Groenewegen, Janna Wettinck, Kevin Strooy, et al. 2012. "Black Tulip: Report of the Investigation into the DigiNotar Certificate Authority Breach." doi:10.13140/2.1.2456.7364.

Hughes, Daniel, and Andrew M. Colarik. 2016. "Predicting the Proliferation of Cyber Weapons into Small States." Joint Force Quarterly 83: 19–26.

Hughes, Trevor. 2015. "Attacks Show Fiber Optic Internet Cables Vulnerable." USA Today. https://www.usatoday.com/story/news/2015/09/16/attacks-show-fiber-optic-internet-cables-vulnerable/32502785/.

Huston, Geoff. 2013. "MITM and Routing Security." APNIC. https://labs.apnic.net/?p=447.

IANA. 2016. "DNSSEC Practice Statement for the Root Zone KSK Operator." https://www.iana.org/dnssec/icann-dps.txt.

ICANN. 2013. "Security, Stability and Resiliency Framework." https://www.icann.org/en/system/files/files/ssr-plan-fy14-06mar13-en.pdf.

———. 2014a. "ICANN - DNS Resilience Model." https://www.icann.org/en/system/files/files/dns-resilience-model-28may14-en.pdf.

———. 2014b. "ICANN - DNS Risk Assessment." https://www.icann.org/en/system/files/files/dns-risk-consultation-28may14-en.pdf.

———. 2016. "New gTLD Program Safeguards Against DNS Abuse." file:///C:/Users/USER/Downloads/safeguards-against-dns-abuse-18jul16-en (1).pdf.

Internet Society. 2017a. "Internet Resilience and Stability." Accessed December 1. http://internetsociety.ngo/what-we-do/issues/security.

———. n.d. "Mutually Agreed Norms for Routing Security (MANRS)." https://wp.internetsociety.org/routingmanifesto/wp-content/uploads/sites/14/2016/09/MANRS_PDF_Sep2016.pdf.

———. 2017b. "Technical Aspects of the Internet." Accessed September 3. https://www.internetsociety.org/internet/how-it-works/technical-aspects.

ISO. 2011. "ISO/IEC 27005:2011." https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en.

Kamen, Matt. 2017. "Governments Shut down the Internet More than 50 Times in 2016." Wired. http://www.wired.co.uk/article/over-50-internet-shutdowns-2016.

Kelley, Michael B. 2017. "Evidence of Iran â€TM Throttling â€TM the Internet Points to an Ingenious Form of Censorship." Business Insider. http://www.businessinsider.com/how-iran-slows-down-its-internet-2013-6?IR=T.

Kende, Michael. 2016. "Global Internet Report 2016." Internet Society.

Khanse, Anand. 2015. "What Is a DNS Hijacking Attack & How to Prevent It." The WIndowsClub. http://www.thewindowsclub.com/what-is-dns-hijacking-prevention.

Kumar, Aparna. 2001. "Libertarian, or Just Bizarro?" Wired. http://www.wired.com/politics/law/news/2001/04/43216.

Leberknight, Christopher S., Harold Vincent Poor, Mung Chiang, and Felix Wong. 2010. "A Taxonomy of Internet Censorship and Anti-Censorship." In Fifth International Conference on Fun with Algorithms, 28. http://trends.ifla.org/node/25.

Leiner, Barry M, Vinton G Cerf, David D Clark, Robert E Kahn, Leonard Kleinrock, Daniel C Lynch, Jon Postel, Larry G Roberts, and Stephen Wolff. 2009. "A Brief History of the Internet Professor of Computer Science." ACM SIGCOMM Computer Communication Review 39 (5): 22–31.

Lemon, Sumner. 2006. "Earthquakes Disrupt Internet Access in Asia." PCWorld. https://www.pcworld.com/article/128337/article.html.

Lévy-Bencheton, Cedric, Louis Marinos, Rosella Mattioli, Thomas King, Christoph Dietzel, and Jan Stumpf. 2015. "Threat Landscape and Good Practice Guide for Internet Infrastructure." doi:10.2824/34387.

Lewis, Nick. 2017. "What Is Domain Shadowing and How Can Enterprises Defend against It?" SearchSecurity. Accessed December 15. http://searchsecurity.techtarget.com/answer/What-is-domain-shadowing-and-how-can-enterprises-defend-against-it.

Ma, Richard T.B., Dah Ming Chiu, John C.S. Lui, Vishal Misra, and Dan Rubenstein. 2010. "Internet Economics: The Use of Shapley Value for ISP Settlement." IEEE/ACM Transactions on Networking 18 (3): 775–87. doi:10.1109/TNET.2010.2049205.

Madory, Doug. 2017. "Widespread Impact Caused by Level 3 BGP Route Leak." ORACLE + Dyn. https://dyn.com/blog/widespread-impact-caused-by-level-3-bgp-route-leak/.

Maier, G, and A Wildberger. 1994. In 8 Sekunden Um Die Welt. Kommunikation Über Das Internet. Bonn, Paris: Addison-Wesley.

Manion, Art. 2003. "Vulnerability Note VU#844360: Domain Name System (DNS) Stub Resolver Libraries Vulnerable to Buffer Overflows via Network Name or Address Lookups." Vulnerability Notes Database. http://www.kb.cert.org/vuls/id/844360.

Marsan, Carolyn Duffy. 2010. "DNSSEC Doesn't Mitigate All DNS Threats." The IETF Journal, no. October. https://www.ietfjournal.org/dnssec-doesnt-mitigate-all-dns-threats/.

Maurer, Tim, and Robert Morgus. 2014. "Stop Calling Decentralization of the Internet 'Balkanization.'" Future Tense. http://www.slate.com/blogs/future_tense/2014/02/19/stop_calling_decentralization_of_the_internet_balkanization.html.

Maurer, Tim, Robert Morgus, Isabel Skierka, and Mirko Hohmann. 2014. "Technological Sovereignty: Missing the Point?" preview.newamerica.org/downloads/Technological_Sovereignty_Report.pdf.

Mohan, Ram. 2011. "Attacking the Internet's Core." Securityweek Network. http://www.securityweek.com/attacking-internets-core.

Noman, Helmi. 2011. "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army." Information Warfare Monitor. Vol. 30. https://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army.

Onwuanumba, Isaiah. 2017. "Nigeria: Govt Sets To Declare Telecoms Facilities 'National Critical Infrastructure.'" IT News Nigeria, March 17. http://www.itnewsnigeria.com.ng/2017/03/17/nigeria-govt-sets-to-declare-telecoms-facilities-national-critical-infrastructure/.

Oti, Stephen Brako, Isaac Bansah, and Tony M. Adegboyega. 2016. "A Configuration Based Approach to Mitigating Man-in- the-Middle Attacks in Enterprise Cloud IaaS Networks Running BGP." International Journal of Computer Applications 146 (1): 23–27. http://www.ijcaonline.org/archives/volume146/number1/oti-2016-ijca-910604.pdf.

Paganini, Pierluigi. 2016. "A Nation-State Actor Is Testing Methods for a Massive Takedown of the Internet According to the Popular Cyber Security Experts an Unknown Nation State Actor May Be Running Tests for Taking down the Entire Internet Infrastructure ." Security Affairs. http://securityaffairs.co/wordpress/51669/hacking/internet-takedown.html.

Piscitello, Dave. 2016. "Attacks Against The DNS." https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/2A.pdf.

Previous Contributors. 2013. "Google's Malaysian Domains Hit with DNS Cache Poisoning Attack." The State of Security. https://www.tripwire.com/state-of-security/latest-security-news/googles-malaysian-domains-hit-dns-cache-poisoning-attack/.

Prince, Matthew. 2012. "Deep Inside a DNS Amplification DDoS Attack." CloudFare. https://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack/.

Qamar, Ali. 2014. "How to Stop DNS Hijacking." Infosec Institute. http://resources.infosecinstitute.com/stop-dns-hijacking/.

Roberts, Paul F. 2002. "Major 'Net Backbone Attack Could Be First of Many." NetworkWorld. https://www.networkworld.com/article/2342906/lan-wan/major--net-backbone-attack-could-be-first-of-many.html.

Schmidt, Eric E., and Jared Cohen. 2014. "The Future of Internet Freedom." The New York Times. http://www.nytimes.com/2014/03/12/opinion/the-future-of-internet-freedom.html.

Schneier, Bruce. 2016. "Someone Is Learning How to Take Down the Internet." Schneier on Security. http://www.amazon.com/Schneier-Security-Bruce/dp/0470395354.

Schuchard, Max, Abedelaziz Mohaisen, Denis Foo Kune, Nicholas Hopper, Yongdae Kim, and Eugene Y. Vasserman. 2010. "Losing Control of the Internet: Using the Data Plane to Attack the Control Plane." In Proceedings of the 17th ACM Conference on Computer and Communications Security, Pp. 726-728, 1–15. doi:10.1145/1866307.1866411.

Shashidhar, K J. 2017. "Govt Asks Telecom Companies to Throttle Mobile Internet Speeds in Kashmir." Medianama. https://www.medianama.com/2017/06/223-throttle-mobile-internet-speeds-kashmir/.

Sigholm, Johan. 2013. "Non-State Actors in Cyberspace Operations." Journal of Military Studies 4 (1): 1–37. doi:10.1515/jms-2016-0184.

SSAC. 2005. "Domain Name Hijacking: Incidents, Threats, Risks, and Remedial Actions." https://archive.icann.org/en/announcements/hijacking-report-12jul05.pdf.

———. 2008. "SAC 032 Preliminary Report on DNS Response Modification." https://www.icann.org/en/system/files/files/sac-032-en.pdf.

Team RiskIQ. 2016. "Domain Shadowing: When Good Domains Go Bad." RiskIQ. https://www.riskiq.com/blog/external-threat-management/domain-shadowing-good-domains-go-bad/.

TechTarget Network. 2010. "Traffic Shaping (Packet Shaping)." Network Management and Monitoring: The Evolution of Network Control. http://searchnetworking.techtarget.com/definition/traffic-shaping.

Terman, Rochelle. 2012. "Internet Censorship (Part 2): The Technology of Information Control." http://townsendcenter.berkeley.edu/blog/internet-censorship-part-2-technology-information-control.

The Economist. 2010. "The Future of the Internet: A Virtual Counter-Revolution." The Economist. http://www.economist.com/node/16941635.

Toonk, Andree. 2013. "Accidentally Stealing the Internet." BGPMon. https://bgpmon.net/accidentally-stealing-the-internet/.

———. 2017. "BGPstream and the Curious Case of AS12389." BGPMon. https://bgpmon.net/bgpstream-and-the-curious-case-of-as12389/.

Turner, Paul, William Polk, and Elaine Barker. 2012. "Preparing for and Responding to Certification Authority Compromise and Fraudulent Certificate Issuance." http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=911197.

US-CERT. 2013. "DNS Amplification Attacks." US-CERT. https://www.us-cert.gov/ncas/alerts/TA13-088A.

US GAO. 2006. "Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan." Methodology. http://www.gao.gov/assets/260/250483.pdf.

Van Alstyne, Marshall, and Erik Brynjolfsson. 1996. "Electronic Communities: Global Village or Cyberbalkans?" In Proceedings of the 17th International Conference on Information Systems, 1–32. Cleveland, OH. ftp://ftp.gunadarma.ac.id/.upload/www.bogor.net/www.bogor.net/idkf-1/aplikasi/electronic-community-global-village-or-cyberbalkans-03-1997.pdf.

Van Beijnum, Iljitsch. 2011. "How Egypt Did (and Your Government Could) Shut down the Internet." Ars Technica. https://arstechnica.com/tech-policy/2011/01/how-egypt-or-how-your-government-could-shut-down-the-internet/.

Wessels, Duane. 2017. "A Closer Look at Postponing of the Root Zone KSK Rollover Decision." CircleID. http://www.circleid.com/posts/20170929_a_closer_look_at_postponing_of_root_zone_ksk_rollover_decision/.

West, Darrell M. 2016. "Internet Shutdowns Cost Countries $2.4 Billion Last Year." https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf.

Wolchover, Natalie. 2011. "How Do You Shut Down the Internet in a Whole Country?" Live Science. https://www.livescience.com/32965-how-do-you-shut-down-the-internet-whole-country.html.

Woolf, Nicky. 2016. "DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say." The Guardian. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

Xu, Young. 2017. "Best Practices to Combat Route Leaks and Hijacks." ThousandEyes. https://blog.thousandeyes.com/best-practices-combat-route-leaks-hijacks/.

MAPPING NATIONAL AND TRANSNATIONAL CRITICAL INFORMATION INFRASTRUCTURES

Prof. Analía Aspis, *University of Buenos Aires*

BRIEFING №4

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

CERT - Computer Emergency Response Team

CI - Critical Infrastructures

CIP - Critical Infrastructure Protection

CII - Critical Information Infrastructures

CIIP - Critical Information Infrastructure Protection

CIR - Critical Infrastructure Resilience

CSIRT - Computer Security and Incident Response Team

EC - European Commission

EPCIP - European Programme on Critical Infrastructure Protection

ENISA - European Union Agency for Network and Information Security

GII - Global information infrastructure

ICT - Information and Communication Technologies

NIPP - National Infrastructure Protection Plan

PPP - Public-Private Partnership

SCADA - Supervisory Control and Data Acquisition

TCI - Transnational Critical Infrastructures

TCII - Transnational Critical Information Infrastructures

WEF - World Economic Forum

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

Today, most modern countries base their economic wealth and societal prosperity on several critical information infrastructures (CII). These CII constitute the cornerstone of countries' growth, and thanks to this role they are beginning to be considered by many States as critical assets that must be protected against possible attacks and malfunctioning. Accordingly, the degree of interconnectivity of information and communication technologies (ICT), systems and networks is increasingly perceived by governments as areas where policies should support not only a continued growth in technology sophistication but also the development of cybersecurity strategies to protect ICT from cyber-attacks. In this context, it becomes necessary to study how the CII are perceived by different countries around the world in order to have a comprehensive understanding of their meaning and scope. As a matter of fact, even though this topic has been treated by different authors, research is still lacking on identification of both global and regional CII approaches.

For these reasons, the main purpose of the present research will be to map national CII so as to serve as an initiative to help stakeholders to identify and share areas of study in the field of cybersecurity and infrastructures interdependence, as well as to motivate them to take action and raise commitment to CII protection worldwide. In this sense, this report will present a recompilation and analysis of the current national CII definitions and cybersecurity initiatives.

The document structure is divided in three parts. In the first part, it provides a background on the relationship between critical infrastructures (CI) and CII, their interdependency and a global approach on how CII are defined. Second, it provides figures, statistical data and an analysis of the CII components, both from a global and regional perspective. Third, the relationship between CI, ICT and cross-border attacks will be presented. Finally, it presents conclusions and proposals for future research in the area of CII and cybersecurity.

With regard to the report methodology, the following steps are involved:

1. First we proceeded to select the number of countries to be studied. For that and considering the research timeline, we decided to focus mainly on countries which were part of the official directory CERT Division of the Software Engineering Institute.[151] As a result, the number of countries selected ended up in 95. This database was used for Section 1.3. We divide those countries into 7 regions, following the division suggested by the European Network and Information Security Agency's CSIRTs map[152] and the UNESCO.
2. From the above database, we carried out a research on the existence of governmental offices related to CII. Such search gave us a result of 173 government offices, with their corresponding denomination and contact details. Due to timeframes, we decided not to include public private partnerships (PPP), even though we did found different offices related to PPP and CII.
3. We conducted a short survey which contains a CII policies oriented questions so as to gather information about CII related themes and the offices working on CII field. The questionnaire was sent, by a third party, to government CII related offices. Responses to the survey have been limited as of report delivery and since such answers did not provide us with additional information other that the already contained in our bibliography and data review we have decided not to include them in the main report but incorporate them in the Annex section.

[151] https://www.cert.org/incident-management/national-csirts/national-csirts.cfm, accessed 24 October, 2017.

[152] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

4. In addition to (I), within the 95 selected countries, we looked at how many of them had a definition of CII. As a result, we found a total of 38 national definitions and 6 other from other bodies. As the responses to the questionnaire were few, we decided that these definitions were going to constitute the principal data which that is going to be visualized in this report. We decided to focus on national definitions, and their regional impact.
5. Finally, an introduction to the concepts of cross-border, nation-wide and global infrastructures and their relationship with CI will be presented.
6. Unless otherwise noted, all figures and tables were created by the author.

According with the objectives and methodological approach described above, the report presents the following results:

- a record of the existing national and regional approaches in the field of CII
- a chronological evolution of the number of definitions
- a detailed list of government offices and specific institutions working on CII initiatives
- a visual mapping that will reflect the different elements of the CII as defined by countries
- a list of existing definitions of nation-wide or cross border critical infrastructures and related examples

The present report is intended to bring to the attention of policymakers analytical perspectives on the above CII topic in order to implement selected aspects suitable to their national environment, with the added benefits of helping harmonize practices and fostering, a global culture of cybersecurity.

SECTION 1: CRITICAL INFORMATION INFRASTRUCTURES (CII): BACKGROUND AND DEFINITIONS

This section aims to introduce the concepts of critical infrastructures, critical information infrastructures and their relationship with cyber-security and cyber-attacks. It also presents a mapping of the global offices related to CII as well as a list of CII definitions, from a global perspective.

1.1 FROM CI TO CII

Critical infrastructures (CI) are at the core of any advanced civilized country. These infrastructures have been continually updated from the beginning of the previous century when the focus was on the protection of railroads, bridges and roads. In general terms, we could state that a critical infrastructure is often identified as "that infrastructure whose incorrect functioning, even for a limited time period, may negatively affect the economy of individual subjects or groups, involving economic losses and/or even expose people and things to a safety and security risk" (TENACE 2014, 6).

In Lazari's words, the term "critical infrastructure is vague (Lazari 2014, 1). The European Commission defines a critical infrastructure as an "asset or system which is essential for the maintenance of vital societal functions" .[153] While each country determines what specifically constitutes a CI, States and academic experts have begun to identify a common understanding of its meaning (CTED 2017, 2). In this sense, CI may include areas such as communications; emergency services; energy; dams; finance; food; public services; industry; health; transport; gas; public communications, radio and television; information technology; commercial facilities; chemical and nuclear sectors; and water.

It is important to point out that CI (electricity, transportation, financial systems, etc.) are increasingly managed electronically. The introduction of network management, monitoring and control systems, as well as the rise of interdependence among infrastructures, have not only improved their management, but have also made possible cyber-attacks-, and the chances of causing a domino effect. Therefore, the scenario has become more and more complex in recent years, as the introduction of advanced technology has added new sources of potential risk alongside the traditional ones.

[153] COM (2005) 576 final: Green paper on a European Programme for Critical Infrastructure Protection, 17 November 2005.

Hence, the introduction of ICT has enabled CI automation possibilities, allowing their complete control to be managed remotely (e.g. over the Internet). The evolution of the infrastructures, which are interlinked with computers, smart sensors and networks of computers, has added another layer of complexity. As a result, industries and governments have been progressively adopting IT systems to consolidate the operations of CI, resulting in a convergence of CI and IT systems.

Consequently a new category has arisen, namely Critical Information Infrastructures (CII), which can refer not only to those ICT elements penetrating traditional CI, but also those networks, systems, assets and services that could be seen as a standalone critical infrastructure, i.e., a type of CI that can also be primarily considered as CII. In this sense, CI include but are not limited to CII,[154] thus CII are critical infrastructures but not necessarily all critical infrastructures should be considered as CII (Luiijf et al. 2016, 5). The complexity of CII derives from their decentralization in terms of geographical location, their public or private ownership and the national economies' reliance on information systems and interconnected networks. A sensitive complex infrastructure has become a priority for governments and other stakeholders, due to their exposure to cyber-attacks. It is important to remember that the breakdown of CII and networks –including the Internet- was identified as the most likely to be at risk globally in the Global Risk Report 2007 of the World Economic Forum (WEF 2016, 11). In another recent report, it was concluded that "Finance, ICT and Energy sectors appear to have a much higher incident cost, in comparison with the rest of sectors" and that "Data seems to be the most affected asset" (ENISA 2016, 25).

In this framework, a typical cyber-attack is launched with the intent to paralyze the CI activities or to purloin its information assets. In the context of CII, it is important to evaluate the possible attack targets to assess the consequences, including the time required to restore normal behaviour in an interconnected CI and CII network. As Colesniuc states, the opening stage of any future war against even a relatively modern state would be likely to include some form of cyber-warfare, or more specifically cyber-attacks on its CII (Colesniuc 2013, 125). Interdependence has inevitably increased the risk of cyber-attacks against governments and business: "as the Internet becomes more powerful and as our dependence upon it grows, cyber-attacks may evolve from a corollary of real-world disputes to play a lead role in future conflicts" (Geers 2011, 9) and, in this sense, the concept of resilience has become as a global priority. Researchers have acknowledged the importance of building resilience in order to face strong cyber-attacks that are bound to take place sooner or later. One of the most widespread definitions of resilience is: "the ability of a system, community or society exposed to hazards to resist, absorb, accommodate and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions" (RECIPE 2011, 86). The following table presents some cyber-attacks perpetrated against CII, sorted by date and with the details of the affected country and a short description of the event. It should be noted that the distinction between a CI and a CII attack is not always clear, in this sense, the following table is illustrative.

[154] Interestingly, the Internet is itself an underlying, critical asset of modern CI, because their controlling systems are often distributed over remote Internet-connected locations.

Table 1: Example of CII cyber-attacks

Date of first public report	Affected country	Description
May 2005	Estonia	DDoS attacks against Estonian government infrastructure and systems.
August 2006	U.S.A.	Attackers downloaded 10 to 20 terabytes of data from the NIPRNet, the U.S. Department Of Defense (DoD) network for exchanging sensitive (but unclassified) information.
June 2009	Iran	"Stuxnet" malware infected Industrial control systems, silently accelerated Iranian nuclear centrifuges until they destroyed themselves.
November 2009	U.S.A.	Operation "Night Dragon": hacked critical infrastructure companies in the US, mainly energy companies.
January 2012	Israel	The data of thousands of credit cards, bank accounts and personal data of Israeli citizens were published online.
March 2012	U.S.A.	US Department of Homeland Security (DHS) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) warned of attempts at cybernetic intrusion into US pipelines.
April 2012	Iran	Iran disconnected computer systems of key oil facilities on Kharg Island (Persian Gulf) after a cyber-attack which used a malware called "Wiper", against Oil Ministry's headquarters and the national oil company.
August 2012	Saudi Arabia - Qatar	The "Cutting Sword of Justice" delete data and infect control systems of an oil producer company. The attack also affected a Qatari company producer of liquefied natural gas.
September 2012	U.S.A.	An Iranian hacker group launched "Operation Ababil" conducted DDoS attacks against U.S. financial institutions, affecting bank websites.
May 2013	Israel	Israeli officials reported an unsuccessful cyberattack on the water infrastructure of the city of Haifa.
March 2014	South Korea	Attackers infected two operating servers of Seoul Metro, which runs four major subway lines.
August 2014	Norway	The National Security Authority Norway reported to have claimed that 50 companies in the oil sector were hacked and another 250 may have been hit too.
December 2015	Ukraine	The first confirmed take down of a power grid. The attackers overwrote the firmware on critical devices at substations, leaving them unresponsive to any remote commands from national operators, and launched a "telephone denial-of-service attack "against customer call centers to prevent customers from calling to report the outage.
May 2017	Global	WannaCry ransomware targeted computers running the Windows operating system, encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. The infection affected companies in the health care, telecommunications, financial and other vital sectors.
June 2017	United Kingdom	The Houses of Parliament have discovered unauthorized attempts to access parliamentary user accounts.

1.2 CII: CATEGORIES AND INTERDEPENDENCE

With regard to CII categories, different types have been identified. For instance, one CII category could be constituted by "those information and communication technology (ICT) based infrastructures that are essential for a Critical Infrastructure" and a second CII category could be y the "ICT-based infrastructure that is a critical infrastructure on its own" (Luiijf 2006, 2-3). Another type of CII category was established by OECD, which has identified three types of CII categories, namely "Information components supporting the critical infrastructure", "Information infrastructures supporting essential components of government business" and/or "Information infrastructures essential to the national economy" (OECD 2007, 4). A more recent report refers to CII categories, considering that one CII category describes CII as "as part of a critical sector or service", and "another CII category describes CII as a distinct critical sector or service itself. It should be noted that the report highlights that those categories are not necessarily considered mutually exclusive" (Kaska and Trinberg 2015, 10).

Interdependency can be defined as a bidirectional relationship between two or more infrastructures through which the state of each infrastructure influences or is correlated to the state of the other[155] (TENACE 2014, 24). CI interdependencies have their own unique characteristics and effects. Within the CII context, it is considered that CII have interdependency if "their state depends on information transmitted through the information infrastructure" (Tadjibayev and Sattarova 2009, 19). Failures affecting interdependent infrastructures are complex and can cause cascading faults, progressive faults, fault damping impact, common cause, or distributed fault impact (Sharma 2017, 46). Many States increasingly depend on infrastructure and assets that are partially or completely located outside their jurisdiction (CTED 2017, 2). They are mostly developed and built at the national level, linked to the infrastructures of other countries. Thus the collapse of a portion of one country's CII would have a serious impact on its neighbours as well, an impact on energy distribution, air traffic control, banking or financial services. (Colesniuc 2013, 124). However, it should be noted that, besides making technology less vulnerable to attacks, some authors argue that it is necessary to face the great challenge of making society less dependent on technology (Koops 2017, 12). According to the Global Risks Report 2016, cyber dependency contributes to the amplification of global risks (WEF 2016, 87).

The interdependence element is a major challenge for risk management in CII due to the fact that economies and societies rely on interconnected infrastructure systems. This gives rise, inter alia, to a phenomenon known as "cascading events" – that is, once a cyber-attack occurs, other disruptions are likely to follow within systems and processes that are connected to the infrastructure affected by the initial disruption (OECD 2008, 5-6).

1.3 CII RELATED OFFICES

Taking into consideration interdependency and CII vulnerabilities and to prevent cyber-attacks and failures events mentioned above, many countries have developed strategies to face these new challenges. From crisis management to risk assessment, many governments have dedicated resources to offices created or designated to handle CII related issues. From a total of 173 offices, it should be pointed out that many have been created as a part of a national security strategy or a critical information infrastructure protection (CIIP) policy. In general, these offices focus their work on four specific objectives: prevention and early warning; detection; reaction; and crisis management (Suter 2007, 1-4) in addition to identifying threats and reducing system vulnerabilities to any type of damage or attack, governmental offices also work to reduce their recovery time. This is why CIIP has been linked to CI assurance since States are "concerned

[155] While the idea of dependence denotes a one-way relationship, there are, at least, four principal categories of infrastructure interdependencies: (i) physical dependencies; (ii) cyber dependencies; (iii) geographical dependencies and (iv) logical dependencies (Rinaldi, Peerenboom, and Kelly 2001, 14-15).

with the readiness, reliability, and continuity of infrastructure services so that they are less vulnerable to disruptions, any impairment is short duration and limited in scale, and services are readily restored when disruptions occur" (Kenneth and Tritak 2002, 12). The following table illustrates all those countries that have a public office related to CII, this being a CERT / CSIRT, a program or a CII center as well as the existence or not of a CII definition in each country. The overall result is the following:

Table 2: Countries with CII related offices and CII definition

United States And Canada		
Country	CII definition	
United States Of America	Yes	
Canada		No
Europe (European Union)		
Country	CII definition	
Austria		No
Belgium		No
Bulgaria	Yes	
Croatia	Yes	
Cyprus		No
Czech Republic	Yes	
Denmark		No
Estonia	Yes	
Finland	Yes	
France	Yes	
Germany		No
Greece		No
Hungary		No
Ireland	Yes	
Italy	Yes	
Latvia	Yes	
Lithuania	Yes	
Luxembourg		No
Malta		No
Netherlands		No
Poland		No
Portugal	Yes	
Romania		No
Slovakia	Yes	
Slovenia		No
Spain		No
Sweden		No
United Kingdom	Yes	

Asia And Pacific		
Country	CII definition	
Azerbaijan		No
Australia		No
Bangladesh		No
Brunei Darussalam		No
Cambodia		No
China	Yes	
India	Yes	
Indonesia		No
Iran		No
Japan	Yes	
Kazakhastan		No
Lao		No
Malaysia	Yes	
Myanmar		No
New Zealand		No
Korea	Yes	
Russian Federation	Yes	
Singapore		No
Sri Lanka		No
Thailand		No
Tonga		No
Uzbekistan		No
Vietnam		No
Europe (Non European Union)		
Country	CII definition	
Albania	Yes	
Georgia	Yes	
Israel		No
Kosovo	Yes	
Moldova		No
Montenegro		No
Norway	Yes	
Turkey	Yes	
Ukraine	Yes	

Africa		
Country	CII definition	
Burkina Faso		No
Cote D'ivoire		No
Egypt		No
Ethiopia		No
Ghana	Yes	
Kenya		No
Mauritious		No
Nigeria	Yes	
South Africa	Yes	
Uganda	Yes	
Tanzania		No
Zambia		No
Arab States		
Country	CII definition	
Argelia		No
Morocco		No
Oman		No
Qatar	Yes	
Saudia Araba		No
Tunisia		No
United Arab Emirates		No
Latin America And The Caribbean		
Country	CII definition	
Argentina		No
Brazil	Yes	
Chile	Yes	
Colombia	Yes	
Costa Rica	Yes	
Cuba		No
Ecuador		No
Mexico		No
Panama		No
Paraguay		No
Peru		No
Uruguay	Yes	
Venezuela		No
Curacao		No

As previously mentioned, from the 95 selected countries, we have identified a total of 173 national offices related to CII. In order to be able to obtain more specific details, we decided to divide them into different categories so as to better understand the type of offices or programs that are working in the field of CII. The results of these categories are as follows.

Table 3: CII offices (per region)

Region	CERT	Cybersecurity Program/Center/ Office	Critical Information Infrastructure Program /Centre/Office	Critical Infrastructures office	Information Security Center/Authority/Office	ICT and other related national offices and programs	Total
United States and Canada	2	1	2	0	0	1	6
Europe (European Union)	23	12	4	0	7	6	52
Europe (Non European Union)	7	1	0	0	0	5	13
Asia and Pacific	24	5	1	4	1	7	42
Africa	12	1	0	0	1	11	25
Arab States	8	0	0	0	0	4	12
Latin America and the Caribbean	13	5	0	0	1	4	23
TOTAL	89	25	7	4	10	38	173

Conversely, almost no CI public office is working on CII related issues. We can observe that governments have developed programs and offices dedicated exclusively to CII. This could be interpreted as a concrete public interest in the protection of such infrastructures.

1.4 NATIONAL GOVERNMENTS' DEFINITIONS OF CII

When conducting research, we have found few compilations of CII definitions. For instance, the ENISA guide[156] only includes two definitions (ENISA 2014) while the CCDCOE provides six.[157] Nowadays, the biggest CII definition compilation is the "CIPedia",[158] however we have found some inconsistencies in its citations, dates, web links and translations. In this sense, despite the numerous attempts made so far, there is still no research that provides a global index of CII definitions that allow us to understand government policies on this subject. The present report intends to contribute to mitigating this lack of information.

As a preliminary observation, we have observed within the 95 countries that have a CII office, less than half of them have a CII definition:

[156] It is interesting to note that according to an ENISA guideline, the presence of a CII definition is considered as an indicator of high maturity in terms of the effective identification of CII assets and services, which could only occur if the CII have been previously recognized as one of the critical sectors for the maintenance of the vital societal functions.

[157] https://ccdcoe.org/cyber-definitions.html

[158] https://publicwiki-01.fraunhofer.de/CIPedia/index.php/CIPedia%C2%A9_Main_Page

Figure 1: Percentage of countries which have a CII definition:[159]

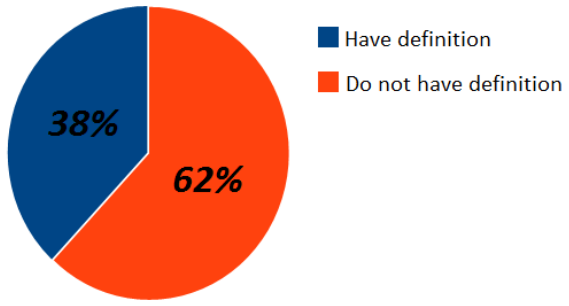


Table 4 illustrates their chronological order of appearance. As can be seen, the first definition of CII found is in 2001, the latest being in 2017.

Table 4: Definitions of CII (by year)

Year	Number of definitions found	Countries
n/d	3	Estonia - France - Portugal
2001	1	Korea
2002	-	
2003	-	
2004	1	Italy
2005	-	
2006	-	
2007	-	
2008	-	
2009	3	India - Brazil - Uruguay
2010	3	Latvia - Malaysia - South Africa
2011	2	Lithuania - United Kingdom
2012	3	United States of America - Georgia - Norway
2013	2	Finland - Turkey
2014	6	Czech Republic - Lithuania - Japan - Ghana - Uganda - Qatar
2015	7	Croatia - Ireland - Slovakia - Albania - Kosovo - Nigeria - Chile
2016	5	Bulgaria - Ukraine - China - China - Colombia
2017	2	Russia - Costa Rica
TOTAL	**38**	

[159] Among the 39% of the countries that do have a CII definition, we have observed that this later comes either from a legal instrument, a national security program, a report or a glossary.

Table 5 shows countries' definitions, separated by region. The list is not intended to be exhaustive although it reflects the most recent compilation.

Table 5: Global CII definitions

REGION: UNITED STATES AND CANADA	
United States of America	"any physical or virtual information system that controls, processes, transmits, receives or stores electronic information in any form including data, voice, or video that is: - Vital to the functioning of critical infrastructure; - So vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on national security, national economic security, or national public health and safety; or - Owned or operated by or on behalf of a State, local, tribal, or territorial government entity
REGION: EUROPE (EUROPEAN UNION)	
Bulgaria	"Systems,services, networks and infrastructures that are a vital part of the national economy and society and provide important goods and services, whose destruction could have a serious impact on the vital functions of society. Critical information infrastructure is both networks, channels, and systems for managing and maintaining them".
Croatia	"communication and information systems whose disturbed functioning would significantly disturb the work of one or more identified critical national infrastructures" (Critical communication and information infrastructure).
Czech Republic	"an element or system of elements of the critical infrastructure in the sector of communication and information systems within the field of cyber security".
Estonia	"Information and communications systems whose maintenance, reliability and safety are essential for the proper functioning of a country. The critical information infrastructure is a part of the critical infrastructure"
Finland	"the structures and functions behind the information systems of the vital functions of society which electronically transmit, transfer, receive, store or otherwise process information (data)"
France	"They are systems for which the threat to security would significantly affect its military actions, the country's economic potential, the security or the nation's survival capacity" (Critical Important Information Systems)
Ireland	"The systems, services, networks and infrastructures that underpin other Critical Infrastructure, or provide essential services themselves, are called Critical Information Infrastructure (or CII) and include telecommunications networks, the Internet, terrestrial and satellite wireless networks".
Italy	"critical infrastructure that uses for its control, or its management or operation, an IT infrastructure"
Latvia	"The critical infrastructure of information technologies is an infrastructure, which is approved by the Cabinet in accordance with the National Security Law". (critical infrastructure of information technologies)
Lithuania	"an electronic communications network, information system or a group of information systems where an incident that occurs causes or may cause grave damage to national security, national economy or social wellbeing"
Lithuania	"electronic communications network or part of it, an information system or part of it, a group of information systems or industrial control system or part of it, regardless of whether the administrative owner is from the public or private sector, where a cyber-incident can cause harm to national security, economy, state or public interest"
Portugal	"any IT systems that support core assets and services of national infrastructure"
Slovakia	"the set of systems, infrastructures, networks and services of information and communication technologies that would, if disturbed, damaged, or unavailable, seriously impact the operation of other sectors of critical infrastructure and of social functions of vital importance, including national, economic and public security". (Critical Information and Communication

	Infrastructure)
United Kingdom	"any IT systems which support key assets and services within the national infrastructure"
REGION: EUROPE (NON EUROPEAN UNION)	
Albania	"the systems and networks of information and communication whose damage or destruction would have a serious impact on the health, safety, and / or economic well-being of the citizens, and / or the effective functioning of the economy of the Republic of Albania.
Georgia	"an information system whose uninterrupted operation is important for the defense and/or economic security of the state, as well as for normal functioning of the state and/or society" (Critical information system)
Kosovo	"ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.)".
Norway	"critical infrastructure for electronic communications" (Critical ICT infrastructure)
Turkey	The infrastructures which host the information systems that can cause, - Loss of lives, - Large scale economic damages, - Security vulnerabilities and disturbance of public order at national level when the confidentiality, integrity or accessibility of the information they process is compromised" (Critical infrastructures)
Ukraine	"national electronic information resources, information, since the requirement of information protection was imposed by law, and also ensuring cyber protection of information infrastructure that is under jurisdiction of Ukraine and disruption of its sustained operation will have a negative impact on the status of national security and defence of Ukraine"
REGION: ASIA AND PACIFIC	
China	"the information facilities concerning the national security, the national economy and the people's livelihood, which may seriously damage the national security and the public interest if the data is divulged, destroyed or lost, including but not limited to providing public communications, broadcasting and television transmission and other services. Information network, energy, finance, transportation, education, scientific research, water conservancy, industrial manufacturing, medical and health, social security, public utilities and other important information systems and important Internet applications" (National Critical Information Infrastructure)
China	"public communication and information services, power, traffic, water, finance, public service, electronic governance and other critical information infrastructure that if destroyed, losing function or leaking data might seriously endanger national security, national welfare and the people's livelihood, or the public interest"
India	"the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety"
Japan	"The backbone of national life and economic activities formed by businesses providing services that are extremely difficult to be substituted. If the function of the services is suspended, deteriorates or becomes unavailable, it could have a significant impact on the national life and economic activities."
Korea	"electronic control and management system related to the national security, administration, defense, public security, finance, communications, transportation, energy, etc. and information and communications network under Article 2 (1) 1 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc" (information and communications infrastructure).
Malaysia	"those assets (real and virtual), systems and functions that are vital to the nations that their incapacity or destruction would have a devastating impact on: • National economic strength; Confidence that the nation's key growth area can successfully compete in global market

	while maintaining favourable standards of living. • National image; Projection of national image towards enhancing stature and sphere of influence. • National defence and security; guarantee sovereignty and independence whilst maintaining internal security. • Government capability to functions; maintain order to perform and deliver minimum essential public services. • Public health and safety; delivering and managing optimal health care to the citizen". (Critical National Information Infrastructure: CNII)
Russia	- "critical information infrastructure": objects of critical information infrastructure, and also networks of telecommunication used for the organization of interaction of such objects. - "objects of critical information infrastructure": information systems, information and telecommunication networks, automated control systems of subjects of critical information infrastructure. -"subjects of critical information infrastructure" - state bodies, public institutions, the Russian legal persons and (or) individual entrepreneurs to whom on the property right, leases or on other legal cause belong the information systems, information and telecommunication networks, automated control systems functioning in health sector, sciences, transport, communication, power, the bank sphere and other spheres of the financial market, fuel and energy complex in the field of atomic energy, the defense, space-rocket, mining, metallurgical and chemical industry, the Russian legal entities and (or) individual entrepreneurs who provide interaction of the specified systems or networks.
REGION: AFRICA	
Ghana	"those assets (real and virtual), systems and functions that are vital to the nations that their incapacity or destruction would have a devastating impact on: • National economic strength: National economic strength Confidence that the nation's key growth area can successfully compete in global market while maintaining favorable standards of living. • National image: Projection of national image towards enhancing stature and sphere of influence. • National defense and security: Guarantee sovereignty and independence whilst maintaining internal security. • Government capability to functions: Maintain order to perform and deliver minimum essential public services. • Public health and safety: Delivering and managing optimal health care to the citizen (Critical National Information Infrastructure: CNII)
Nigeria	"certain computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters as constituting Critical National Information Infrastructure"
South Africa	"Critical Information Infrastructure means all ICT systems, data systems, data bases, networks (incl. people, buildings, facilities and processes), that are fundamental to the effective operation of the State."
Uganda	"The ITU regards Critical Information Infrastructure (CII) as the virtual element of critical infrastructure. The information and communication technologies (ICTs), that form CII, increasingly operate and control critical national sectors such as health, water, transport, communications, government, energy, food, finance and emergency services; their physical assets and the activities of personnel".
REGION: ARAB STATES	
Qatar	The information and communications technology systems, services, and data assets that are critical to Qatar based on the following classification criteria: 1. Identify the organization's key, core business processes and their dependency on assets owned and managed by the organization (e.g., power plant, refinery, general ledger, etc.); 2. Use impact severity table to determine an impact score for the loss/non-functioning of each key asset; and 3. Classify all assets as critical when the criticality score is greater than twenty
REGION: LATIN AMERICA AND THE CARIBBEAN	
Brazil	"the subset of information assets that directly affect the achievement and continuity of state mission and the safety of society. Information assets are the means of storage, transmission and processing, the information systems, as well as the

	places where those means are located and the people who have access to them"
Chile	"includes the installation, networks, services and physical and information technology equipment whose impairment, degradation, rejection, interruption or destruction may have an important impact on the security, health and wellbeing of people and on the effective operation of the State and the private sector".
Colombia	"infrastructure supported by ICTs and operating technologies, whose operation is indispensable for the provision of essential services for citizens and for the State. Their impact, suspension or destruction can have negative consequences on the economic well-being of citizens, or in the effective functioning of organizations and institutions including the public administration "(National Critical Cyber Infrastructure)
Costa Rica	"IT systems that support key assets and services in the national infrastructure, when an incident that occurs causes or may cause serious damage to national security, national economy or social welfare".
Uruguay	"Those information assets necessary to ensure and maintain the correct functioning of services vital to the operation of the government and the economy of the country" (Critical Information Assets of the State)

It is important to point out that after an in-depth study of the totality of the definitions of CII listed, we observe that most of them are composed of four parts, detailed as follows:

Table 6: CII definition components

COMPONENTS	ATTACKS	PLACE	AREAS OF IMPACT
In this section the definition refers to the elements (technological or not) that are present in the CII. The elements can be mentioned under generic terms, with specific examples, or both.	In this section the definition refers to forms or actions that may affect the components.	In this section the definition refers to the place or space where the consequences of the attack are manifested.	Areas or values affected by attacks on CII.

These categories will help us to better identify CII elements in Section 2 where we will map each element, both from a global and from a regional perspective.

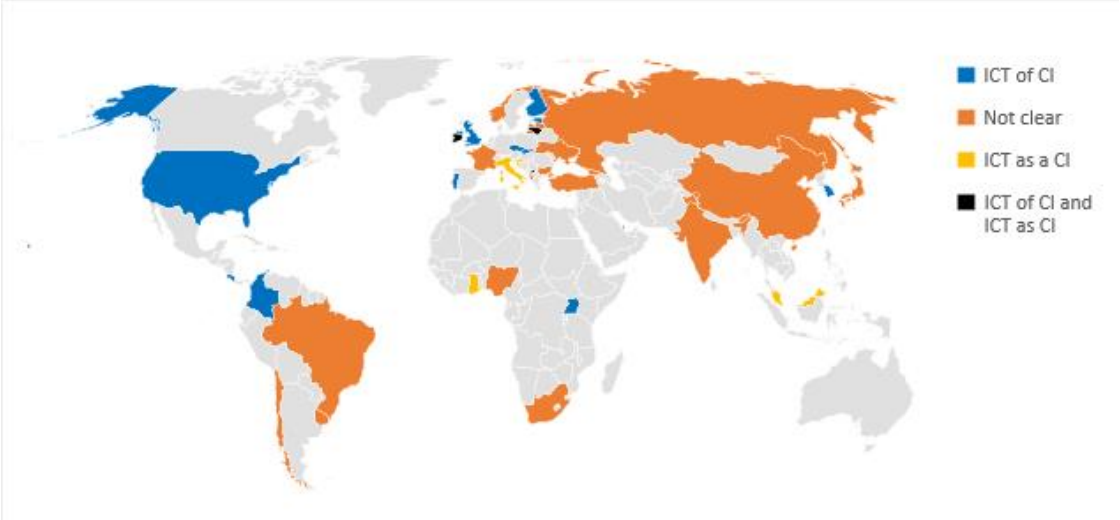
SECTION 2: GLOBAL AND REGIONAL CII MAPPING APPROACH

In this section we present a mapping of the global and regional CII. The first part (2.1) reviews all of the CII definitions presented in Section 1.4 and presents different figures and maps that show statistics and categories related to them. The second part (2.2) reviews all of the CII definition results presented in Section 2.1 and presents maps, figures and tables, from a regional perspective. In both parts, the mapping approach takes into consideration the four elements of a CII definition, namely; components, attacks, place, and areas of impact.

2.1 GLOBAL APPROACH

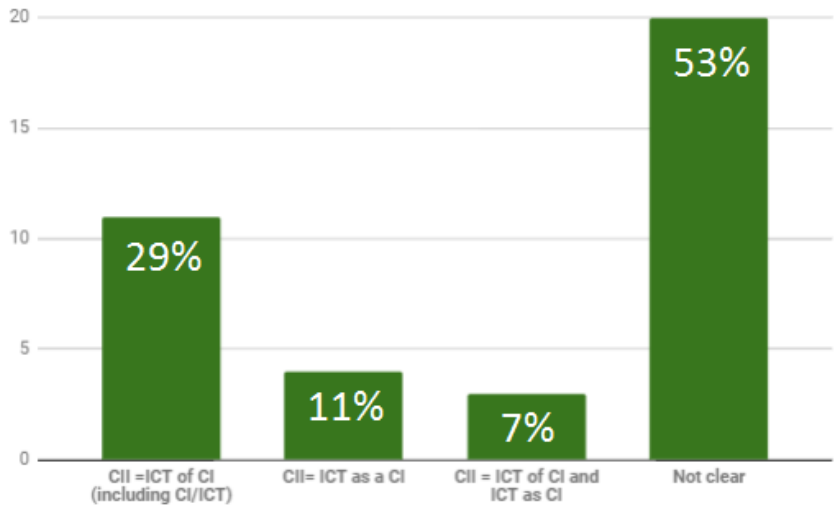
As Table 6 illustrated, the list of CII definitions encompasses four elements, namely; components, attacks, place and areas of impact. As a preliminary step, we identified within the 38 definitions, that the perception of the CII as defined by countries, was related to four categories: (i) CII is equal to an ICT critical infrastructure (ICT as a CI), (ii) CII are the ICT component of a critical infrastructure – including those that consider ICT as a CI; (iii) CII are critical infrastructures by themselves as well as the ICT component of other critical infrastructures and (iv) it was not clear to which category the definition was referring. The results of these perceptions is illustrated as follows:

Figure 2: Global relationship between CII and CI



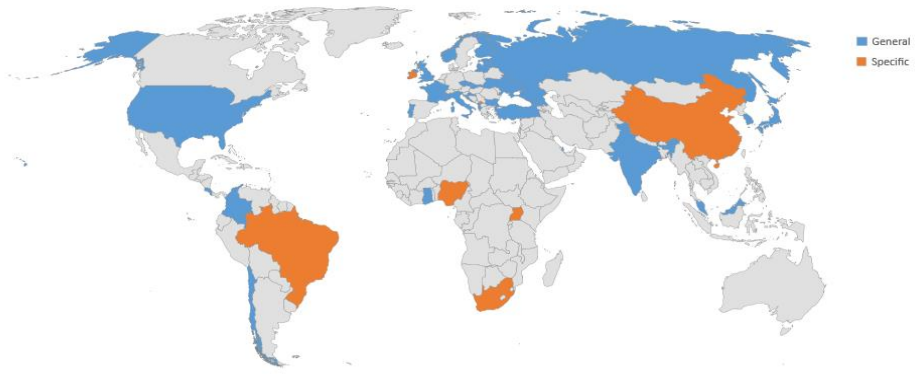
The map shows that most of the countries have definitions that are not clear about the relationship between CI and CII. In the other cases, the wording of the definition allowed us to identify which category CII belong to. Below, we present the corresponding percentages:

Figure 3: Global categorisation of CII



Once we had identified in each definition the relationship between CI and CII, we identified those country's definitions where the components of a CII, (components understood as those elements -technological or not - that are present in the CII), were defined in a generic or specific manner by the countries. It seems necessary to draw attention to the fact that the majority of the approaches led to the non-designation of specific elements of CII. Among the 38 definitions, only seven countries referred to CII components in a specific manner.

Figure 4: Countries in which CII definition refers to components only in general terms and countries that include specific examples



We observe that only Ireland, Kosovo, China, Nigeria, South Africa, Uganda and Brazil, have mentioned in their definitions, one or more specific elements that they considered to be part of a CII. The following table shows the percentage of elements mentioned within their definitions:

Table 7: Specific CII components

Telecommunication networks	10%
Internet	10%
Terrestrial wireless networks	5%
Satellites	10%
Computers	5%
Software	10%
Data	5%
Traffic data	5%
Databases	5%
People	15%
Buildings	5%
Mean of data storage	5%
Internet applications	10%

Those countries that have mentioned CII components only in a generic manner, have opted for a vague or too broad terminology. This makes it difficult to tell precisely which part of the element mentioned is critical, or, if the whole element is considered CII by the country. The next table enumerates all the elements mentioned in the definitions and the number of times that these elements were mentioned.

Table 8: Generic CII components

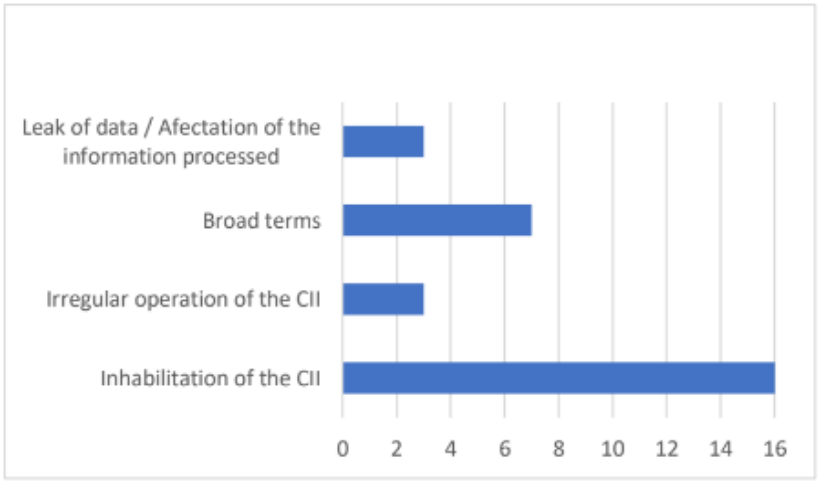
Information systems	10
Systems	7
Services	5
Networks	3
Infrastructure	5
Channels	1
Communication systems	3
IT infrastructure	2
Electronic communication networks	2

Industrial control systems	1
IT systems	3
Information/Communication services	1
Information and Communications technologies	2
Information networks	3
Communication/telecommunications networks	3
Electronic Information Resources	1
Facilities and functions	3
Business	1
Electronic systems	1
Assets	6
Automated control systems	1
Computer resources	1

We observe that those definitions that opt to use generic language with respect to the CII elements make it difficult to clearly identify which assets, services or elements should be considered "critical". Subsequently, general references such as "systems" or "networks" and their interdependence makes it difficult to identify government priorities or how the elements are perceived as key parts of their CII. As a preliminary conclusion, it could be stated that vague definitions of CII elements might hamper the development of security measures or specific policies.

Later we saw how many CII definitions make reference to attacks (attacks understood as actions that may affect the components.) It should be noted that 53% of the definitions make reference to the form of attacks or incidents, as Figure 5 illustrates:

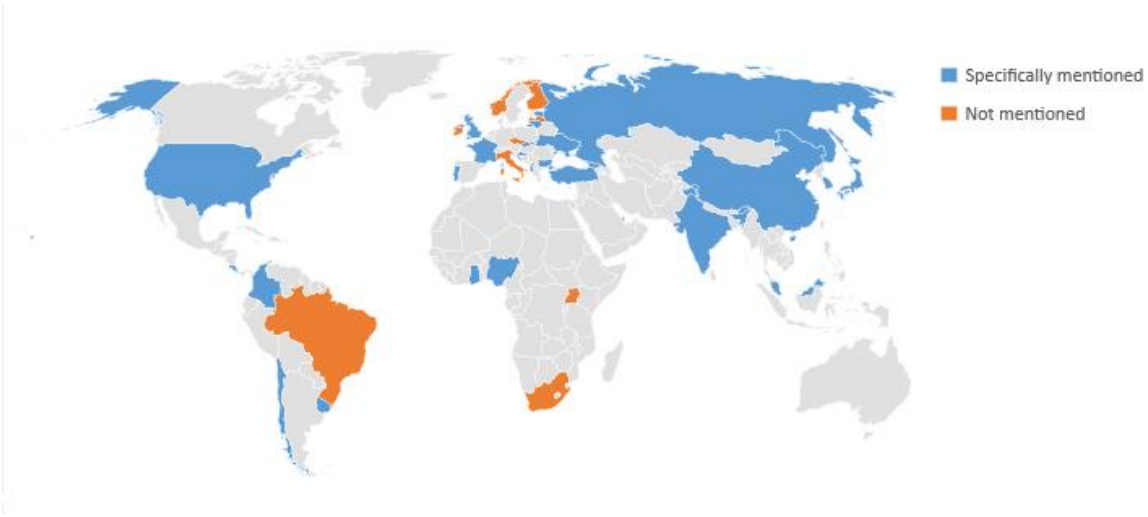
Figure 5: Form of attacks to CII



Looking at this list of potential threats, we can observe that the assessment of the threats tends to be case-specific, allowing a number of factors to be involved. It should also be noted that, in general terms, governments' CII definitions tend to take an "all hazards approach" which includes incidents, threats, irregular operations or deliberate attacks.

Most definitions specifically mention the component place, i.e. the site or space where the consequences of the attacks are manifested within their text, indicating that this consequence would occur on their national territory.

Figure 6: Consequence of the CII incident would occur in the national territory



Next, we inquired about the areas or values affected by attacks on CII (areas of impact). Figure 7 shows those countries which have a specific mention of areas of impact and Figure 8 maps the specific content of those areas impacted:

Figure 7: Definition does refer to areas of impact

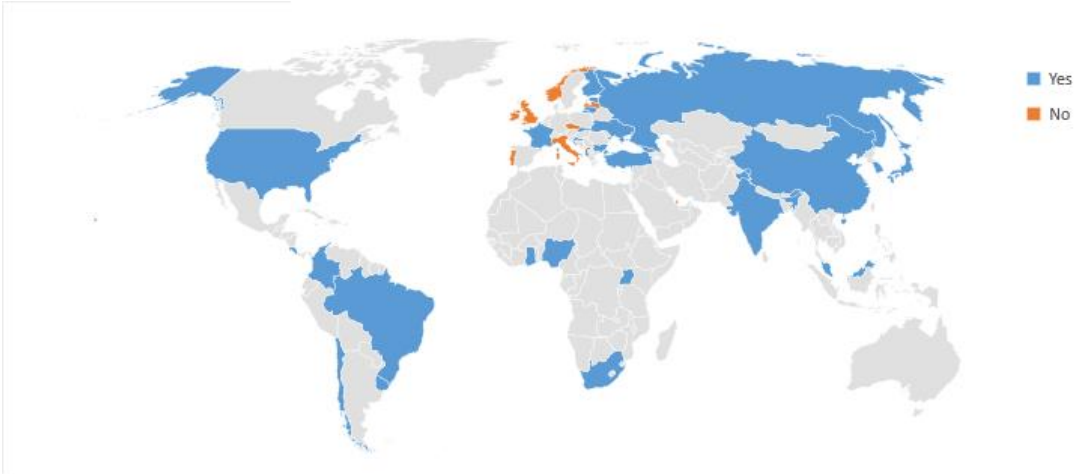
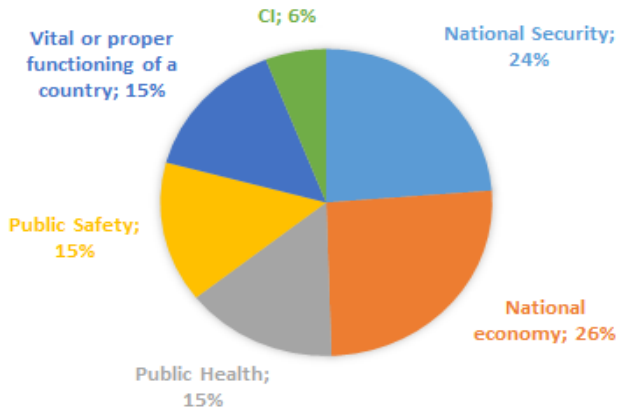


Figure 8: Detail of areas of impact

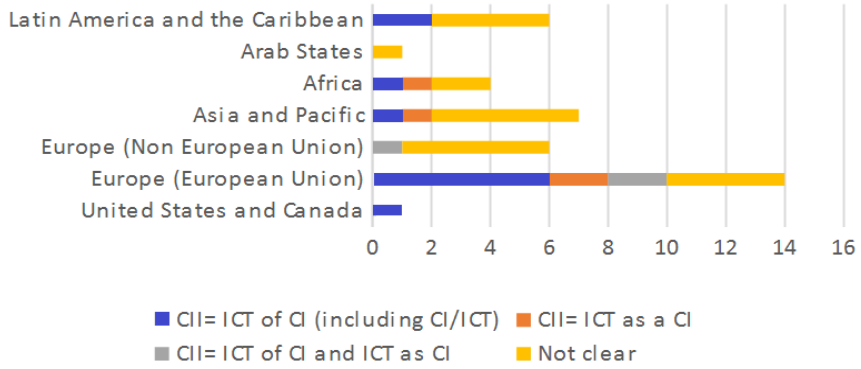


Both national security and the economy are considered by States as the highest-priority values that might suffer an impact when CII are attacked, with the national economy at the top of the list. With regard to the national economy, definitions do not indicate if the impact is on the private sector, the public sector, or both. Finally, public safety and public health are considered important values to be protected.

2.2 REGIONAL APPROACH

We identified within the regions, that the perception of the CII was related to the four types of categories mentioned in 2.1.The results of these perceptions is illustrated as following:

Figure 9: Relationship between CII and CI by region



Once we had identified regional results with regard to the relationship between CI and CII, we observed those regions where the components of a CII (components understood as those elements - technological or not - that are present in the CII) were defined in a generic or specific manner. There was very little designation of specific elements of CII using the regional approach.[160] The following table shows the percentage of elements mentioned within the 7 regions.

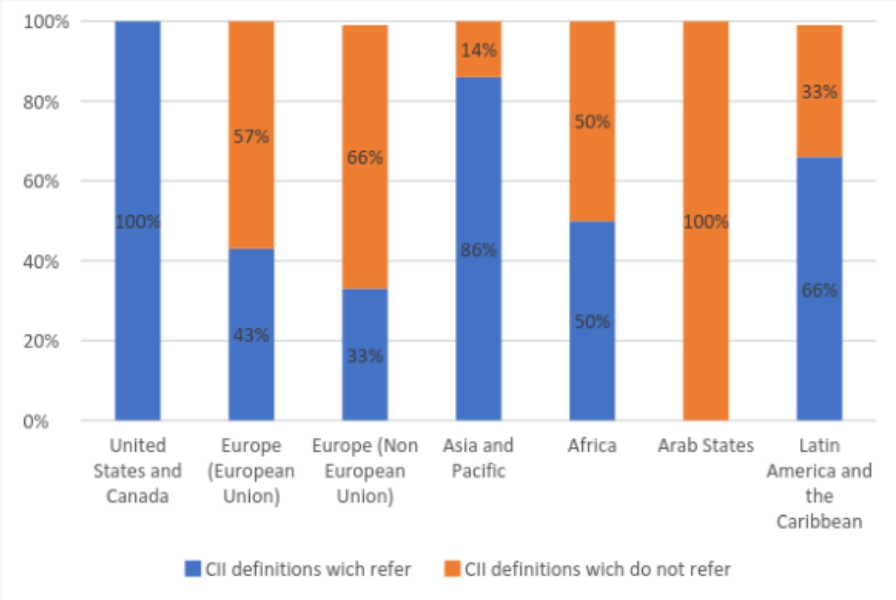
[160] Only Ireland, Kosovo, China, Nigeria, South Africa, Uganda and Brazil have mentioned in their definitions, one or more specific elements that their considered as part of a CII

Table 9: Regions where CII definitions refer to components only in general terms and regions that also include examples

Region	General	Specific
United States and Canada	1	0
Europe (European Union)	13	1
Europe (Non European Union)	5	1
Asia and Pacific	6	1
Africa	2	3
Arab States	1	0
Latin America and the Caribbean	4	1
TOTAL	32	6

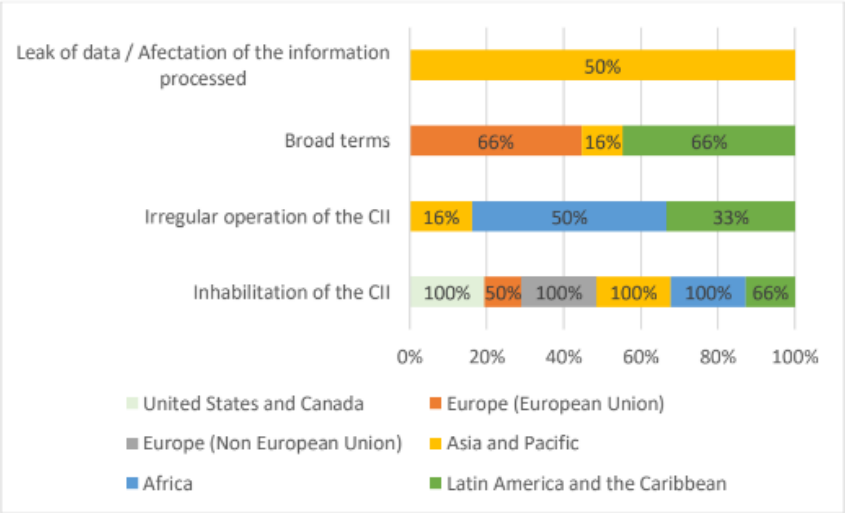
Then, we calculated the percentage by region of references to the forms of attack, whose percentages are presented in Figure 10:

Figure 10: Regions where CII definitions refer to attacks



Next, we illustrated the different forms of attacks (attacks understood as forms or actions that may affect the components) by region:

Figure 11: Form of attacks mentioned



Later, we explored global results related to CII impacts and divided them into regions. Table 10 exposes those regions with a specific mention of areas of impact and Table 11 maps the specific content of those areas impacted.

Table 10: Consequences of the CII incident would occur in the national territory (by region)

Region	Specifically mentioned	Not mentioned
United States and Canada	1	0
Europe (European Union)	9	5
Europe (Non European Union)	4	2
Asia and Pacific	7	0
Africa	2	2
Arab States	1	0
Latin America and the Caribbean	4	1
Total	**28**	**10**

Table 11: Regional detail of areas of impact related to CII

Region	National Security	National economy	Public Health	Public Safety	Vital or proper functioning of a country	CI
United States and Canada	1	1	1	1	0	0
Europe (European Union)	4	4	0	1	6	2
Europe (Non European Union)	2	3	3	2	2	0
Asia and Pacific	6	5	3	4	2	0
Africa	2	3	3	2	0	1
Latin America and the Caribbean	2	3	1	1	1	1
Total	**17**	**19**	11	11	11	4

The overall result shows again that both national security and the national economy are considered to be the areas that might suffer the largest impact when any CII are attacked.

Thus far, we have presented a global and regional mapping and analysis of CII definitions. In section 3, we will investigate the relationships between the CI, CII, interdependencies and their international implications.

SECTION 3 : TRANSNATIONAL CRITICAL INFRASTRUCTURES

This section aims to introduce the concepts of transnational critical infrastructures (TCI) as well as the relationship between CI and the TCI. To this end, we first sent out a short survey to the different governmental offices listed in Annex A, which contained CII policy-oriented questions in order for us to gather information related to CII, TCI and related topics. We have received few answers but we certainly expect more feedback in the near future. For the moment, such answers did not provide us with additional information outside of what is already contained in our literature review and data analysis. For this reason, instead of incorporating those answers in this section, we decided to take an approach to the TCI subject from a theoretical point of view and from consultation of normative sources.

3.1 FROM CI TO TCI. EXAMPLES

We have already observed in Section 1 that cyber-attackers use network interconnection to perform their unlawful acts and that in many cases, the site where the attack happens is independent of the presence and location of the attackers who perpetrated it. In this sense, it is possible to argue that many cyber-offences are international and that the existence of cross-border threats is becoming, increasingly, an inevitable challenge for CI. In this sense, international infrastructure dependency and interdependency may affect citizens and critical national services. However, the international elements of CI and the networks where those cyber-attacks take place have not been defined by research or governmental bodies yet. Therefore, the question arises: should the CI also be considered as transnational critical infrastructures (TCI)?

So far, this new form of international critical infrastructures has been addressed or referred to using alternative terms, such as cross-border critical infrastructures, nation-wide critical infrastructures, or European Critical Infrastructures. Below are some examples:

- In an OECD report,[161] Australia, Canada, Japan, Korea, the Netherlands, the United Kingdom, and the United States identified the major cross-border challenges for the protection of critical information infrastructure, recognizing "the need for international cooperation, a national operational infrastructure security capability, a willingness and ability to share information, close co-operation with the relevant parts of the private sector, a legal framework against cybercrime, and a strong culture of security in the face of rapid technological growth, and consequential social changes" (OECD 2007, 5). A common approach of these countries was to involve the private sector owners and operators of critical information infrastructure in future discussions.
- Another example is the recognition of the interconnected nature of critical infrastructure made by the governments of Canada and United States in their Action Plan for Critical Infrastructure.[162] Through this plan, they established a coordinated, cross-border approach which called for joint sector meetings and collaborative risk

[161] The report is based on two studies conducted in 2006 and 2007 and offers an analysis of the critical information infrastructure security policies

[162] https://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf

management activities. The plan also supported regional cross-border relations and encouraged cooperation among State, provincial, and territorial authorities (Public Safety Canada 2010, 3).

- Additionally, the European Programme on Critical Infrastructure Protection (EPCIP) refers to the CI from a regional perspective, therefore beyond the national countries. The EPCIP provides network-based guidelines for member States to identify critical infrastructure assets. It should be pointed out that an asset may only be designated as European critical infrastructure if it complies with a four steps criterion and additionally if it is approved as such by the member state in whose jurisdiction it is located. If the member state disagrees with the critical infrastructure asset designation, then the asset is not deemed as critical infrastructure, even if it meets all the criteria involved.[163]
- Finally, the U.S. Critical Foreign Dependencies Initiative annually compiles and updates a comprehensive inventory of CI and key resources that are located outside U.S. borders and whose loss could critically impact the public health, economic security, and/or national and homeland security of the United States. Clemente argues that the project is part of the larger National Infrastructure Protection Plan (NIPP), and is essentially an international version of the Department of Homeland Security National Asset Database (Clemente 2013, 21).

Despite the examples presented, it should be noted that there are two particular cases that make reference to the existence of a global information infrastructure (GII). This is the case of the International Telecommunication Union and the government of the United States of America, as the following table shows:

Table 12: GII definitions

Date	Definition of Global Information Infrastructure (GII)	Source
March 2000	A collection of networks, end user equipment, information, and human resources which can be used to access valuable information, communicate with each other, work, learn, receive entertainment from it, at any time and from any place, with affordable cost on a global scale.	ITU-T Y.101. Global Information Infrastructure terminology: Terms and definitions
October 2007	The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure.	The US Department of Defense, Department of Defense Dictionary of Military and Associated Terms, Joint Publication No. 1-02

[163] The European Programme for Critical Infrastructure Protection provides guidance for critical infrastructure risk management efforts in Europe. The program fulfils the requirements set forth by European Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. The program scope is limited to the transportation and energy sectors, and calls for all-hazards consideration in critical infrastructure protection efforts.

It is then possible to argue that the above examples may be addressed as international or TCI, which could be described as those infrastructures identified as critical, not only because of their particular elements but also because of the cascading effects that their disruption may cause on other infrastructures. TCI dependency should be seen as an important factor, since disruptions of an infrastructure in one nation may have serious effects in other nations (RECIPE 2011, 27). The conception of a CI as transnational allows that, in the event of a crisis or attack, one State can be addressed by another State even if the latter did not suffer a direct attack. This new scenario might also cause repercussions in international economic cooperation: since some CI are nationwide, operators and economic agents could be required to cooperate at a regional and international level for reasons of efficiency, interoperability and risk management in case of a cyber-attack (Olesen 2017, 260-261). Subsequently, "the addition of a cross-border dimension to this paradigm by means of an extraterritorially located essential 'asset, system, or part thereof' not merely adds a further element of complexity to the system, but also increases the diversity of actors required to manage it" (Kaska and Trinberg 2015, 15).

This new TCI scenario highlights global interdependencies that might redefine the CI, which "challenges the notions of national sovereignty and forces policy-makers to reconsider the tensions inherent in this highly optimized yet fragile system of physical, logical and social connections" (Clemente 2013). A clear attribution of competencies and responsibilities and the recognition of events and circumstances beyond the capacity of action or a single nation could, for instance, facilitate cross-border policy issues (OECD 2007, 4).

In addition, it should be pointed out that one of the least explored areas of cyber vulnerabilities concerns cross-border or transnational critical information infrastructure (TCII). Nevertheless, the provision of vital services such as banking or telecommunications is increasingly reliant on such infrastructures which may be also located in another country or may have a critical dependency on systems outside of a country's jurisdiction (Kaska and Trinberg 2015, 7). This trend is expected to continue alongside globalization, and future research will have to acknowledge the relationship between CII and technologically-driven business practices such as the adoption of cloud computing services over the Internet, as they might constitute a target for cyber-attacks. As Abele-Wigert and Dunn argues, "it is becoming increasingly important to enhance the security of communication networks and information systems. This urgency is due to their invaluable and growing role in the economic sector, their interlinking position between various infrastructure sectors, and their essential role for the functioning of many of the critical services that are essential to the well-being of developed societies" (Abele-Wigert and Dunn 2006, 27).

To sum up, it can be argued that the borderless and transnational nature of cyberspace is enabling many forms of criminality that can disrupt digitally-interlinked and interdependent CI and CII.

CONCLUSION

The main purpose of this research was to present a map of international approaches to CII to serve as a framing device to help experts identify and share areas of study in the field of cybersecurity. Moreover, it introduced the concepts TCI as well as the relationship among CI, CII ad TCI. We have presented the results of a review of currently available CII definitions, which allowed us to model their taxonomy, characteristics and core elements at a global and regional level.

Mapping roles and responsibilities and understanding thresholds for cross-border cooperation within CI, CII and TCI across countries is complex due to the involvement of different cultures and political conceptions. In this sense, we understand that no study about the complex phenomenon of CII can be undertaken without looking at their corresponding definitions as it is essential to understand what constitutes critical information infrastructure and why it is so difficult to afford them adequate protection.

We have found many similarities related to CII elements which led us to understand that there is a great opportunity to develop international co-operation. CII constitute an important source of interdependencies; therefore the need to address vulnerabilities requires greater flexibility, awareness as well as the specific commitment to surveilling and protecting both publicly- and privately-owned infrastructure.

We have also observed that a number of governments have shown their interest in the protection of their CII, by allocating resources to national CII offices. We understand that the ambiguity about what constitutes a CII could lead to the inefficient use of limited homeland security resources.

With regard to TCI, there are few national strategy documents or academic texts that emphasize the importance of the topic. In this sense, we have observed that an established, commonly accepted, discernible approach to cross-border CII dependencies is currently lacking and examples of legal and regulatory measures to mitigate the risks arising from CII located outside of national territory are almost non-existent.

Cyber-enabled critical infrastructure dependencies spread across national boundaries and become global. Stakeholders should expand and strengthen their cross-border efforts to ensure that the globally-connected critical infrastructure is both secure and resilient.

BIBLIOGRAPHY

Abele-Wigert, Isabelle and Dunn, Myriam. 2006. International CIIP Handbook 2006 Vol. I. Zurich: Center for Security Studies.

Clemente, Dave. 2013. Cyber Security and Global Interdependence. What Is Critical? Great Britain: Chatham House.

Colesniuc, Dan. "Cyberspace and Critical Information Infrastructures". Informatica Economica Vol. 17, no. 4 (2013): 123-132.

Counter-Terrorism Committe Executive Directorate (CTED), United Nations Security Council. 2017. Physical protection of critical infrastructure against terrorist attacks. Available in https://www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-8-March-2017-Final.pdf.

European Union Agency For Network And Information Security (ENISA). 2014. Methodologies for the identification of Critical Information Infrastructure assets and services. Available in https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis/at_download/fullReport.

European Union Agency For Network And Information Security (ENISA). 2016. The cost of incidents affecting CIIs. Available in https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis/at_download/fullReport.

Geers, Kenneth. 2011. Strategic Cyber Security. Tallinn: CCD COE Publication.

Kaska, Kadri and Trinberg, Lorena. 2015. Regulating Cross-Border Dependencies of Critical Information Infrastructure. Tallinn: CCD COE Publication.

Kenneth, Juster I. and Tritak, John S. 2002. "Critical Infrastructure Assurance: A Conceptual Overview". Security in the Information Age. Washington DC: White House.

Koops, Bert-Jaap. "Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research". Combatting Cybercrime and Cyberterrorism. (2017): 3-16.

Lazari, Alessandro. 2014. European Critical Infrastructure Protection. Switzerland: Springer International Publishing.

Luiijf, Eric A.M. 2006. "How to prepare for the next waves of Information Assurance issues". Proceedings of the Euro-Atlantic Symposium on Critical Information Infrastructure Assurance. Available in https://www.researchgate.net/publication/242667474_How_to_prepare_for_the_next_waves_of_Information_Assurance_issues.

Luiijf, Eric et al. 2016. The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers. Available in https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf.

Olesen, Nina. "European Public-Private Partnerships on Cybersecurity". Combatting Cybercrime and Cyberterrorism. (2016): 259-278. Switzerland: Springer International Publishing.

Organisation for Economic Co-operation and Development (OECD). 2007. Development of Policies for Protection of Critical Information Infrastructures. Available in https://www.oecd.org/sti/40761118.pdf.

Organisation for Economic Co-operation and Development (OECD). 2008. Protection of 'critical infrastructure' and the role of investment policies relating to national security. Available in https://www.oecd.org/investment/investment-policy/40700392.pdf.

Public Safety Canada. Action Plan for Critical Infrastructure 2014-2017. Available in https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/pln-crtcl-nfrstrctr-2014-17-eng.pdf.

Recommended Elements of Critical Infrastructure Protection for policy makers in Europe (RECIPE). 2011. Good practices manual for CIP policies. Available in

http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/FINAL_RECIPE_manual.pdf.

Rinaldi, Steven M., Peerenboom, James P. and Kelly, Terrence K. "Complex Networks, Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies". IEEE Control Systems Magazine. (2001): 11-25.

Sharma, Munish. 2017. Securing Critical Information Infrastructure, Global Perspectives and Practices. New Delhi: Institute for Defence Studies and Analyses.

Suter, Manuel. 2007. A Generic National Framework For Critical Information Infrastructure Protection (CIIP). Available in https://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf.

Tadjibayev, Furkhat and Sattarova, Feruza. "Categorization of Critical Infrastructures and Critical Information Infrastructures". International Journal of Advanced Science and Technology, Volume 8. (2009): 19-26.

TENACE Project. 2014. Critical Infrastructure Protection: Threats, Attacks and Countermeasures. Available in http://www.dis.uniroma1.it/~tenace/download/deliverable/Report_tenace.pdf.

World Economic Forum (WEF). 2016. The Global Risks Report 2016, 11th Edition. Available in http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf.

ANNEX

LINKS TO CII DEFINITIONS	
United States of America	https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf
Bulgaria	http://www.cyberbg.eu/doc/20161024_Cyber_strat_proekt.pdf
Croatia	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/croatian-cyber-security-strategy/view/++widget++form.widgets.file/@@download/Croatian+National+Cyber+Security+Strategy+-+2015.pdf
Czech Republic	https://www.govcert.cz/download/legislation/container-nodeid-1122/actoncybersecuritypopsp.pdf
Estonia	https://www.ria.ee/en/ciip.html
Finlandia	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf
France	https://www.ssi.gouv.fr/entreprise/glossaire/s/
Ireland	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf
Italy	http://www.vigilidelfuoco.gov.it/aspx/ReturnDocument.aspx?IdDocumento=2832
Latvia	http://www.dvi.gov.lv/en/legal-acts/law-on-the-security-of-information-technologies/
Lithuania	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf
Lithuania	https://www.e-tar.lt/portal/en/legalAct/5468a25089ef11e4a98a9f2247652cf4
Portugal	https://www.cncs.gov.pt/recursos/glossario/
Slovakia	http://www.nbu.gov.sk/wp-content/uploads/cyber-security/Cyber-Security-Concept-of-the-Slovak-Republic-for-2015-2020.pdf
United Kingdom	http://www.parliament.uk/documents/post/postpn389_cyber-security-in-the-uk.pdf
Albania	http://www.akce.gov.al/wp-content/uploads/2016/04/Dokumenti%20i%20Politikave%20per%20Sigurine%20Kibernetike%202015-2017.pdf
Georgia	http://www.dea.gov.ge/uploads/GISA_ENG_FINAL_2015_ver.pdf

Kosovo	http://www.kryeministri-ks.net/repository/docs/National_Cyber_Security_Strategy_and_Action_Plan_2016-2019_per_publikim_1202.pdf
Norway	https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/cyber_security_strategy_norway.pdf
Turkey	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/TUR_NCSS.pdf
Ukraine	http://cert.gov.ua/pdf/NationalCyberSecurityStrategy.pdf
China	http://politics.people.com.cn/n1/2016/1227/c1001-28980829.html
China	http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm
India	http://www.eprocurement.gov.in/news/Act2008.pdf
Japan	http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3_r1.pdf
Korea	https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=38785&type=part&key=43
Russia	https://cis-legislation.com/document.fwx?rgn=98928
Ghana	https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Ghana_Cyber-Security-Policy-Strategy_Final_0.pdf
Nigeria	https://cert.gov.ng/images/uploads/CyberCrime_(Prohibition,Prevention,etc)_Act,_2015.pdf
South Africa	http://pmg-assets.s3-website-eu-west-1.amazonaws.com/docs/100219cybersecurity.pdf
Uganda	http://www.nita.go.ug/sites/default/files/publications/National%20Information%20Security%20Policy%20v1.0_0.pdf
Qatar	http://www.ictqatar.qa/sites/default/files/national_cyber_security_strategy.pdf
Brazil	http://dsic.planalto.gov.br/legislacao/2_Guia_SICI.pdf
Chile	http://ciberseguridad.interior.gob.cl/media/2017/04/NCSP-ENG.pdf
Colombia	https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
Costa Rica	https://micit.go.cr/images/imagenes_noticias/10-11-2017__Ciberseguridad/Estrategia-Nacional-de-Ciberseguridad-de-Costa-Rica-11-10-17.pdf
Trinidad & Tobago	https://www.sites.oas.org/cyber/Documents/Trinidad%20and%20Tobago%20-%20National%20Cyber%20Security%20Stategy%20(English).pdf
Uruguay	https://www.cert.uy/wps/wcm/connect/certuy/2b1721ca-ef15-4020-9dae-0b76da5fee78/Decreto+No.+451_009.pdf?MOD=AJPERES

COUNTERING THE PROLIFERATION OF OFFENSIVE CYBER CAPABILITIES

Mr. Robert Morgus, *Cybersecurity Initiative & International Security Program, New America*

Mr. Max Smeets, *Centre for International Security and Cooperation (CISAC), Stanford University*

Mr. Trey Herr, *Harvard Kennedy School*

MEMO №2

TABLE OF CONTENTS

SECTION 1: INTRODUCTION

The tenor of the cyber stability debate, often moribund and moving more sideways than forward, changed with the 2010 United Nations Governmental Group of Experts (UN GGE) Consensus Report that international law applied to cyberspace.[164] It followed a position paper by the Obama administration published in January of that year to bring the various sides closer together. Though it wasn't a steep trend line which followed, the slow process towards cyber norms was considered to be meaningful and positive.[165]

Despite this and subsequent progress, however, the events of 2017 have shed doubt on this progressive dynamic. The collapse of the UN GGE process in June sent an alarming message that we are moving *away* from establishing a meaningful cyber stability regime, rather than towards it. Moreover, global cyber attacks, such as WannaCry and NotPetya, once again demonstrated the destabilizing potential of the proliferation of cyber capabilities.[166]

Norms and legal interpretations are one way to bring order to international society.[167] The purpose of this policy report is to offer a new set of recommendations, derived from a clear framing of the proliferation process and likely to contribute to meaningful progress toward cyber stability at the international level. Over the past decade a great deal of time, energy, and precious focus has been dedicated to developing norms of responsible behavior—what states and other international actors *should* and *should not* do in cyberspace. But this is only half of the conversation. Progress against proliferation must also consider what groups *can* and *cannot* do. In short, time is ripe to explore countering the proliferation of offensive cyber capability. This leads to our core research question: what are the key facets of the ecosystem that facilitates the proliferation of offensive cyber capability?

This policy report provides a framework for mapping the process of proliferation in cyberspace and its implications for states and policymakers, with the aim of understanding how to better counter it. In our analysis we introduce the Transfer-Actors-Capabilities-Effects (TrACE) framework, which helps to explain the dynamics of proliferation in cybersecurity and serves as an intellectual basis for counterproliferation efforts by the policy community. This framework captures how proliferation occurs between a diversity of actors and encompasses three overlapping activities: i) the purchase and sale of individual malicious software information and individual components that contribute to the development of offensive cyber capabilities, ii) continued research and innovation by a small set of

---

[164] Note that there were already already signs of this change in 2008. See: John Markoff, "Step Taken to End Impasse on Cybersecurity Talks," *The New York Times*, (July 17 2010) retrieved from: http://www.nytimes.com/2010/07/17/world/17cyber.html?mcubz=0.

[165] Michael Schmitt and Liis Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms", *Just Security*, (June 30, 2017), retrieved from: https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

[166] Victory Woollaston, "WannaCry ransomware: what is it and how to protect yourself," *Wired* (May 22, 2017), retrieved from: http://www.wired.co.uk/article/wannacry-ransomware-virus-patch; Andy Greenberg, "The Wannacry Ransomware Hackers Made Som Real Amateur Mistakes," *Wired*, (May 15, 2017), retrieved from: https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/; Lily Hay Newman, "Latest Ransomware Hackers Didn't Make Wannacry's Mistakes," *Wired*, (June 27, 2017), retrieved from: https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/.

[167] See Hedley Bull, *The Expansion of International Society.*

advanced states, and iii) the inadvertent transfer of capabilities—both sophisticated and not—to non-state groups and less capable states.

Applying the model to counterproliferation efforts, we indicate that *current* feasibility of international agreements is low. The implementation of export controls could weaken defense more than offense.[168] Also, arms control agreements are not conceived to be an effective path due to the current infeasibility of setting and enforcing standards of behavior. The feasibility of such interventions in the future, however, remains unclear.

We find that, in the short term, institutional tools that could be leveraged unilaterally or within like-minded coalition are more feasible. This includes the enhancement of both defensive and offensive capabilities, as well as the (further) implementation of a diplomatic toolbox.[169]

Our recommendations are therefore aimed at increasing the cost of developing offensive cyber capabilities, diminishing the utility of capabilities in the hands of troublesome actors once spread, and providing a way forward for meaningful action on increasing the barriers to actors transferring these capabilities.

The remainder of this report proceeds as follows. Section II sets out the scope of our analysis. Section III discusses the objectives in counterproliferation. In section IV, we provide an overview of the TrACE framework to explain cyber proliferation dynamics. Section V, in turn applies the TrACE framework to counterproliferation efforts, outlining a range of connected initiatives, tackling all processes within proliferation. The final part, Section VI, concludes and provides a list of recommendations for policymakers.

---

[168] Trey Herr, "Malware Counter-Proliferation and the Wassenaar Arrangement," in *2016 8th International Conference on Cyber Conflict: Cyber Power* (CyCon, Tallinn, Estonia: IEEE, 2016), 175–90, https://ccdcoe.org/cycon/2016/proceedings/12_herr.pdf.

[169] We note that the manipulation of the market through purchasing power will be more difficult in the current environment.

SECTION 2: SCOPE OF ANALYSIS

This section clarifies the scope of our analysis. The call for counterproliferation of offensive cyber capabilities is not new. Indeed, the potential control of "intrusion software" was embedded in the Wassenaar Arrangement aimed at "creating consensus approach to regulate conventional arms and dual-use goods and services."[170] Our approach differs significantly from previous efforts which primarily sought to counter cyber proliferation through imposing standards *like* Weapons of Mass Destruction (WMD) prevention programs.[171]

Although there may be valuable lessons to learn from the WMD approach, we argue that this approach on its own is *not* viable.[172] After all, cyber proliferation is embedded in a unique ecosystem of actors and information.[173] Previous efforts have focused on blocking the flow of cyber capabilities without developing a detailed understanding of the *mechanisms* of cyber proliferation. The starting point of our analysis is that we can only find ways to counter the spread of these capabilities if we know *how* they spread.[174] We also need to be much clearer about the objectives of a counterproliferation effort. While a "cyber-weapon-free" world is unlikely, it should provoke debate over what goals are feasible in the near to mid-term.

There are four assumptions underlying this paper. First, we assume that countering the proliferation of offensive cyber capabilities is a useful activity in the context of cybersecurity.[175] Moreover, we believe that counterproliferation is a *necessary* activity for the maintenance and improvement of international stability.

---

[170] See: "About us", Retrieved from: http://www.wassenaar.org/about-us/

For an excellent basic overview see: Cristin Flynn Goodwin and Brian Fletcher, "Export Controls and Cybersecurity Tools: Renegotiating Wassenaar," Marina Bay Sands, (July 20-22, 2016) retrieved from: https://www.rsaconference.com/writable/presentations/file_upload/fle1-r01_export-controls-and-cybersecurity-tools-renegotiating-wassenaar.pdf

[171] Also see Greenberg's review of Clarke and Knake's proposal of a 'Cyber War Limitation Treaty'. See: Andy Greenberg, "Weapons of Mass Disruption," *Forbes*, (April 8, 2010), retrieved from: https://www.forbes.com/forbes/2010/0426/opinions-cyberwar-internet-security-nsa-ideas-opinions.html; Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, (HarperCollins: 2010)

[172] Trey Herr, "Governing Proliferation in Cybersecurity," *Global Summitry* 2, no. 1 (July 2017), https://academic.oup.com/globalsummitry/article/doi/10.1093/global/gux006/3920644/Governing-Proliferation-in-Cybersecurity?guestAccessKey=f88e2727-737a-4be2-991e-a3696624b420.

[173] For a discussion of the limits of the 'cyberspace ecosystem' metaphor see: Alexander Klimburg, *The Darkening Web: The War for Cyberspace*, (New York: Penguin Press: 2017)

[174] Note that, in the case of the Wassenaar agreement, there was also said to be a lack of technical expertise—partially because governments had no prior history of engaging with issues related to cyber security. For similar point see: Goodwin and Fletcher, "Export Controls and Cybersecurity Tools"

[175] There has been a vivid debate on nuclear proliferation on whether 'more may be better'. Waltz' famous logic on why the spread of nuclear weapons likely contributes to further stability was based on a number of propositions: i) nuclear states can only score small victories due to a fear of escalation, ii) the escalation costs are extremely high; iii) there is

Second, we define "cyber weapon" narrowly in this context but recognize that any analysis of proliferation must take more than this tiny sub-set of capabilities into account. A cyber weapon is any software which can cause destructive physical effects.[176] Offensive cyber capabilities, which are a wider category of which weapons are a subset, may also include software which causes destructive logical or digital effects. Cyber proliferation refers to the intentional *or* unintentional diffusion of offensive cyber capabilities between actors to cause effects through information systems or networks. This means our analysis addresses a range of capabilities which, while not weapons by any reasonable definition, could be combined to create destructive effects.

Third, our analysis does not consider the tools or services used to propagate narratives in information and influence operations. However, the tools which are used to *obtain* confidential information leveraged in information and influence operations do fall under this discussion.

Finally, this counterproliferation approach is not meant to *replace* ongoing international activities around the codification and enforcement of normative behavior and the identification of deterrence structures. Instead, these two pillars work *in concert* with one another to reinforce global stability.

There are several factors which may change and thus impact this analysis. The examples and descriptions used in this framework represent a snapshot of what is currently known. As time progresses, more actors may enter the space and capability may develop to elicit new and previously unforeseen effects. Capabilities may become radically more destructive or accessible, actors who employ these capabilities may become less numerous, and the rise of computing platform vendors like Google and Microsoft could change the attacker/defender innovation cycle. Each of these changes would impact the levers used to influence proliferation and while none require radical change to our framework, we note them as potential sources of change for assumptions and descriptions of behavior in future. As these factors change, so too will factors that determine the feasibility of the counterproliferation applications of the framework outlined in the next section. Nonetheless, while the factors within the TrACE framework are malleable, the framework itself is designed to be an evergreen way of analyzing the proliferation ecosystem.

---

increased certainty about relative strength, and iv) outcome of war is more certain. Note that for the use of offensive cyber capability, these propositions are much less likely to hold; there is much less clarity on relative strength as well as the outcome of a cyber conflict. It is also unlikely that the use of offensive cyber capability is as destructive. See: Scott D. Sagan and Kenneth N. Waltz, *The spread of nuclear weapons : a debate*, (New York: W.W. Norton: 1995)

[176] For an alternative definition see: Max Smeets, "A Matter of Time: On the Transitory Nature of Cyberweapons," *Journal of Strategic Studies*, (2017)1:28

SECTION 3: THE PILLARS AND OBJECTIVES OF COUNTERPROLIFERATION

This section lays out the two pillars of counterproliferation and several potential objectives. Norms, laws, and deterrence appeal to actors' perception of what they should or should not do—they only constrain behavior as far as the threat of retroactive retribution can. In some cases, actors with capability will deem the potential retributive cost low enough to still break the norm or law and not be deterred. Counterproliferation takes this construct one step further. Certainly, it also constrains behavior by affecting the decision calculus of potential adversaries—in ways similar to those of normative, legal, and deterrent structures—but a comprehensive approach to counterproliferation goes one step further. It seeks to also limit what adversaries are capable of doing—what they can and cannot do—by taking steps to limit the spread or development of capability.

Counterproliferation in the context of weapons of mass destruction (WMD) is conventionally defined as "[d]irectly forestalling, rolling back, or eliminating efforts to proliferate [a weapon, and preventing an actor that has already obtained the weapon] from realizing any benefit from owning or employing these weapons."[177] Based on the above definition, counterproliferation involves two pillars, which can be used to guide a discussion about countering the proliferation of offensive cyber capability.

The first pillar focuses on how actors can *prevent* the acquisition or transfer of a certain weapon technology. The goal in relation to this pillar could be one of three: i) slowing, ii) limiting, or iii) stopping the spread. Regardless of the goal, this pillar does not only seek to address the spread of the finished product, but also to disrupt the independent development of capability and the spread of components that enable said development.

First, *slowing* the spread implies that spread is undesirable, but inevitable, so action is taken to forestall the development or acquisition of capability by a diverse set of actors. In conventional terms, an example of such an effort are the initiatives to stem the flow of small arms.

Second, *limiting* the spread implies that a certain subset of actors can be trusted to utilize the capability or material implicit in the capability responsibly. In these cases, efforts are made to block the transfer of capability to certain actors, while transfer to others is deemed acceptable. The efforts by the Non-Proliferation Treaty to stymie the flow of nuclear technology to states beyond those who initially developed it are a contemporary example of such an initiative.

Third, *stopping* the spread means halting any and all spread. In conventional terms, we might think of nuclear nonproliferation efforts as absolute prevention. The goal of these initiatives is to ensure that no form of nuclear capability spreads to any actor that does not already possess it.

[177] Justin Anderson, Thomas Devine and Rebecca Gibbons, "Nonproliferation and Counterproliferation," (March, 2014), retrieved from: http://oxfordindex.oup.com/view/10.1093/obo/9780199743292-0026

The second pillar focuses on how to reduce the utility of offensive capabilities already in the possession of an actor.[178] Changing this utility aims to shape decision calculus of those actors who would deploy it. There are many ways the decision calculus of an actor can be affected. This includes making it more difficult for an actor to deploy a capability, bolstering defenses to make the capability less impactful once deployed, and communicating the potential consequences of deploying a capability to one's adversary.

[178] There is no agreed upon definition of the terms "counterproliferation", "nonproliferation", and "arms control".

SECTION 4: THE TRACE FRAMEWORK

This section lays out the TrACE Framework, a parsimonious conceptual model to describe the key elements of proliferation: Transfers, Actors, Capabilities, and Effects. The purpose of the framework is to identify critical nodes in the proliferation process which provide opportunities for constructive intervention. The basic features of the framework are provided in *Table 14: Summary of TrACE framework*. What follows here is a more detailed description of each element. Along with the description of the particular components of the framework and their subcategories, we provide a non-exhaustive set of examples intended to develop better understanding, but not to provide an exhaustive or even extensive list of all known examples.

Transfers refers to the actual spread of capabilities between actors. These transfers can be *intentional* or *unintentional*.[179]

Intentional transfers describe a purposeful transaction or exchange. These could be ephemeral, as with a conference presentation, or tangible, like the rental of a botnet or the government purchase of surveillance malware from a company like BlueCoat.

Table 1: Examples of Intentional Transfer

Example	Explanation
Legitimate business sales	In some cases, companies are permitted by local laws to develop and sell what could be considered offensive cyber capability.
Criminal transfers	Criminal forums like Silk Road and AlphaBay facilitate the underground market for offensive cyber capability.
Transfers at conferences like BlackHat, DefCon, Chaos Community Congress	Sometimes, presentations at conferences or online seminars spread information about offensive capability. The intention of these presentations is generally not to spread capability to nefarious actors, but instead to prove the possibility of something to garner attention from defenders to craft fixes.
Transfers between states	Though little evidence suggests that states actively share or transfer cyber capability to one another, some traditional military and intelligence alliances are exploring avenues to do share capability.

Unintentional transfers refer to capabilities discovered and obtained through their use, such as through forensic analysis of a piece of malware, or through leaks.[180]

[179] Trey Herr, "Governing Proliferation in Cybersecurity," *Global Summitry* 2, no. 1 (July 2017), https://academic.oup.com/globalsummitry/article/doi/10.1093/global/gux006/3920644/Governing-Proliferation-in-Cybersecurity?guestAccessKey=f88e2727-737a-4be2-991e-a3696624b420.

Table 2: Examples of Unintended Transfer

Example	Explanation
ShadowBrokers	Capabilities discovered via a leak or a breach of internal security.
Duqu 2.0	Capabilities discovered through reverse engineering of previously deployed capability.

Actors are the entities responsible for developing, deploying, and defending against malicious capabilities. Our framework differentiates actors not based on their "stateness", but instead on their functional role. Thus, we break actors into four categories: (1) developers, (2) defenders, (3) enablers, and (4) deployers. In many cases, individual actors or entities fit into more than one of these categories.[181] For example, well-resourced nation states can be all the above, and an individual with meager means could be a developer. Consider the, at times, countervailing incentives within the American NSA; the agency has a long and storied defensive cybersecurity mission while being simultaneously responsible for executing signals intelligence collection and supporting US Cyber Command through the development, maintenance, and deployment of offensive cyber capabilities. Developers might also be defenders, nearly all of the software vendor community for instance, develops code but also works to defend it. In this analysis, we focus on developers of malicious capability to explain this taxonomy.

The traditional state/non-state distinction is lacking in this discussion, in part because there is little uniformity in the capabilities and behavior of all states or all non-state groups. Both states and non-states play different roles in the supply and demand of offensive cyber capabilities and related tools. While the legal status of states clearly differs from non-state groups, this is of little difference in our analysis of incentives, intentions, and behavior. The discussion of some non-state groups as proxies working on behalf of states is a attribution and control issue which presupposes little about the capacity of these groups or the source of their capability. The variation in proxy models means this would do little for our analysis as a standalone category.

Developers, in the context of the TrACE framework, are groups and individuals that manufacture and help maintain *offensive* capabilities including knowledge and software. These include individual researchers, national intelligence agencies, companies like Hacking Team, and even some criminal groups (though many are deployers rather than developers). Where a relatively few, well-resourced developers can produce robust capabilities from scratch, others patch together capability based on openly available or leaked information.

Table 3: Examples of Developers

Examples	Explanation
U.S. Cyber Command, GCHQ, German Cyber and Information	Intelligence agencies and military commands are key developers of offensive cyber capability. Many states have declared intention to develop robust offensive capability, though it is unclear

[180]For discussions see: Steven M. Bellovin, Susan Landau, and Herbert S. Lin, "Limiting the undesired impact of cyber weapons: technical requirements and policy implications," *Journal of Cybersecurity,* 3:1(2017)59-68; Ben Buchanan, "The Life Cycles of Cyber Threats," *Survival: Global Politics and Strategy*, 58:1 (2016)39-58

[181] Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (Rand Corporation, 2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

Space Command	how many have been successful.
NSO Group, Gamma Group, Hacking Team	A small group of private companies work closely with intelligence and law enforcement agencies to develop and ultimately sell offensive capabilities.
Paras Jha, Josiah White, Dalton Norman (all of the Mirai botnet), and Robert Tappan Morris (Morris worm)	Sometimes individuals will develop offensive capability. Sometimes these individuals will use these tools for personal gain or to prove a point. Other times they may release them unintentionally.
Russian Business Network, Yanbian Group, Hellsing, Carbon, Spiker/Carbanak	Some criminal groups are purported to have developed cyber capabilities on their own. In some cases these capabilities are sold or loaned out. In others, the criminal groups leverage the capabilities themselves.

Enablers are the groups and individuals that maintain a capability or facilitate its transfer. These can often be developers as well as covert groups like exploit brokers who are not developing or deploying a capability. These middlemen most often reside outside of government, whether companies like ReVuln and Vupen or criminal groups, such as those operating forums like AlphaBay.[182]

Table 4: Examples of Enablers

Examples	Explanation
AlphaBay, Hansa, Silk Road, Silk Road 3.0, Russian Anonymous Marketplace	Online message forums, often on the deep or dark web, provide platforms that enable the black market exchange of "goods" like vulnerabilities, completed capabilities, and tailored solutions.
Zerodium, Vupen	Some companies also provide a middleman service for individual and groups that possess vulnerabilities or capabilities to broker sales to willing and able buyers.

Defenders are the groups and individuals that try to prevent capability from having its intended (or indeed any) effect. As with the previous two categories of actors, defenders reside both in government, like the network of national computer emergency response teams, and outside of government, like independent security researchers, security vendors, and software and hardware manufacturers. While defenders ideally do not play a role in intentionally proliferating offensive capability, they play a potentially crucial role in countering the proliferation of offensive capability, as explained below.

Table 5: Examples of Defenders

Category	Example	Explanation
CSIRTs	JP-CERT, GovCERT Austria, CanCERT, CNCS	Increasingly governments around the world are developing computer security incident response teams (CSIRTs). The competencies and roles of these teams vary widely, but in most cases, CSIRTs housed in governments provide defensive services for government systems and critical infrastructure.

[182] Kurt Thomas et al., "Framing Dependencies Introduced by Underground Commoditization," 2015, http://damonmccoy.com/papers/WEIS15.pdf.

Security Researchers	H.D. Moore, Natalie Silvanovich	Independent security researchers play a crucial role in improving security by discovering and reporting vulnerabilities as well as other activities.
Software Companies	Microsoft, Oracle, SAP, Adobe Systems, Amadeus IT	The software industry is a key player in the defensive ecosystem. Some companies actively test their software for weakness and nearly all prominent software providers engage in the market for software vulnerabilities, sometimes paying outside researchers
Cybersecurity Vendors	Symantec, McAfee Check Point Software Technologies, Kaspersky Labs, Fox-IT,	Cybersecurity vendors provide products and services intended to reduce an organization's 'cyber risk'.
Cyber Commands and Intelligence Agencies	GCHQ, Dutch Cyber Command	Just as military cyber commands and intelligence agencies can and often are developers of offensive capability, many of these organizations are also tasked with defensive activity.

Deployers are the myriad individuals and organizations, from hacktivists to nation-states who use these capabilities. Some deployers are able to independently develop capabilities but many acquire components if not entire capabilities through transfer.

Table 6: Examples of Deployers

Category	Examples
Intelligence Agencies	The United States' NSA, Russia's Main Intelligence Directorate (GRU), GCHQ
Military Cyber Commands or equivalent units	U.S Cyber Command
Law Enforcement Agencies	U.S. Federal Bureau of Investigation
Criminal Groups	The Russian Business Network, Matsnu Gang, Zeus Gang, actors behind 'Operation Ghoul'
Individuals	Albert Gonzalez, Max Vision, Michael Calce, Jonathan James, Sven Jaschan, Kevin Poulsen, 'Kuji', 'Datastream Cowboy', Ehud Tenebaum, David Smith

Capabilities refers to the objects of proliferation, whether the knowledge behind a new tactic, the infrastructure used to support the deployment of capabilities, or the software deployed on a computer to have an effect. Capabilities are not monolithic, nor are they easily parsed. We frame capabilities as four related and sometimes overlapping components: knowledge, tools, infrastructure, and platform.[183]

Knowledge, like a software exploitation technique, is important in cyber security, more instrumental even than in traditional kinetic domains.

[183] Scholars attempting to do this include: Dale Peterson, "Offensive Cyber Weapons: Construction, Development, and Employment," *Journal of Strategic Studies*, Vol. 36, No. 1 (2013); Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security,* 41:3 (2016/17):72-109: Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, 22: 3 (2013)365– 40.

Table 7: Examples of Knowledge

Example	Explanation
Software vulnerability or exploit	Vulnerabilities in software and hardware exist, but the information on what they are and how to utilize them (exploits) can be seen as similar to a commodity.
Information about a physical system	Information about a physical system is integral in the development of cyber capabilities that try to affect physical infrastructure to cause damage or disruption.
Passwords or personal information	Breached passwords and personal information are often the means by which nefarious actors enter into systems they should not have access to, allowing them to carry out an attack.
The Art of the Possible	Sometimes, the simple depiction of what is possible is enough to spawn a new line of development of offensive capability.

Tools take this knowledge or a particular function and embody it in software. These might be tools to develop offensive capabilities or limited-use malware.[184]

Table 8: Examples of Tools

Example	Explanation
Acunetix	A web vulnerability scanner which focuses on web applications.
John the Ripper	A well known password cracker
Metasploit	A package of tools to determine which exploit to use (and how to configure it) as well as payload to use (and how to configure it).

Infrastructure describes connectivity resources like hosting and bandwidth as well as compromised computer networks like botnets and command & control servers used to sustain the operation of an offensive capability.

Table 8: Examples of Infrastructure

Category	Example	Explanation
Test Infrastructure	None publically available	In many cases, to achieve physical effects through cyber means, an attacker or attackers will need to possess nuanced understanding of how a physical system they plan to attack works and how different code injections will impact that system. To do so, some more well-resourced actors have been suspected of building test facilities with systems that mirror those they plan to attack.
Command and control infrastructure	CloudMe accounts used to communicate with recent Red October malware.	Command and control infrastructure is the infrastructure an attacker uses to conduct the attack.

[184] On the relationship between knowledge and tools in this context see: Slayton, "What Is the Cyber Offense-Defense Balance?"

Platforms range from from narrowly tailored tools like the Dridex banking trojan to the Equation Group espionage malware.[185] The most multi-featured and intricate appear to generally be a product of a small group of advanced states but there is no strict correlation.

Table 9: Examples of Platforms

Example	Explanation
Project Sauron	"[A] top-of-the-top modular cyber-espionage platform in terms of technical sophistication, designed to enable long-term campaigns through stealthy survival mechanisms coupled with multiple exfiltration methods," as Kaspersky Lab describes it.
BlackEnergy	An evolving set of Russian espionage malware, likely originally developed by criminal groups and later employed in attacks against Ukraine's power infrastructure. BlackEnergy is designed to execute "tasks" that are commissioned by its Command & Control servers and implemented by the plugins.

Effects are the changes produced on a computing system or attached hardware because of a capability's operation. These operations impact a system's confidentiality (its ability to keep data secret to certain people), availability (its ability to keep data or services available to users), or integrity (its ability to guarantee that data has not been changed or manipulated to produce an unintended effect).

Effects can fall on a spectrum, from access, through espionage and theft, to disruption, and ultimately destruction.

Access suggests a capability can operate on a computer system but implies no effects to change the system like an intelligence agency preparing a system for later operations. One example is the use of tools like Duqu to establish a digital beachhead on computer networks, in preparation for future activity like espionage. We define access as an effect because of the political significance of detecting an unauthorized actor in a computer network. Even without changing anything about the network, the presence of software like this can motivate crisis response and communicate substantial vulnerability.[186]

Table 10: Examples of Access Effects

Example	Explanation
Bowman Avenue Dam	In 2016, an Iranian hacker was able to remotely penetrate the back-office systems for a small dam, merely to gain information without attempting to influence the dam's operation.

[185] See Nikita Slepogin, "Dridex: A History of Evolution" *Kaspersky Lab,* (May 25, 2017), https://securelist.com/dridex-a-history-of-evolution/78531/.

and Ben Buchanan, "The Legend of Sophistication in Cyber Operations," Belfer Center White Paper (Cambirdge, MA: Harvard Kennedy School, January 2017), https://www.belfercenter.org/sites/default/files/files/publication/Legend%20Sophistication%20-%20web.pdf.

[186] DHS/ US CERT, "Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors," accessed November 12, 2017, https://www.us-cert.gov/ncas/alerts/TA17-293A.

Espionage & Theft compromises confidentiality and extracts data or information from a computer system for the attacker's gain. For example, the Red October malware was a multifaceted Russian espionage platform designed to siphon information from business, universities, and some government agencies.[187]

Table 11: Examples of Espionage & Theft Effects

Example	Explanation
OPM Hack	In 2015, Chinese hackers breached the computer system of the U.S. Office of Personnel Management (OPM), stealing key security clearance information on U.S. personnel.
Moonlight Maze	During the late 1990s, Russian hackers (Carberb) targeted US military information (technical research, contracts, encryption techniques, unclassified specifications of US war-planning systems) on the Pentagon, Department of Energy, NASA, private universities, and research labs' networks.
SWIFT Heist	Using the Dridex malware, unknown hackers (believed by some to be North Korean in origin) compromised the computer systems of several banks around the world and rerouted funds using vulnerabilities in the SWIFT system.
Anthem	A group based out of China, according to FireEye, were said to be responsible for a medical breach of information of Anthem. Although the CEO of Anthem said it was a 'very sophisticated' attack, other indicators suggest that it did not take anything extraordinary to compromise the systems.

Disruption compromises availability. Disruption can be as little as harassment or pose substantial risks to the stability of the Internet when it targets critical resources. The Mirai botnet, a collection of Internet of things (IoT) devices collected into a swarm, was used to target journalist Brian Krebs as well as disrupt internet availability and the domain name service (DNS) in 2016 and is a stark example of *disruption*.[188]

Table 12: Examples of Disruption Effects

Example	Explanation
Dyn, Estonia, Georgia,	Distributed Denial of Service (DDoS) attacks are an increasingly common form of disruption. The scale of DDoS attacks varies widely from rendering a single webpage inoperable to shutting off large swaths of the internet.
Witty Worm	An unknown actor wrote an exploit code, exploiting a vulnerability just two days after it was disclosed, with a destructive (lagged) payload
NotPetya	Ransomware is another increasingly common disruption effect that encrypts locks a user out of a computer or computer system until a bounty is paid to the attackers. Although early iterations of ransomware were reversible (the attackers could unlock the infected system upon receipt of payment), recent iterations have been less forgiving (in other words, they more function like wipers).

[187] Kaspersky, "'Red October' Diplomatic Cyber Attacks Investigation," SecureList, January 14, 2013, http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation#5.

[188] Ben Herzberg, Dima Bekerman, and Igal Zeifman, "Breaking Down Mirai: An IoT DDoS Botnet Analysis," *Incapsula Blog* (blog), October 26, 2016, https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html.

Destruction compromises integrity. This last category, destruction, can escalate, from integrity violations like damaging a file system, to wiping data, or even manipulating attached hardware to cause physical destruction. Destructive effects are the least frequent but most discussed effect on this spectrum. These operations include manipulating digital systems to cause physical effect but also a range of data destruction activities. These include the Stuxnet campaign and the crippling of a German steel mill in 2014 but also incidents like the Shamoon wiper attack against Saudi Aramco and Rasgas and the Dark Seoul wiper attacks against South Korea. [189]

Table 13: Examples of Destruction Effects

Example	Explanation
Stuxnet	In at least one case, cyber capability has been deployed to disrupt weapons programs, as was the case with the Stuxnet campaign, which caused physical damage to the Iranian nuclear enrichment facility in Natanz
Sony Pictures, Saudi Aramco	In both the Sony Pictures and the Saudi Aramco cases, hackers gained access to corporate computer systems and rendered machines inoperable using variants of wiper malware.

Capabilities leveraged to create such effects on confidentiality are often rudimentary and differ generally in terms of their level of obfuscation or covertness. Moving up the scale to disruptive effects, things like distributed denial of service attacks are common. Some of these are handled daily by major content delivery networks (CDNs) like Akamai.[190] Others have such marked impact that they occupy the public consciousness as with the Mirai botnet when it targeted a major domain name service (DNS) provider.

Table 14: Summary of the TrACE framework

	Transfers	Actors	Capabilities	Effects
Definition	The transfer of capabilities, knowledge, infrastructure, resources, or techniques between actors.	The entities responsible for developing and deploying malicious capabilities.	The software tools, techniques, or tradecraft used to produce some effect on a computer system.	The change produced on a computing system or attached hardware as a result of a capability's operation.
Categories	i) Intentional ii) Unintentional	i) Developers ii) Enablers iii) Defenders iv) Consumers	i) Knowledge ii) Tools iii) Platform iv) Infrastructure	i) Access ii) Espionage iii) Disruption iv) Destruction

[189] CFR, "Cyber Operations Tracker," https://www.cfr.org/interactive/cyber-operations.

[190] Buyya, Rajkumar, Mukaddim Pathan, and Athena Vakali, eds. "Content delivery networks", *Springer Science & Business Media*, 9 (2008), retrieved from: https://pdfs.semanticscholar.org/6ba0/658e77f3502a5f050b73d0cfbf2a571d0714.pdf

SECTION 5: MAKING PROGRESS ON PROLIFERATION: APPLYING THE TRACE MODEL

This section discusses the TrACE framework and uses it to offer guidance on how to counter the destabilizing effects of cyber proliferation. As said, counterproliferation implies a range of connected initiatives aimed at limiting, slowing, or stopping the spread of capability and diminishing its utility. Here, using the TrACE framework as guidance, we describe some possible counterproliferation activities in the context of cybersecurity and discuss their viability and current challenges. Several of these efforts exist, either directly or in more limited form.

Based on the TrACE Model, we now discuss the possible goals of proliferation and offer a series of recommendations. The first three elements of the TrACE model connect to Pillar I (transfer), while the last element of the model, effects, connects to Pillar II (utility). Though a comprehensive understanding of the model is required, we can now look at these elements individually because different interventions address different actors.

POTENTIAL INTERNATIONAL AGREEMENTS

Considering the first element, transfers, we focus on the *enabler* portion of actors. The second element, actors, does not apply in this context. The third element, capabilities, focuses on *developers* and *deployers*. For the final element, effects, we focus on *deployers*.

Non-cyber initiatives, which seem to be applicable to cybersecurity tend to address only one or two elements of the TrACE model. With this understanding, we can consider how conventional interventions relate to each of these elements and actors. Most prominently, for example, export control agreements would affect the *enablers*. Arms control addresses *developers*. One could also consider models for drug transfer controls and disease control, which would relate to *deployers* and *enablers*. Here, however, we focus on two types of international agreements: export controls and arms control. More research is needed to explore the potential utility of other international agreements, like law enforcement agreements (looking at drug enforcement as a potential model), disease control, or climate change.

In this context, we explore how an international agreement of any sort could apply to one or all elements of the TrACE framework. A successful international agreement requires the following features. First, it must be able to set a clear threshold or guideline for what is tolerated or not under the agreement. Second, it requires monitoring and verification of adherence. Third, there needs to be the potential for punishment if an actor fails to comply.[191]

[191] In some international discussions, the argument is made that actual punishment may not be required as long as the threat of punishment exists.

Table 15: Essential Features of International Agreements and the TrACE Framework

	Tr	A	C	E
Which actor does it address?	Enablers	NA	Developers	Deployers
Threshold - Long Term Feasibility	Yes	NA	Yes	Yes
Threshold - Short Term Feasibility	Low	NA	Low	High
Monitoring and Verification - Long Term Feasibility	Yes	NA	Yes	Yes
Monitoring and Verification - Short Term Feasibility	Low	NA	Low	High
Punishment - Long Term Feasibility	Yes	NA	Yes	Yes
Punishment - Short Term Feasibility	High	NA	High	High

Currently, traditional tools to limit the spread of capability, like export controls and arms control, are lacking in these areas in the context of cybersecurity. The deficiencies of ongoing international norms deliberations mean that the international community lacks clear consensus on thresholds or guidelines for what is and is not acceptable. A clear definition of these thresholds is a necessary prerequisite for meaningful application of export or arms control. The covertness of offensive cyber programs poses challenges for monitoring and verification. Finally, as with many international agreements, more work must be done to identify meaningful punishment for defectors or those who choose not to comply. Here we outline these and other shortcomings in more detail and offer a series of challenges that must be addressed before such international interventions reach a threshold of feasibility.

ARMS CONTROL AGREEMENT

Arms control agreements could most readily apply to states developing capabilities, aimed at limiting or entirely banning this development activity. Progress through such agreements is likely to be limited and would likely require clarity on existing standards of behavior like the development or use of destructive offensive capabilities.

While not directly pointed at addressing the *transfer* of capability, an arms control agreement would target the development of capability. An arms control agreement for offensive cyber capability would involve states (possibly with other *developers*) agreeing to cease the production of either segments of or all offensive capability. Contemporary analogues for this type of intervention include the Chemical Weapons Convention (CWC), the Ottawa Landmine Treaty (Ottawa Convention), and Biological Weapons Convention (BWC). Yet, there are several challenges.[192]

Kenneth Geers examined the feasibility of a Cyber Weapons Convention based off of the CWC, pointing to the convention's success in minimizing the use of chemical weapons, which has drastically fallen since WWI when chemical

[192] Including where an arms control agreement could raise uncertainty about or, at worst, outright ban some defensive activities like penetration testing and vulnerability reporting.

weapons caused one third of casualties.[193] He concludes that three characteristics that make the CWC so effective apply to a cyber arms control regime: (1) political will , because the threat posed by cyberattacks is sufficiently severe worldwide for political consensus on the issue; (2) universality, because "everyone is a neighbor in cyberspace," which naturally lends itself to shared or universal goals; and (3) sufficient assistance, because an organization dedicated to helping member states improve their cybersecurity situations is feasible. While these conditions may be feasible in the long run, all three are currently absent.

At a basic level, an international arms control agreement is likely only effective when it is agreed to by the biggest *developers* of offensive capabilities. Even if we assume the most prominent of these developers are nation-states—an uncertain characterization given the sophistication of some non-state groups—we face a definitional challenge: what is a cyber weapon? Some states conflate information weapon and cyber weapons, viewing tools that enable the propagation of narratives or news as cyber weapons, while others define them as only tools that manipulate computer hardware and software.[194] Meaningful progress on bridging this divide is a prerequisite to an effective arms control arrangement.

Even if there were ready definitional agreement, the problem of political will remains. As alluded to above, landmines, chemical, and biological weapons are the major precedents. They share a common trait in that they are viewed as morally abhorrent for either their blatant inability to distinguish between targets (landmines) and the existence of more humane means to achieve the same or similar military ends (chemical and biological weapons). In short, they clearly breach international humanitarian legal principles of distinction and necessity. Although some capabilities do not distinguish between legitimate military targets and non-targets, to some, cyber capabilities are seen as perhaps the most humane tool to achieve military ends due to their non violent nature.[195] Arms control only works if the major players agree to cease production and use. It is exceedingly difficult to picture a world in which the political will would exist to create an arms control agreement for any current capability. Depending on how cyber capabilities evolve, this could change, and that change will be driven by *effects*.

The final challenge is a purely operational one: how and by whom would such an agreement be verified? The BWC and Ottawa Convention both lack formal verification and compliance mechanisms. However, the CWC does provide a potential model for verification through the permanent Office for the Prohibition of Chemical Weapons (OPCW). The OPCW is similar to the better-known International Atomic Energy Association, in that it is a permanent international organization that "includes a verification division with an international corps of about 180 inspectors who travel to declared military and industrial sites around the world."[196] The CWC model also shows promise as an analogue for a cyber arms control agreement because the two technologies share one crucial trait: the material and knowledge leveraged to develop capability both change quickly as new discoveries are made and are dual-use. The CWC addressed this arms control challenge by creating and consistently updating a scheduling apparatus to identify the most potentially harmful types of chemicals.

---

[193] Kenneth Geers - Cyber Weapons Convention, http://www.sciencedirect.com/science/article/pii/S0267364910001081

[194] See, for example, the conflation of cyber and information security in the repeated calls for a Code of Conduct for Information Security by several Shanghai Cooperation Organization states. https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf

[195] Tim Maurer - "The Case for Cyberwarfare," *Foreign Policy,* http://foreignpolicy.com/2011/10/19/the-case-for-cyberwarfare/

[196] Jonathan B. Tucker - "Verifying the Chemical Weapons Ban: Missing Elements," *ArmsControl Association*, https://www.armscontrol.org/print/2289

EXPORT CONTROL ARRANGEMENT

Though export controls hold some promise for countering the proliferation of offensive cyber capabilities, the sloppy application of the tool threatens defense as much or more than offense.

An export control arrangement would harmonize the export controls of nations *developing* or harboring *developers* to limit the *transfer* of *capabilities* or the means to develop capabilities to a set group of nations. The counterproliferation opportunity associated with an export control arrangement resides in preventing the spread of capability from agreeing *developers* to a group of identified state, corporate, and/or individual consumers. To provide an analogue, export controls are an important tool in the implementation of the Nuclear Nonproliferation Treaty (NPT) through the Zangger Committee.[197]

However, export controls face a number of challenges in the context of cyber counterproliferation. First, an export control arrangement does not ban the proliferation of capabilities within states. Second, at a fundamental level, export controls only restrict the flow of goods and services in white markets. As at least a portion of interstate *transfer* already occurs on black markets, this will not necessarily pose a new challenge, but it is likely to increase the challenge. In addition to these challenges, the use of export controls in the context of cyber proliferation poses two discrete risks. First, overly inclusive controls could place detrimental limits on spreading defensive technology and information. Second, export controls tend to push trade in materials to black, less visible markets.

Controls proposed via the Wassenaar Arrangement, a 41-member multilateral export control regime, was an initial foray into the use of export controls to limit the spread of cyber capability and starkly illustrates these risks and challenges. Indeed, the "intrusion software" control, proposed by the British delegation, was initially framed to focus on "Advanced Persistent Threat Software (APT) and related equipment (offensive cyber tools)."[198] The purpose of the proposal was to harmonize the export controls of Wassenaar members to limit the spread of intrusion software, but the ongoing controversy around the control starkly demonstrates one of the potential risks, that of over inclusiveness, as discussed here.

The intrusion software control used broad language in an attempt to capture as much malicious capability as possible. However, in doing so, this overly inclusive definition had the unintended consequence of also limiting defenders. Indeed, many in industry and academia fear that the restrictions could also apply to benevolent pursuits like penetration testing and information sharing on vulnerabilities, as the language of the control does not differentiate based on intent.[199] In addition to the concerns of security companies that the controls would restrict their ability to do

---

[197] Nuclear Threat Initiative. "Zangger Committee (ZAC)." *Nuclear Threat Initiative*. http://www.nti.org/learn/treaties-and-regimes/zangger-committee-zac/

[198] Reports from the Business, Innovation and Skills, Defence, Foreign Affairs and International Development Committees Session 2013-14 Strategic Export Controls: Her Majesty's Government's Annual Report for 2011, Quarterly Reports for 2011 and 2012, and the Government's policies on arms exports and international arms control issues; Response of the Secretaries of State for Defence, Foreign and Commonwealth Affairs, International Development and Business, Innovation and Skills, para. 88, October 2013. http://www.official-documents.gov.uk/document/cm87/8707/8707.pdf (p. 37)

[199] Sergey Bratus et al., "Why Wassenaar Arrangement's Definitions of Intrusion Software and Controlled Items Put Security Research and Defense At Risk—And How To Fix It" (Public Comment, October 9, 2014), http://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf.

business,[200] security researchers harbored concerns that these controls would prevent penetration testers in countries that implement controls from responsibly reporting vulnerabilities discovered across borders. In short, the over inclusiveness of the intrusion software language threatens to do more to hinder better security than help it.

A second major risk lies in the propensity of export controls to push transfers to black markets. In doing so, defensive actors lose important visibility into the market for offensive products, thereby hindering their ability to forecast and proactively defend.

The current feasibility of export controls to meaningfully decrease the spread of offensive cyber capability is limited. However, in order to further explore the potential feasibility of an export controls intervention policymakers should work to better understand the two major risks in order to manage them as well as working to address the three major challenges regarding thresholds, verification, and punishment.

TOOLS FOR STATES OR LIKE-MINDED ACTORS

In addition to sweeping international agreements, states have tools that they could leverage unilaterally or within like-minded coalitions.

Table 16: Summary Tools for States or Like-minded Actors

	TrACE Framework Element Addressed	Actor Effected	Current Feasibility	Longue Durée
Manipulate the market through purchasing power	Transfer and Capabilities	Developers, Deployers, and Enablers	Low	Yes
Enhance defensive capabilities	Capabilities and Effects	Defenders, Deployers	High	Yes
Enhance offensive capabilities (cyber and non-cyber)	Capabilities and Effects	Deployers	High	Yes
Diplomatic toolbox	Actors and Effects	Deployers	High	Yes

Market Manipulations

Given that there is a market for cyber capabilities, however fragmented across language and skill level, how can market manipulation contribute to a counter-proliferation strategy? There are at least three basic strategies to manipulate a market with as many information asymmetries as that for cyber capabilities - undermine trust, affect supply or demand,

[200] Cheri McGuire, "U.S. Commerce Department Controversial Cybersecurity Rule Will Weaken Security Industry and Worldwide Protections," *Symantec Global Government Affairs* (blog), accessed November 11, 2017, http://www.symantec.com/connect/blogs/us-commerce-department-controversial-cybersecurity-rule-will-weaken-security-industry-and-worl.

or break market functionality. The last is the most straightforward - block markets to make them inaccessible to buyers or disrupt the market for transaction critical services like payment processing or hosting.[201]

Disrupting supply or demand require more influence on the underlying goods at trade. One proposal, from Dan Geer in his now famous 2014 keynote for the BlackHat conference, suggested that the United States could allocate the resources necessary to buy up all software vulnerabilities.[202] Accepting that the speech was intended to kickstart a conversation about software liability, the proposal was nonetheless both provocative and compelling. The idea that one player in the market could vacuum up the available supply to such an extent that new sales would be possible only on the fringes, would limit new capabilities to those groups who could develop them, or obtain them directly from a developer.

An alternative to Geer's approach would be to enhance the speed and depth of vulnerability discovery and patching states could undermine the development of cyber capabilities which rely on software vulnerabilities by encouraging more effective vulnerability discovery, disclosure, and patching. Reducing the supply of vulnerabilities through this discovery and patching will raise of the cost of acquiring these capabilities and help disrupt the activity of sellers unable to update their products fast enough. This market manipulation doesn't involve purchasing vulnerabilities directly, instead it reduce their useful life by more rapidly patching them.

Not all vulnerabilities are equally easy to find or take advantage of and not all offensive capabilities require the use of one of these vulnerabilities. This proposal to target vulnerabilities for discovery, disclosure, and patching targets only those offensive capabilities which take advantage of these software flaws. This is not an argument for how to restrict the transfer of offensive capabilities more effectively. Instead, it is a means of focusing on a common supporting component for many offensive cyber capabilities.

Disrupting trust is a more amorphous set of objectives. The seizure of Alphabay followed a period where the site was operated by law enforcement, leading to the possibility that every future market going dark could be accompanied by the same long tail. Breeding this sort of suspicion is one thing with these underground markets but is more difficult looking at many of the companies involved in selling capabilities in whole or in part like Zerodium, Hacking Team, or NSO Group. The use of legal discovery mechanisms to force client lists and other sales documents from these groups into the public domain could be a means to create mistrust or the potential for compromise in the minds of secrecy minded customers.

ENHANCE OFFENSIVE AND DEFENSIVE CAPABILITY

A growing number of states have already stated that they are looking to increase offensive capability. However, it is just as important to focus on the defensive side. In this case, the nuclear analogy is a missile defense system, designed to make it more difficult to achieve the effect of nuclear capability once developed or purchased. In addition to ultimately diminishing the effects of proliferation, rendering capability less or unuseful is also likely to dampen the demand for offensive capability. Diminishing the attack surface, through interventions in the market for vulnerabilities like the one described above, is one way to diminish utility. An increased velocity of vulnerability discovery and reporting renders capabilities built on those vulnerabilities transient, diminishing their long-term utility.

---

[201] https://motherboard.vice.com/en_us/article/evd7xw/us-europol-and-netherlands-announce-shutdowns-of-two-massive-dark-web-markets and http://www.tandfonline.com/doi/full/10.1080/17440572.2016.1197123

[202] https://www.darkreading.com/dan-geer-touts-liability-policies-for-software-vulnerabilities/d/d-id/1297838?piddl_msgorder=thrd

However, more can still be done to diminish the utility of offensive cyber capabilities including two goals achievable in the near term. First is enhancing the speed and volume of information sharing between organizations to more rapidly counter attacker innovation and changes in capabilities. Attackers will become more conservative in target selection and capability deployment if any target they assault can alert all others to the details of their attack. Second is an emphasis on cloud computing, where defensive organizations can implement changes and patch vulnerabilities for all users in an organization much more rapidly than in the traditional enterprise computing model. These approaches are technical but can be encouraged by international agreement (especially information sharing) and or soft norms like the adoption of principles through plurilateral forums, like the OSCE or ASEAN, which encourage regulatory environments and security cooperation which complement these approaches.

DIPLOMATIC TOOLBOX

In addition to activities designed to address the proliferation of offensive cyber capability, states and other actors can work to diminish the utility of capability, once spread. Diplomatic efforts, like the European Union's Diplomatic Toolbox to deter cyberattacks are a key way to do this, and sanctions are at the heart of diplomatic efforts and conceived to be the key tool for deterring, compelling, and/or incapacitating adversaries.[203]

Sanctions are a key tool to punish an actor for bad behavior. When utilized after an incident, sanctions are intended raise the perceived cost of an action to an adversary, thereby deterring further, similar action. However, sanctions can also be utilized before adversarial action takes place as capability is being developed. This kind of preemptive punishment is designed to disincentivize future action.

A second potential use for sanctions lies in incapacitating adversaries with limited resources. Because the development of some strata of capability (and perhaps more importantly the persistent development and deployment of some strata) requires institutional strength and financial backing, targeted sanctions could diminish the capacity of a *developer* to produce capability. Targeted sanctions can also provide a powerful disincentive for individuals contributing to development on their own or as part of a team. Additionally, sanctions could diminish the capacity of some *deployers* to purchase capability.

Most impactful when they are implemented universally, sanctions pose substantial risk of collateral harms and can be politically fraught for fragile alliances or coalitions of consensus. Other challenges associated with a sanctions regime to address the *transfer* and *actors* in the proliferation ecosystem are numerous. One key challenge lies in identifying key individuals or groups of both *developers* and *deployers*. Furthermore, sanctions are likely to only have an appreciable impact on *actors* with limited resources.

[203] Sico van der Meer - "EU Creates a Diplomatic Toolbox to Deter Cyberattacks," Council on Foreign Relations - Net Politics Blog, June 20, 2017, https://www.cfr.org/blog/eu-creates-diplomatic-toolbox-deter-cyberattacks.

SECTION 6: RECOMMENDATIONS

In this section, we first explain the need for patience, then provide a series of recommendations aimed at: (1) increasing the cost of developing offensive cyber capabilities, (2) diminishing the utility of capability once spread, and (3) further exploring ways to increase barriers to spreading offensive cyber capability. The TrACE framework provides a good guide for researchers and policy-makers for conceptualizing proliferation of capability, but more work is needed to truly understand the mechanics of development, spread, and deployment.

1. PATIENCE.

The first lesson that policy-makers must heed is that the construction of a security regime—and particularly of a counterproliferation regime—is arduous. It takes time, subject matter expertise needs to be developed and infused into policy circles, hurdles like crafting a viable verification or inspection mechanisms must eventually be overcome, and an understanding of the above and below ground markets for relevant goods and services must be developed and leveraged. Efforts like the preparatory workshops for the Group of Governmental Experts (GGE) meetings and indeed the Global Commission on the Stability of CyberSpace (GCSC) aid in that essential diffusion of expertise.

For the policy-makers involved in the process, patience is paramount. In his 1953 "Atoms for Peace" speech, Eisenhower noted the imperativeness of patience, saying:

> *"In this quest, I know that we must not lack patience. I know that in a world divided, such as ours today, salvation cannot be attained by one dramatic act..."*[204] Eisenhower's words ring equally true today in the context of cybersecurity.

As we've witnessed in the past, negotiation processes around these sorts of regimes are generally long, drawn-out, and controversial. The NPT took nearly 20 years to craft from its early beginnings in 1957 to end and nations continued to iterate on the overarching regime until the mid-1990s with the Comprehensive Nuclear-Test Ban Treaty. Similarly, negotiating the surprise inspection provision of the CWC during the tensions of the Cold War was incredibly difficult diplomatically, but ultimately fruitful.

Policy-makers must also accept that the process of building a regime will not be easy. As demonstrated by the shortcomings of the Wassenaar Arrangement, it is possible that the international community will not be able to simply transpose an existing model on top of the cybersecurity problem. Instead, it is far more likely that new and innovative models will need to be built to address the challenge. In order to craft a regime that both has the desired effect and minimizes the negative externalities, a deep understanding of the technologies in question must be infused into the policy process. Practicing physicists made the progress of the NPT, from hard initial negotiations to eventual ratification, possible. While the cybersecurity threat may not be existential, as the nuclear threat, the risks should not be ignored.

[204] Eisenhower, Atoms for Peace.

2. INCREASE THE COST OF DEVELOPING OFFENSIVE CYBER CAPABILITIES

Raising the cost of offensive cyber capabilities can be accomplished through reducing the supply (and thus cost) of software vulnerabilities and increasing the speed at which defenders can adapt to attackers by enhancing the use of cloud computing. By raising the cost of development, the number of developers in the market will decrease. This supply-side decrease could then reverberate throughout the proliferation ecosystem, limiting the transfer, diminishing the number of deployers, and possibly limiting capability to primarily the most profitable forms of capability.

Reducing the supply of vulnerabilities will raise the cost of acquiring offensive cyber capabilities and help disrupt the activity of actors involved in transferring capabilities to others by forcing them to update their products with unsustainable rapidity. This strategy to counter proliferation in cyberspace could encourage more effective discovery, disclosure, and patching of software bug instead of building new or more refined export controls. It could enhance information sharing between state organizations with insight into attacker trends and major software vendors and cloud service providers. Reducing the utility of cyber capabilities looks to attack demand rather than use of these capabilities, with benefits that will trickle up to the larger security ecosystem.[205]

Key to limiting the use of malware is modifying attacker's incentives to build and deploy this software. This can be accomplished by increasing the pace and volume of software vulnerability discovery, disclosure, patch development, and patch application. The result of these changes would undermine the supply of software vulnerabilities available to attackers using malware which depend on these vulnerabilities. This would reduce how long any piece of malware might be useful for, before its targets had patched their software. Malware authors would have to write code faster and faster to keep it current, increasing costs and potentially driving many out of the business altogether. This accelerated vulnerability disclosure and patching cycle would also lead to more robust software, making it easier to defend organizations, though it may adversely affect a country's own offensive arsenal.

The resulting increase in costs to develop offensive cyber capabilities target attackers' incentives—pricing less-resourced actors out of the security ecosystem and constraining the capabilities of better resourced groups. This pushes states towards collaboration with the private sector to influence attacker behavior by shifting the incentives to develop and use capabilities. As such it implicates both actors and capabilities in the TrACE model, looking at a public-private nexus.

Offensive cyber capabilities often depends on exploits targeting vulnerabilities in software or hardware to gain and maintain access to computer systems, with destructive attacks like Stuxnet espionage operations like Red October, even common surveillance tools.[206] Most cyber capabilities requires these vulnerabilities at some stage of operation

---

[205] Trey Herr, "Countering the Proliferation of Malware: Targeting the Vulnerability Lifecycle," Belfer Center White Paper, Cyber Security Project Paper (Cambridge, MA: Harvard Kennedy School, June 27, 2017).

[206] Stuxnet - Nicolas Falliere, Liam O. Murchu, and Eric Chien, "W32. Stuxnet Dossier" (Symantec, 2011), http://www.h4ckr.us/library/Documents/ICS_Events/Stuxnet%20Dossier%20(Symantec)%20v1.4.pdf; Ralph Langner, "Langner - To Kill a Centrifuge.pdf" (The Langner Group, November 2013), http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

Red October - Kaspersky, "'Red October'. Detailed Malware Description," *Securelist.com*, January 17, 2013, http://www.securelist.com/en/analysis/204792265/Red_October_Detailed_Malware_Description_1_First_Stage_of_Attack#1.

Surveillance tools - Bill Marczak and John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used against a UAE Human Rights Defender," *The Citizen Lab*, August 24, 2016, https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/; Stefan Esser, "PEGASUS iOS Kernel Vulnerability Explained |

but not all. Reducing the supply of these vulnerabilities would limit those available to attackers and increase the cost necessary to acquire them. Groups with few resources might avoid targets while less cost-sensitive organizations, like major intelligence agencies, may find themselves constrained by this shortfall in new exploits to enable their operation. Limiting the supply of vulnerabilities doesn't remove attackers from the security ecosystem but it disrupts the process of developing and deploying malware, making these critical pieces of information scarce and thus more difficult to acquire. Versions of this approach have already had success with lower hanging fruit, as more secure web application technologies have impacted the supply of vulnerabilities for commonly used exploit kits.[207]

Counter-proliferation can also raise the cost to attackers by making defenders more agile and quick to adapt through expanded adoption of cloud computing. Cloud computing enables vendors and defensive organizations to more rapidly shift defensive technologies to blunt attacker's innovations, for example by making global changes to an organization's entire software stack in a few short minutes. The size of some global cloud providers also means they can see even small and highly targeted attacks, rapidly disseminating information about the threat to defend organizations around the world. This increases the likelihood that an offensive capability, technique, or tactic, once used, will be exposed and its value commensurately reduced.

3. FURTHER EXPLORE WAYS TO INCREASE BARRIERS TO SPREADING OFFENSIVE CYBER CAPABILITY

There has been a lively debate over the potential utility of agreements to limit the spread of offensive capabilities, potentially along the line of arms control agreements for nuclear and biological weapons. This topic is one that deserves further development and study as a standalone topic outside the specific discussion of counterproliferation. As such, we note it here but leave it as a starting point for further exploration.

Defining offensive capabilities in relation to effect is likely to become a prominent part of the next phase of debate over proliferation. This Commission could convene expert working groups to set tiers, or thresholds, between different types of capabilities according to the severity of effects they produce. Non-destructive capabilities, taken at sufficient scale like botnets, or at important points in a process, like information on an industrial control system, can impose substantial harm. Developing a threshold for determining what effects are significant however remains a largely political act in its explicit valuation of some potential targets over others. For this reason, we believe the conversation over these thresholds should start within the policy community and this Commission rather than this document.

The policy community should explore the applicability of all models focused on the spread of goods, materials, information, and more. While many will be drawn to nuclear comparisons—possibly simply due to language parallels involving the word "proliferation"—explorations should not be so limited.

SektionEins GmbH," September 2, 2016, http://sektioneins.de/en/blog/16-09-02-pegasus-ios-kernel-vulnerability-explained.html.

[207] https://www.trustwave.com/Resources/Trustwave-Blog/Why-Exploit-Kits-Are-Going-Dark/

CONCLUSIONS

The core of this report, the TrACE framework, is intended as an evergreen model to provide policymakers and others looking at proliferation within cybersecurity a means to conceptualize and discuss major factors in proliferation. In our development of this framework, we offer a snapshot of the security ecosystem and proliferation activities as they can be observed at this moment.

Key to understanding proliferation with an aim towards countering it is differentiating between types of capabilities. We know that not all capability is created equally. The development of Stuxnet, for example, is rumored to have cost orders of magnitude more than the development of simple phishing tools to steal credentials. Intuition tells us that the more resource-intensive capabilities are likely the ripest targets for counterproliferation efforts.

Thus, a key element for consideration by analysts and researchers is how to set these tiers or thresholds to differentiate types of capabilities. Conventional analysis tends to conflate effects with capabilities but this undersells the disparity with regard to ease of development between some capabilities that cause similar effects. We suggest that the development of such thresholds requires careful consideration from the policy and technical community and would be a meaningful step towards understanding the proliferation ecosystem, but falls outside the scope of this document.

To that end, this exploration is simply a starting point to prod the international conversation about cybersecurity in what we view to be a more meaningful direction. However, this report does not portend to have all the answers, and it may indeed offer more questions that it does answers. To help guide future research and exploration, we outline a set of those open questions here:

- What are the best forums for counterproliferation discussions internationally? Does counterproliferation lend itself to an approach embracing only like-minded participants or is it feasible in a broader multi-lateral format?
- In the context of cyber proliferation, what sorts of scenarios are the international community most concerned about? Would the mechanics of slowing or blocking the proliferation of capability to non-state terror groups like the Islamic State differ from countering the proliferation of capability to a large nation-state adversary?
- What is the threshold on capabilities a state could transfer to a malicious actor to violate a consensus or normative limit?
- While we offer an exploration of potential export and arms control approaches, what other international mechanisms might produce positive results, and what models might we explore to help generate better understanding about countering the spread of goods, services, information, and more? What might we learn about the spread of offensive cyber capability from experiences in the chemical and biological weapons community? What about from unmanned aerial vehicles? Are there lessons to be drawn from experiences in countering narcotics or disease control? What other areas are ripe for exploration?

The immediate and increasing threat of cyber capabilities may drive an inclination on the part of policymakers around the world to act swiftly and decisively to counter the proliferation of these capabilities. However, without the requisite knowledge about how the proliferation ecosystem functions, how capability is developed and spreads, and a clear picture of what mechanisms might be available to slow, block, or otherwise counter this proliferation, hasty policy interventions are likely to fail—or worse: throw further fuel on the problem.

WHAT MAKES THEM TICK: EVALUATING NORMS ON CYBER STABILITY

Dr. Arun Mohan Sukumar, *Observer Research Foundation*

Madhulika Srikumar, *Observer Research Foundation*

Bedavyasa Mohanty, *Observer Research Foundation*

MEMO №3

TABLE OF CONTENTS

SECTION 1: INTRODUCTION

The exploitation of digital networks by nation-states for political and military objectives has amplified the need for "rules of the road" or norms of conduct in cyberspace. Despite several rounds of multilateral conversations on the subject — a UN Group of Governmental experts set up to articulate cyber norms has been meeting since 1998 — states have found it easy to disrupt and costly to discourage destabilising conduct in cyberspace. Disruptive actions by states and their proxies prompt not only a renewed debate on deterrence in cyberspace, but also the effectiveness of an international regime to predict, manage and define their behaviour. In 2015, a GGE comprising the United States, Russia and China, among other countries, recognized the applicability of international law to the conduct of states in cyberspace, and sought a "common understanding" of its application. (GGE Report: 2015)[208] The GGE's report, endorsed by the UN General Assembly, marks the first instance where states invoked the urgent need to "legislate" or legalise norms around cyber-stability. Yet, the 2016/ 17 iteration of this Group was unable to agree *which* international laws or rules should govern the conduct of states.

The 2016/17 GGE's failure throws up more questions than answers: What role do norms[209] play in guaranteeing cyber stability? If states are indeed motivated by "rational" interests, what hope does the international community have of articulating norms that reflect restraints on their conduct? What is the appeal of cyber norms to states: is it moral, legal, political, military or economic? With the benefit of hindsight, it is possible today to evaluate the progress made by states in crafting and committing to cyber norms, and attempt to answer these queries. The UN GGE set up in 1998 "on matters related to the security of Information and Communication Technologies" has met five times now — as stated earlier, its last session in 2016/17 ended without a report, reflecting the disagreements between member states on the applicability of of international law to cyberspace. In subsequent UN forums, states have suggested that there should be an "Open Ended Working Group" to deliberate international law applicable to cyberspace.[210] Others suggest that international law already applies to cyberspace,[211] leaving only the question of "how" to interpret its application on a case-to-case basis.

The applicability of international law is conjoined with the continued existence of cyber norms. Without ensuing state practice or a binding, legal framework in the form of a treaty or a convention to support their conduct, cyber norms remain expressions of hope about the conduct of states. This is not to discard their utility. A norm, on account of its persuasive value, could trigger its "legalisation" by inducing states to observe it. This is especially important in the context of cyberspace, where many states are unsure of, and impatient for, guidelines of behaviour to emerge organically over time, given the stakes for their digital economies. But norms themselves are not a constituent element

---

[208] *UN Group of Governmental Experts Report on Developments in the field of information and telecommunications in the context of international security*, A/70/174, June 2015.

[209] For the purposes of this memo, a norm is understood to be a non-binding guideline or recommendation for the conduct of states and non-state actors.

[210] ReachingCriticalWill (RCW_), "A #cyber OEWG would help lay groundwork for future strategy. Int'l law is applicable, including #UN Charter @IranUNMission #FirstCommittee", October 24, 2017,

https://twitter.com/RCW_/status/922568530742034432

[211] ReachingCriticalWill (RCW_), " States must implement agreements made before discussions stalled in #UN #cyber expert group, says @franceonu #FirstCommittee", October 24, 2017,
https://twitter.com/RCW_/status/922559445649035264

of international law. One view in the burgeoning international law/ international relations cross-discipline treats *legalisation* of norms as an outcome, reached when states create, through practice or formal instruments, norms with a high degree of precision and solemn intent to conform.[212] Another, perhaps more dynamic, approach emphasises the process by which norms accrue legitimacy in the eyes of states.[213]

Using existing analytical frameworks, this paper sets out to evaluate the efficacy and 'pull' of cyber norms agreed to by the UN GGE and other international forums. The norms studied in this paper relate closely to the idea or conception of the "public core", although this term may be construed widely in the absence of any internationally accepted definitions. Chapter 1 sets out the centrality of cyber stability norms for the peaceful use of ICTs. Chapter 2 introduces a framework for assessing the emergence and application of these norms - and lays out the conditions necessary for norms to induce changes in state behaviour. Chapter 3 illustrates the role of norms in ensuring cyber stability by analyzing the current discourse on information operations.

[212] Kenneth W. Abbott, Robert O. Keohane, Andrew Moravcsik, Anne-Marie Slaughter, and Duncan Snidal, (2000) The Concept of Legalization, International Organization 54, 3, Summer 2000, pp. 401–419

[213] Martha Finnemore and Stephen J. Toope, (2001), *Alternatives to Legalization: Richer Views of Law and Politics*, International Organization, Vol. 55, No. 3 (Summer, 2001), pp. 743-758

SECTION 2: ROLE OF NORMS

In the absence of a formal, institutionalised regime to regulate or oversee the conduct of states in cyberspace, norms acquire special significance. Cyber norms agreements are ideal incubation laboratories for states to practise and promote stabilising conduct. They are not binding international legal instruments. If anything, the pursuit of an international legal agreement with robust frameworks to support its implementation is ill-advised. For instance, the 2015 GGE report that recommended — or perhaps reinforced — the norm of non-interference in cyberspace is an important step to designing a cyber stability regime, but developments in the last decade reflect the difficulties in pursuing this goal. In the months leading to the 2016 US presidential elections, and soon after, the United States formally attributed cyber attacks on its election infrastructure to Russia.[214] The nature of alleged Russian intrusions into US digital networks illustrate the hurdles to setting up a multilateral instrument that can enforce stability in cyberspace.

Firstly, Russian hackers were reportedly able to breach the email servers of the Democratic National Committee but did not destroy or tamper with the integrity of correspondence, preferring instead to leak it to third party outlets. (Sanger, Shane: 2016)[215] There are no uniform or common minimum data protection standards that apply across jurisdictions, limiting the remedies available for countries to prosecute and enforce sanctions against perpetrators.[216]

Secondly, the United States did not, at the time of the incident, classify its electoral systems as "critical infrastructure", signalling to adversaries that targeting them may not invite strong retaliatory action.[217] The 2015 GGE report called on states not to "conduct or knowingly support" cyber attacks on "critical infrastructure" from their territory, but does not clarify the scope of the term.[218] An expansive approach to "critical infrastructure" offers room for states to interpret it in line with domestic objectives, but also creates legal ambiguity that makes international cooperation difficult in the wake of a cyber attack.

Given the difficulties to realise an international law-driven framework, therefore, cyber norms assume great importance. Exercises to create normative convergence or to codify the "rules of the game" in cyberspace need not necessarily be distinguished from *realpolitik* or the cold-blooded calculations of states. The continued and uninterrupted functioning of the Internet and its underlying infrastructure — and the resilience of all public institutions that depends on it — is undoubtedly in the common interest of all states. Cyber norms agreements therefore aim to arrive at voluntary guidelines that ensure the smooth functioning of the internet, which is crucial to economic output today.

---

[214] David Sanger and Charlie Savage, *U.S. Says Russia Directed Hacks to Influence Elections*, The New York Times, October 7, 2016.

[215] David Sanger and Scott S. Shane, *Russian Hackers Acted to Aid Trump in Election, U.S. Says*, The New York Times, December 9, 2016,

[216] *Data Protection*, Privacy International, https://www.privacyinternational.org/node/44 [Last Accessed on December 20, 2016].

[217] Kate O'Keefe and Byron Tau, *U.S. Considers Classifying Election System as 'Critical Infrastructure'*, Wall Street Journal, August 3, 2016.

[218] *Supra* n. 1 at ¶ 13(f).

Thus, international norms that help "shepherd" state behavior have not only emerged as an acceptable compromise, but they are perhaps the most pragmatic option. Norms of cyber stability have become more prominent in recent years in response to increased dependence of global political and economic infrastructure on cyberspace and a sharp spike in malicious activity through ICTs, often perpetrated or sponsored by nation states.[219] The protection of ICT infrastructure that economic, social and political activity is dependent on, from external attacks, goes to the heart of the international legal principle of non-interference. Norms agreements allow states to respect this important principle, without appearing to make binding commitments on their behavior.

It is worthwhile to specifically identify those norms that ensure the continuation of ICT activity in a peaceful manner. Central among norms on cyber stability are those that seek to protect critical information/Internet infrastructure (CII) that supports economic and political activity globally. The protection of the "public core" a term that acknowledges in its most minimal conception the critical DNS functions of the Internet, but can be expansively understood to be mean public institutions and infrastructure essential to governance — in particular, is a necessary prerequisite for peaceful use of ICTs. First introduced in 2015, by the Netherlands Scientific Council for Government Policy[220], the idea of the public core has slowly gained acceptance in various other fora including the Internet Society, [221] the UN GGE and with the Government of the Netherlands.[222] Most recently, the Global Commission on the Stability of Cyberspace called for a norm on non-interference with the public core, inclusively defined as routing infrastructure, the domain name system, certificates and communication cables.[223] At its most threadbare interpretation — that of the forwarding and naming functions of the Internet — the protection of the public core represents a norm that all states should and can agree upon. Any activity that disrupts the continued functioning of the Internet by interfering with the essential naming and forwarding functions can have serious impact on use of the ICTs beyond their borders.[224] The protection of the public core, therefore, is twofold: 1) to refrain from interfering with the logical and physical layer of the Internet and 2) to deter non-state actors within a state's territory from doing the same. Similarly, critical information infrastructure (CII), which are potential targets of cyber-attacks and central to a state's domestic economy, are key to ensuring stability in cyberspace.

While it is difficult to comprehensively assess existing norms of cyber stability as they relate to the public core and CII, it is possible to arrive at an indicative list of norms that, when taken together, can largely help prevent, deter and respond to malicious cyber activity. Many of the norms that relate to cyber stability have arisen out of deliberations from the UN

---

[219] Symantec, *Internet Security Treat Report*, Symantec, Volume 21, April 21, 2016 https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

[220] Dennis Broeders, (2015) *The Public Core of the Internet. An international Agenda for Internet Governance*. (Amsterdam: Amsterdam University Press) https://english.wrr.nl/publications/reports/2015/10/01/the-public-core-of-the-internet.

[221] Internet Society, A policy framework for an open and trusted Internet An approach for reinforcing trust in an open environment, (2016): 7. http://www.internetsociety.org/sites/default/files/bp-Trust-20170314-en.pdf.

[222] Government of the Netherlands 'Building Digital Bridges'. International Cyber Strategy. Towards an integrated international cyber policy, (2017): 5. See: https://www.government.nl/documents/parliamentary-documents/2017/02/12/international-cyber-strategy.

[223] Global Commission on the Stability of Cyberspace, *Call to Protect the Public Core of the Internet,* November 2017, https://cyberstability.org/wp-content/uploads/2017/11/call-to-protect-the-public-core-of-the-internet.pdf.

[224] Government of the Netherlands 'Building Digital Bridges'. International Cyber Strategy. Towards an integrated international cyber policy, (2017): 5. See: https://www.government.nl/documents/parliamentary-documents/2017/02/12/international-cyber-strategy.

GGE while others have been a result of bilateral negotiations among states or have been unilaterally forwarded by certain actors. The latter norms have also seen varying degrees of subsequent success in acceptance and adoption by other states. The evolution of these norms can provide lessons for future processes of norm development.

An example of a successful norm is the one concerning the unacceptability of cyber-enabled theft of intellectual property for commercial gain. This norm was a result of the US-China bilateral agreement of 2015 and is argued to have contributed to a subsequent reduction in Chinese attacks on US companies.[225] The agreement has also paved the way for similar bilateral agreements between China and other countries such as the UK and Canada recently.[226]

These instances signify that the success or failure of a norm is determined by a complex set of factors, including the forum where the norm is introduced, the actor forwarding the norm and the problem that the norm seeks to address among many other critical factors. Therefore, any metric that is developed to assess the effectiveness of these norms will necessarily have to be flexible enough to take into account the diversity in origins and objectives of the norm, while being quantitatively rigorous to be able to effectuate real world state behavior.

[225] David E. Sanger, (2016), Chinese Curb Cyberattacks on U.S. Interests, Report Finds, New York Times, June 20, 2016, https://www.nytimes.com/2016/06/21/us/politics/china-us-cyber-spying.html.

[226] Reuters, *China agrees to stop cyberattacks on Canadian private sector - Globe and Mail,* June 26, 2017*,* https://www.reuters.com/article/canada-china-cyber/china-agrees-to-stop-cyberattacks-on-canadian-private-sector-globe-and-mail-idUSL3N1JN1AI.

SECTION 3: ASSESSMENT OF NORMS

Norms can "shepherd" behavior in cyberspace by distinguishing between state actions that are acceptable and those that are not.[227] These norms are usually proposed as either positive or negative obligations and gain acceptance when internalized by actors.[228] The functioning of cyberspace is currently maintained through a series of agreements relating to the technical layer of the Internet, such as the management of the DNS and technical protocols. The current threat to cyber-stability, however, emanates from the lack of clear rules of the road or guiding principles that *deter* malicious activity in cyberspace.

Such "negative" obligations emerge not only through a common understanding of what constitutes malicious activity but also through widespread acceptance. Martha Finnemore and Kathryn Sikkink illustrate the process of norm acceptance [229], which involves emergence, cascade and internalization as the three stages of evolution in a norm's lifecycle. Many cyber norms today appear to be at the "emergence" stage – the *what*, *who* and *where*. This involves identifying baseline behavior that the norm seeks to internalize, appealing to different actors whose behavior the norm seeks to regulate and engaging in the most appropriate fora where the norm can be forwarded.

We classify cyber norms into three categories – political, legal and those relating to confidence building measures. The violation of the first category of norms will carry political costs for the state in question, usually in the form of "naming and shaming" costs or other reputational harms. "Legal" norms on the other hand reflect an aspiration by state actors to codify an existing principle of international law in a certain domain, or evolve altogether new rules of conduct. Confidence building measures comprises mechanisms that facilitate inter-state cooperation, information exchange and verification mechanisms and capacity building exercises aimed at flagging, mitigating and responding to cyber attacks.

With states increasingly adopting norms to regulate malicious cyber activities, it is necessary to to develop criteria to assess their effectiveness. While scholars have previously examined what makes a norm successful and studied how states strategize and promote norms internationally, a comprehensive framework on assessment of existing and future cyber norms is yet to be developed. In line with Joseph Nye's assessment of norms in his 2014 GCIG paper,[230] the authors have tried to develop metrics for the categorization and evaluation of norms that the Global Commission on the Stability of Cyberspace, and indeed all interested actors, may use as an analytical tool.

---

[227] Martha Finnemore and Kathryn Sikkink, (1998), International norm dynamics and political change, International organization 52.4 (1998): 887-917.

[228] Toni Erskine and Madeline Carr, (2016), Beyond 'Quasi-Norms': the Challenges and Potential of Engaging with Norms in Cyberspace, International Cyber Norms: Legal, Policy & Industry Perspectives. Tallinn: NATO CCD COE Publications (2016).

[229] Martha Finnemore and Kathryn Sikkink, (1998), International norm dynamics and political change, International organization 52.4 (1998): 887-917.

[230] Joseph Nye, , *The Regime Complex for Managing Global Cyber Activities*, Global Commission on Internet Governance, Paper Series No. 1 (2014).

Table 1: Assessment of existing cyber norms

NORMS	CONTENT Does the content of the norm establish a baseline against which behavior can be measured?	ACCEPTANCE Has the norm been endorsed in formal or institutionalised processes?	ADHERENCE Does the norm adequately target and induce behavioural change from actors in cyberspace?	EASE OF ADOPTION How likely is it that this norm will be adopted by actors in cyberspace?	TESTING Has the norm been tested through occurrences in cyberspace or geo-political developments?	IMPLEMEMTATION Has the norm proven effective in managing state behaviour?
Political Norms						
Not conduct or knowingly support cyber-enabled theft of intellectual property, trade secrets or other confidential business information.	High	High	Medium to High	Easy	Frequently	Effective
Norms relating to International Law						
Recognize the application of international law and the UN Charter to cyberspace.	Low	High	Low	Easy	Rarely	Ineffective
Confidence Building Measures						
Cooperate to exchange information, assistance, prosecution for terrorist and criminal use of ICTs and to address critical infrastructure vulnerabilities.	High	High	High	Medium	High	Low

This is a difficult exercise for a variety of reasons. First, the question of whether norms are effective in regulating behavior, is yet to be settled. As the experience with nuclear arms control or outer space treaty negotiations suggest, states may not be compelled by norms so much as a catastrophic event that shakes their closely held perceptions and interests. Second, there is a growing consensus among experts that success of a particular norm is not merely determined by the content of the norm but also the process through which the norm has been cultivated.[231] Third, the range of actors, instruments and platform through which norms are discussed, expressed and promoted make it difficult to assess its effectiveness through a unified metric. Fourth, the occurrence or non-occurrence of a cyber incident cannot be easily linked to the existence or effectiveness of a norm. Lastly, it is difficult to assess the interaction among norms and incidents where a single cyber incident can signify why some norms succeed and others don't. For instance, an attack against a critical infrastructure can represent the failure of a norm on non-interference, however, post facto cooperation among states, can be considered as the success of a norm on confidence building measures.

The six metrics suggested in this paper – content, acceptance, adherence, ease of adoption, testing and implementation — can be used as a tool to study the relationship of both existing and future norms with real world cyber incidents –are these norms effective in deterring, defending and responding to attacks? A norm that is clear or specific in its content, has been internalised among relevant stakeholders, and is relatively easy to adopt is likely to be successful. Although this is not an entirely reliable metric, how often states invoke specific norms in response to real-world cyber incidents is yet another sign of norm-"internalisation".

CONTENT- THE SCOPE AND SUBJECT OF THE NORM

The metric "content" refers to whether the norm in question establishes a baseline against which state behavior can be measured. The "norm entrepreneur"[232] who promotes it on an international stage defines the content – over time, this language becomes the subject of diplomatic deliberations, pushbacks and compromise. The articulation of the norm is material to creating both a prescriptive and an evaluative force.[233] The norm may prescribe either a positive or a negative obligation, that is, mandating or prohibiting the state from performing an activity.

The norm should be specific and address particular cases of cyber insecurity, and at the same time dynamic to reflect future behavior in cyberspace. Often, consensus can be achieved easily only if the norm is prescribed in a manner of first principles where signatories can easily make a broad commitment. Such a norm, however, would require further clarifications to understand what would constitute as acceptable state behavior in a given circumstance. Norms that lack a specific commitment, however, can often be perceived as less likely to succeed for this reason and will be rated as "low" in the index. The norm on the application of international law and humanitarian law to cyberspace that arose out of the 2013 and 2015 UN GGE consensus, while momentous, was not immediately actionable. In the 2017 UN GGE meeting, a lack of consensus on the application of specific principles like the law of counter measures and self defence caused a deadlock.

---

[231] Martha Finnemore and Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, American Journal of International Law 110.3 (2016): 425-479.

[232] Martha Finnemore, Cultivating International Cyber Norms, America's Cyber Future: Security and Prosperity in the Information Age, 2 (2011): 89-100.

[233] Toni Erskine and Madeline Carr, (2016), Beyond 'Quasi-Norms': the Challenges and Potential of Engaging with Norms in Cyberspace, International Cyber Norms: Legal, Policy & Industry Perspectives. Tallinn: NATO CCD COE Publications (2016).

In contrast, the norm mandating that states not conduct or support cyber-espionage for theft of IP or trade secrets would be rated as "high" under content in this index – since it is actionable, has economic consequences and engages the right actors.

ACCEPTANCE - PLACES WHERE THE NORM IS PROPOSED OR ENDORSED

Acceptance refers to whether the norm has been endorsed in different fora ranging from multistakeholder institutions to multilateral or bilateral platforms. While mere endorsement of the norm is not a signifier of the norm's success, the forum where the norm was endorsed is material to how it is treated by other actors. For instance, a norm promoted by a 'cyber power', such as a US, China or Russia is more likely to invite a debate and in some cases facilitate its acceptance and in other cases lead to automatic opposition. The norm on ICT enabled theft of intellectual property or trade secrets first found in the 2015 US-China agreement was eventually adopted by the G20 and by several other states in bilateral agreements. Similarly, no norm pertaining to the de-militarisation of cyberspace is likely to succeed without the buy-in of traditional military powers.

ADHERENCE - THE ACTORS THAT INTERNALISE THE NORM

The success of a norm is primarily determined by its ability to induce behavioural change among different actors in cyberspace – from rogue states to hacktivists, all driven by different motivations. If a norm fails to target the right actors, it is highly unlikely that "adherence" to the norm by all actors will be high. For this reason, norms proposed and accepted by states with divergent interests are likelier to succeed. If norms arise out of inclusive platforms incorporating states with varying cyber capacities and across political views, the norm will enjoy popular acceptance and consequently, adherence.

EASE OF ADOPTION- THE TECHNICAL CAPACITY AND CAPITAL REQUIRED TO ADHERE TO THE NORM

The ease of adoption of a cyber norm is not determined by any single factor; rather, it depends on a mix of economic and political variables. Norms that are resource intensive are less likely to be accepted by states that lack cyber capacity. For this reason, the norm on due diligence for ensuring that a cyber attack does not emanate from within a state's territory has been found to be unacceptable to many nations that are unwitting hosts for cyber attacks.[234] On the other hand, confidence building measures have been found to be easier to adopt through bilateral agreements and regional groupings with like-minded states.

TESTING- WHETHER THE NORM HAS BEEN INVOKED IN RESPONSE TO CYBER INCIDENTS

Testing of a cyber norm depends on whether the norm has been called into question in response to a real world cyber incident. This does not directly determine the effectiveness of the norm, rather, it focuses on how frequently or infrequently the norm has been invoked in response to the cyber instability it seeks to address. An indicator of successful testing of a norm can be whether it is specifically referred to by political leadership in the aftermath of a

[234] Schmitt, Michael N., In Defense of Due Diligence in Cyberspace (June 22, 2015). 125 Yale Law Journal Forum 68 (2015), https://ssrn.com/abstract=2622077.

cyber incident, whether the norm is listed in a state's bilateral agreements etc. For instance, on the same day that three US intelligence agencies released a summary of Russian interference with US elections, the Department of Homeland Security classified elections as critical infrastructure.235 This had the effect of granting election infrastructure higher normative protections – those that are available to CII – in the aftermath of a cyber incident. Norms that are tested more, are likely to address a pressing concern.

IMPLEMENTATION- WHETHER THE NORM HAS BEEN PROVEN CAPABLE OF INDUCING CHANGES IN STATE BEHAVIOUR

Implementation of a cyber norm is the determination of how effectively the norm is able to deter, prevent or mitigate a cyber incident. The norms assessment would be based on a mix of whether states abide by the norm, whether there are political, economic or legal consequences to non-adherence. For instance, the emerging norm of non-interference with political infrastructure was put to use by the United States in the aftermath of the DNC hack against Russia through economic and political sanctions. A norm will be considered implementable if it is capable of alienating adversarial states and imposing costs on malicious cyber activity. Such a norm will be considered highly effective.

[235] Kaveh Waddel, *Why Elections Are Now Classified as 'Critical Infrastructure'*, The Atlantic, Jan 13, 2017, https://www.theatlantic.com/technology/archive/2017/01/why-the-government-classified-elections-as-critical-infrastructure/513122/.

SECTION 5: NORMS IN CONTEXT

Long established principles in international law such as non-interference and political self-determination were tested last year with allegations of Russian influence operations hanging over the US elections. Multiple US intelligence agencies claimed that the hacking of the DNC server and the spread of disinformation through social media were originating from Russia. Similar incidents of Russian interference have also emerged across multiple states in Europe.[236] These have given rise to a global debate about the ways in which cyberspace is being used to subvert democratic processes and strike at the heart of state sovereignty.

Ironically, the potential of 'Information Operations' to disrupt domestic political processes, that governments around the world are concerned about today, was first brought to the fore by groups of countries led by Russia and China. Starting from 2009, Russia, China and a group of smaller states have been calling for an international treaty on information security that codifies informational sovereignty and the abstinence from using ICT technologies to interfere with States' domestic processes.[237] In 2011, a Russia led coalition, wrote a letter to the UN General Assembly, seeking the codification of a norm to "not use information and communications technologies and other information and communications networks to interfere with the internal affairs of other states or with the aim of undermining their political, economic and social stability."[238] The Shanghai Cooperation Organisation - an international grouping now comprising eight states including Russia, China, India and Pakistan, has reiterated these ideas.[239]

This approach varied significantly from norm creation processes led by the United States and other liberal democracies.[240] While the US and its allies have been focused on applying existing international law to cyberspace, Russia on the other hand has been advocating for creating a new set of rules to govern state behaviour in cyberspace. The US' hesitation with calling for new rules for cyber governance is steeped in skepticism around the idea of 'information sovereignty' that is central to Russian and Chinese perspectives. Information security as a cyber norm, some argue, is linked to state attempts to regulate content for political ends that could result in human rights violations.

---

[236] Vasco Cotovio and Emanuella Grinberg, Spain: 'Misinformation' on Catalonia referendum came from Russia, CNN, November 14, 2017, http://edition.cnn.com/2017/11/13/europe/catalonia-russia-connection-referendum/index.html

[237] Henry Roigas, *The Ukraine Crisis as Test for Proposed Cyber Norms*, Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn 2015, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Roigas_15.pdf.

[238] United Nations, General Assembly, Sixty-sixth Session, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General,* September 14, 2011.

https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

[239] Henry Roigas, *The Ukraine Crisis as as Test for Proposed Cyber Norms*, Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn 2015, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Roigas_15.pdf.

[240] Rob Morgus, *The Normative Bait and Switch - How Russia's Electoral Hacking Might Push Forward its Agenda for the Internet*, New America, December 1, 2016, https://www.newamerica.org/weekly/edition-144/normative-bait-and-switch/.

This assumes significance with the emergence of new reports claiming that the Russians approached the US with an offer mutual restraint in each other's political affairs in the aftermath of the 2016 elections.[241] The meeting between Russia's Deputy Foreign Minister Sergei Ryabkov and US State Department Officials seemingly sought a diplomatic understanding that Russia would stop its interference in US political affairs if the US efforts to promote democracy in Russia. This offer, however, was rejected by the Department of State over a lack of faith in Moscow and given the ongoing investigations into the extent of Russian interference.

Experts are divided over whether a diplomatic agreement such as this would usher in any lasting change. Nevertheless, an extra-legal norm around non-interference can help ensure stability in the interim. While dealing with the important questions of attribution and state responsibility, the history of the norm on non-interference in political affairs through cyberspace offers interesting insights into why its success in the future can help guide other multilateral processes of norm creation. The rule prohibiting states from unlawful intervention is crystallized in customary international law, with the International Court of Justice famously holding in the Nicaragua case that states are permitted by the principle of state sovereignty to make political, economic and social choices freely. That said, in the absence of any consensus on the application of international law to information operations, diplomatic talks and agreements play a crucial role on developing a norm on acceptable state behaviour on non-intervention in the information space.

Unsurprisingly, the United States and Russia are now engaging in efforts to create a dialogue around cyber norms. Whether it succeeds or not, it can hardly be denied that bilateral discussions have in the past borne fruit. The US-China cyber agreement on commercial espionage reportedly resulted in a decrease in the number of cyber attacks emanating from China. There may therefore, be greater value to engaging with adversarial nations more than a group of like-minded countries.

The development of this norm over the next few years will reflect the importance of the metrics highlighted in the previous chapter - that states will need to work with other states that are not "like minded". States will have to arrive at a common understanding of the content of the norm, adequately target crucial states through bilateral frameworks and look to have the broader community endorse it.

Despite Russia and China having forwarded the norm for nearly a decade, the norm has not gained much headway primarily because of US' reticence. However, if US were to initiate this conversation, the possibility of the norm gaining legitimacy would brighten, especially among many European and Asian states. The United States will have to weigh the costs and benefits of agreeing to a norm addressing content on the Internet and the human rights implications of agreeing to such a norm. On the other hand, it is just as likely that these states with differing agendas will not achieve any consensus. This was evident in the appeals of commentators who suggested the US impose stronger sanctions against Russia instead of ceding ground.[242] The implementation of the norm ultimately will depend on the internalization of the norm by Russia, and the bargain implicit in its adherence.

---

[241] John Hudson, *How Secret Talks With Russia to Prevent Election Meddling Collapsed*, Buzzfeed, December 9, 2017, https://www.buzzfeed.com/johnhudson/no-deal-how-secret-talks-with-russia-to-prevent-election?utm_term=.hhBnZaMDa#.khLjGga8g.

[242] AJ Vicens and Dan Friedman, *Cyber Experts: Trump-Putin Group May Not Be a Bad Idea, But Be Very Very Careful,* Mother Jones, July 7, 2017, http://www.motherjones.com/politics/2017/07/a-us-russia-cyber-security-working-group-isnt-a-bad-idea/.

ANNEX: SURVEY CIRCULATED TO CYBER COORDINATOR

NORMS	CONTENT Does the content of the norm establish a baseline against which behavior can be measured? (1: Strongly Disagree – 5: Strongly Agree)	ACCEPTANCE Has the norm been endorsed in formal or institutionalized processes? (1: Not Institutionalized – 5: Highly institutionalized)	ADHERENCE Does the norm adequately target behavioral change from actors in cyberspace? (1: Limited – 5: Expansive)	EASE OF ADOPTION How likely is it that this norm will be adopted by actors in cyberspace? (1: Very unlikely – 5: Very likely)	TESTING Has the norm been tested through occurrences in cyberspace or geo-political developments? (1: Rarely – 5: Frequently)	IMPLEMENTATION Has the norm proven effective in managing state behavior? (1: Highly ineffective – 5: Highly effective)
Ensure that internationally wrongful acts using ICTs do not emanate from within a State's territory.						
Not target or knowingly support ICT activity that intentionally damages critical infrastructure or impedes their use to provide services to the public.						
Not target or knowingly support ICT activity that either prevents emergency response teams (CERTs) from responding to incidents or use CERTs to engage in malicious activity over cyberspace.						
Not conduct or knowingly support cyber-enabled theft of intellectual property, trade secrets or other confidential business information.						

	CONTENT	ACCEPTANCE	ADHERENCE	EASE OF ADOPTION	TESTING	IMPLEMENTATION
Not conduct or knowingly support ICT activity that interferes in the political, economic or social functions of another state.						
Not use proxies to commit internationally wrongful acts through use of ICTs.						
Protect critical infrastructure from ICT threats.						
Ensure the integrity of supply chain and the security of ICT products.						
Promote public-private partnerships and develop mechanisms to exchange best practices of responses to cyber incidents.						
Report ICT vulnerabilities and share information on available remedies for such vulnerabilities.						
Cooperate with the private sector and other stakeholders to effectively regulate technology products.						
Respond to requests for assistance by another state whose critical infrastructure is attacked.						
Cooperate to exchange information, assistance, prosecution for terrorist and criminal use of ICTs and to address critical infrastructure vulnerabilities.						
Adopt a multilateral instrument to harmonize domestic regulations and combat cybercrime.						

	CONTENT	ACCEPTANCE	ADHERENCE	EASE OF ADOPTION	TESTING	IMPLEMENTATION
Not conduct or knowingly support ICT activity that interferes in the political, economic or social functions of another state.						
Not use proxies to commit internationally wrongful acts through use of ICTs.						
Protect critical infrastructure from ICT threats.						
Ensure the integrity of supply chain and the security of ICT products.						
Promote public-private partnerships and develop mechanisms to exchange best practices of responses to cyber incidents.						
Report ICT vulnerabilities and share information on available remedies for such vulnerabilities.						
Cooperate with the private sector and other stakeholders to effectively regulate technology products.						
Respond to requests for assistance by another state whose critical infrastructure is attacked.						
Cooperate to exchange information, assistance, prosecution for terrorist and criminal use of ICTs and to address critical infrastructure vulnerabilities.						
Adopt a multilateral instrument to harmonize domestic regulations and combat cybercrime.						

	CONTENT	ACCEPTANCE	ADHERENCE	EASE OF ADOPTION	TESTING	IMPLEMENTATION
Recognize the right of states to respond to internationally wrongful acts committed through ICTs.						
Recognize the right of states to exercise self defense in cyberspace.						
Recognize the applicability of international humanitarian law to cyberspace.						
Recognize the right to invoke collective self defense in response to cyber attacks.						`

SECRETARIAT

The Hague Centre for Strategic Studies

EastWest INSTITUTE

PARTNERS

Ministry of Foreign Affairs

CSA SINGAPORE

Microsoft

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Internet Society

SPONSORS

Ministry of Foreign Affairs

Of Estonia

SUPPORTERS

Black Hat USA

Packet Clearing House