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, BRATISLAVA 2018

Bratislava, May 2018

GCSC ISSUE BRIEF №2

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 that enhance international security and stability and guide responsible state and non-state behavior in 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.

The opinions expressed in this publication are those solely of the authors and do not reflect the views of the Global Commission on the Stability of Cyberspace (GCSC), its partners, or The Hague Centre for Strategic Studies.

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) is helping to promote mutual awareness and understanding among the various cyberspace communities working on issues related to international cybersecurity. By finding ways to link the dialogues on international security with the new communities created by cyberspace, the GCSC has a genuine opportunity to contribute to an essential global task: supporting policy and norms coherence related to the security and stability in and of cyberspace.

Chaired by Marina Kaljurand, and Co-Chairs Michael Chertoff and Latha Reddy, the Commission comprises 25 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 will be linked to existing initiatives, such as the Global Commission on Internet Governance and the London Process, through Special Representatives.

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.

As a result of the Commission Meeting in New Delhi in November 2017, the GCSC issued a set of Requests for Proposals (RFPs) for four research projects. The Commissioners selected the winning proposals at the Commission Meeting in Lille, France, in January 2018. The researchers received the funding associated with the RFPs and were invited to present their work to the Commissioners during the Commission Meeting in Bratislava in May 2018.

TABLE OF CONTENTS

BRIEFING 1
ADAPTATIONS TO ENHANCE THE STABILITY OF CYBERSPACE

Prof. Shen Yi, Director, Research Center for the Governance of Cyberspace, Fudan University

Dr. Jiang Tianjiao, Researcher, Research Center for the Governance of Cyberspace, Fudan University

Ms. Wang Lei, Research Assistant, Research Center for the Governance of Cyberspace, Fudan University

BRIEFING №1

REDEFINING STABILITY / INSTABILITY OF CYBERSPACE

Though scholars and policymakers have mentioned and analyzed “stability” or “instability” of cyberspace repeatedly, the concept has to be redefined. We argue that relevant existing discourses have failed to describe the essence of stability or instability of cyberspace, despite some enlightening arguments that are beneficial for further discussion. We believe a new theoretical framework is needed to define the stability of cyberspace from a structural perspective, through which coordinating core interests of sovereign states is both possible and an effective instrument for managing threats in global cyberspace.

Cyberspace has been viewed over time as a space of instability as a result of the rising risks of asymmetric strikes that technology-dependent countries are facing. In this theory, the popularization of information technology and the low costs of launching cyber attacks prompt actors like revisionist countries and non-state actors to target advanced countries. Lucas Kello (2013) has summarized the mechanism, pointing out that instability derives from technical characteristics of cyber offense and defense, including offense dominance, attribution difficulties, technological volatility, poor strategic depth, escalatory ambiguity, as well as low barriers for actors to enter cyberspace. Some Chinese scholars (Ren, 2014) also stress this logic leading to strategic instability in cyberspace, which is widely expressed as “cyber Pearl Harbor” or “cyber 9/11”. This theory defines instability of cyberspace as a status that some states or non-state actors may take advantage of cyber technology to launch asymmetric attack against developed countries, which in turn has a huge impact on the existing order in the real world.

Criticisms arise in recent years towards this perception of strategic instability in cyberspace, claiming that it exaggerates the effect that cyber attacks can exert. Erik Gartzke (2013) made an effort of “bringing war in cyberspace back down to earth” by demonstrating that cyberwar alone cannot meet the objectives that can be achieved through traditional military violence. Gartzke and Lindsay (2015) then refuted the proposition of offense dominance in cyberspace by advocating the function of deception strategy. Based on these arguments, cyber deterrence is thought of as a credible instrument for dealing with cyber attacks (Shen and Jiang, 2018). While accepting this view, we disagree with the idea that misperception of the dynamics of cyber offense and defense means an exaggeration of instability in cyberspace, and believe instability is rooted in the very structure of cyberspace[1], which contains misperceptions and divergences among state actors. The international society is still far away from forming a consensus on principles of conducting cyber offense and defense, notwithstanding the rising assertion on limitations of cyber attacks, let alone contradictions on more issues including the role of state actors in cyberspace and the approach of defining interests of different actors. In this situation, the main reason for cyber attacks among state actors becomes misjudgments about actors of other states and the vision that attacks are superior to defense in cyberspace, rather than ideological divergence between advanced countries and revisionist states. As a result, with developing countries increasing their dependence on information technology, any country and actor can become the victim of cyber attacks. Events in Estonia, Iran, Russia, France, and the United States represent this situation:

[1] The term “structure” used here is used in the framework of the theory of International relations in which it is mainly defined by the distribution of power among different actors, mainly represented by the nation-state.

none of these states could afford to tolerate those behaviors produced in cyberspace to affect their national security via either attacks on infrastructure or via organized manipulation of social media during a critical domestic political process. That is the main reason we should focus more on how to find a pragmatic path toward building strategic stability in cyberspace.

To define from a structural perspective, instability of cyberspace could be understood as a certain digital version of the anarchy in the real world. Although states still seek self-preservation and maintenance of security and stability of property in cyberspace, they have not found a way to build the bases of a "society of states" in terms of common interests, values, and rules. While there exists a sovereignty doctrine that lays the foundation for coexistence among nation states in the real world, global cyberspace operates in the absence of consensus on basic norms, principles, and rules on two tiers — the state-state tier and state-non-state tier.

On the state-state tier, scarcity of both norms on the macro level and appropriate behavior principles for cyber offense and defense on the micro level remains the status quo. The scarcity makes the state actors fall into a dilemma that, while almost all the states regard cyber attacks on their information assets as a violation of their sovereignty, they also try their best to develop their own capacity to launch operations in the cyberspace which include attacks, defense and espionage that make themselves feel safer. Though it is not widely accepted, one of the most important steps to save the state from that dilemma is to recognize the application of sovereignty in the cyberspace. Theoretically, it is not that difficult to understand why sovereignty could be applied into cyberspace: According to the latest version of the Tallinn Manual 2.0, "the physical, logical, and social layers of cyberspace are encompassed in the principle of sovereignty "(Michael N. Schmitt, 2017, p. 12), and "the International Group of Experts did not adopt them on the ground that they disregard the territorial features of cyberspace and cyber operations that implicate the principle are conducted by persons or entities, over which States may exercise their sovereignty prerogatives" (ibid.). But this kind of understanding still needs a proper time to be widely accepted so that it will finally transform into a de facto norm.

At the practical level, it is quite clear that the applicability of cyber sovereignty has not received wide recognition among state actors. As a result of this dilemma, a large number of information resources and end users are exposed to invasions from both state actors and non-state actors without a legal approach to be protected. The problem is, essentially, that (1) the distribution of ICT capacity among states is uneven; and (2) in an anarchic world, states cannot have 100% trust in each other. The result is that only if the core security of states can be ensured via acceptance of sovereignty principle will there be enough driving force to launch the cooperation to build a sufficient legal framework in the cyberspace.

The lack of consensus on behavior principles for cyber offense and defense is the main reason for risk of conflict escalation among states. In the current situation, states generally favor first strikes in cyberspace on the one hand, and are liable to make misjudgments on the cyber threats they are facing on the other hand. The deficiency of common rules on action, especially the belief of offense dominance in cyberspace, aggravates the security dilemma among states. On the state-non-state actors tier, the two types of actors in cyberspace are competing for governance rules in global cyberspace; state actors try to deny the autonomy and authority of non-state actors in cyberspace governance while the private sector and civil society are seeking to dominate the establishment of global cyberspace governance institutions, excluding the functioning of state actors – though state actors often declare that they would like to promote cyberspace governance through cooperation with private sectors. To solve the tension between sovereignty doctrine and public good of global cyberspace is not an easy task for state actors, while denial of state actors' role in cyberspace by private sectors will also cause disorder and increase the difficulty in making rules.

On the basis of confirming the sources of instability in cyberspace, the stability of cyberspace should be considered as a process of state actors and the private sector working toward common norms and rules applied in cyberspace to respect and coordinate core interests of each actor, limit respective behaviors and manage cyber threats effectively. In short, on the sovereignty issue in cyberspace, it could be briefly concluded as follows:

Firstly, the international system of sovereign states existed well before the revolution of cyber technology. The evolution of cyberspace and its further development can hardly be achieved without the recognition and cooperation of sovereign states. Yet such cooperation rests on the premise that sovereign states believe cyberspace will not threaten their national regime and security.

Secondly, in order to maintain the development of cyberspace, it is important to prevent sovereign states from choosing to either join global cyberspace or to damage their own national security. When facing serious threats, any countries will take radical measures such as cutting off the network. However, the value of cyberspace is to keep connected countries and users as much as possible. If such connection brings political risks including a threat to the regime survival, the value of cyberspace will decline rapidly.

Thirdly, sovereignty has a double meaning in terms of internal and external affairs. When some observers express their concerns about the concept of sovereignty in cyberspace, they only refer to the domestic sovereignty and argue that respect for sovereignty will lead to barriers separating cyberspace. However, with the further development of global cyberspace, external sovereignty deserves more attention. Whether developed or underdeveloped, all countries have equal rights to join in the development of cyberspace and further their interests. The principle of Common Heritage of Humankind raised by the United Nations when dealing with other global commons provides a good example here. For any country, the weakness of technical capability should never affect the legal rights of self-preservation.

CORE INTERESTS OF SOVEREIGN STATES IN CYBERSPACE

The key to the stability of cyberspace is to make clear the core interests of sovereign states. Approaches from both a normative perspective and on an operational level have been proposed by scholars, think tanks and international organizations to enhance the stability of cyberspace. The effect of these approaches, however, is limited due to their ambiguity in identifying the aforementioned key to cyberspace stability. We intend to define the core interests of a sovereign state beyond the continuous debate between doctrines of cyber sovereignty and global commons. An inclusive definition of core interests of sovereign states and a mutually supportive relation with public core of the Internet will provide a framework for pursuing stability of cyberspace on both normative and operational levels.

In recent years, the most mentioned stabilizers of cyberspace include norms and cyber deterrence. Norms can act on the relationship among actors in cyberspace to improve confidence and transparency. Deterrence, as Joseph S. Nye Jr. (2016/17) has argued, can function through cultivating actors' knowledge on costs and benefits of cyber operations, and advocators of cyber deterrence hold that cyberspace will be stabilized through strengthening the credibility of deterrence. It is a fact that norms and cyber deterrence can contribute to the stabilization of cyberspace, but existing narratives are insufficient in pointing out how the two factors can work properly and effectively for the objective of stabilizing global cyberspace. Firstly, for many discussions, the starting point is to protect interests of individual countries or partial countries in the world. Though talking about common norms applied in cyberspace, some scholars and organizations (Kramer, 2012; International Security Advisory Board, 2014; Mazanec and Thayer, 2015) only regard cyber norms as an expected outcome of cooperation among the United States and its allies. Global cyberspace is divided on the basis of ideology, which will impede the formation of common norms to integrate cyberspace. The aim of conducting credible cyber deterrence is limited to protecting the interests of individual countries so that the possibility of an arms race in cyberspace cannot be excluded. Secondly, how norms and deterrence can deal with the tension between state actors and non-state actors in cyberspace remains to be further explored. In practice, nation states are leaving the opportunity of making rules for cyberspace to non-state actors for fear of being constrained by binding rules, especially those referring to arms control or dealing with arms conflicts in cyberspace (Macak, 2017). Against this background, the dominating force of the rule-making process in cyberspace is yet to be decided given the significant role of state actors, as well as the voices supporting coordinating actions among nation states in cyberspace. When urging nation states to lead and cooperate for rule-making, people have not clearly answered the question that how nation states can apply a set of norms and rules that are both beneficial for all the nation states and the private sectors in cyberspace. Thirdly, whether norms and cyber deterrence can harmonize with each other for the stability of cyberspace is still controversial. Some scholars (Mazanec and Thayer, 2015) consider fostering norms as a way of guaranteeing the effectiveness of cyber deterrence, while some others (van der Meer, 2015) think cyber deterrence entails a risk of conflict escalation among countries and is not compatible with norms in the process of reducing instability in cyberspace.

To address the deficiencies, the stability of cyberspace should be built on normative and operational approaches with a renewed theory on subjects of the approaches and an inclusive way to cope with interests of different actors in cyberspace. We here propose a focus on the core interests of sovereign states. This concept contains two main elements: nation states as the dominating force of the rule-making process in cyberspace act as the protective power of both national and private interests, including the public core of the Internet; it is through coordination and coexistence of the core interests of sovereign states, on the basis of unbiased stipulation and distribution of rights and obligations among state and non-state actors, that a community of global cyberspace can be established.

The concept of core interests of sovereign states accepts the proposition that the sovereignty doctrine applies to cyberspace, while taking a further step to deal with the antagonism between cyber sovereignty and other claims in cyberspace. The sovereignty principle has been adopted by some countries and multilateral platforms as a basic norm for cyberspace governance. The 2013 UN GGE report is an example, claiming that "state sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory". "Sovereignization" of cyberspace is a result of the fact that development of cyberspace depends on the information infrastructures and net users that belong to sovereign states (Huang, 2017). The sovereignty doctrine applied in cyberspace does not only imply sovereign states' rights in governing the information assets within borders, but also adds constraints on state actors for respect and admission of the rights with each other, thus laying a foundation for a rule-based cyberspace in which state actors play significant roles. Despite this, at least three concerns raised toward the sovereignty doctrine in global cyberspace cannot be ignored. For one, there is concern that the sovereignty doctrine and countries' corresponding policies add barriers to the cross-border free flow of data (Information Technology & Innovation Foundation, 2017), which is a widespread value in cyberspace. Second is the reality that those who stand for the sovereign doctrine in cyberspace do not share a common view on the merits and origins of information sovereignty (Zeng, Stevens and Chen, 2017), which usually refers to the rights of sovereign states to control and manage cross-border information flows. Moreover, the way of implementing the sovereignty doctrine on a practical level for actors in cyberspace has yet to be clarified, which poses another challenge. The concept of the core interests of sovereign states provides an approach to deal with these concerns while adhering to the sovereignty doctrine in cyberspace.

The core interests of sovereign states are an aggregation of interests on three layers, extending the narrow definition of information sovereignty. The first layer is the interests related to regimes of a national government and national security. This layer of interests implies that state regimes and their political activities should avoid interference from the outside by means of information, and the confidentiality, integrity, and availability of sovereign states' critical infrastructure should be protected against cyber threats. The second layer of interests focuses on the operation of ICT companies. In the globalized era, information infrastructure and applications worldwide build on the sufficient cooperation and orderly competition among ICT companies. The growth of ICT companies forms a part of the cyber capacity of sovereign states, and the growth cannot be achieved without a stable and flourishing global market. Therefore, this layer of interests of sovereign states closely connects with the status of global markets so that it cannot be gained through actions going against the development of global markets. Finally, the rights of access to the Internet of end users and their privacy rights constitute the third layer of interests. Promoting the individual rights is both the objective of developing information and telecommunication applications as well as a guarantee for the prosperity of cyberspace.

The multi-layer approach of defining the core interests of sovereign states indicates several critical features of the new theoretical framework committed to the stability of cyberspace. Firstly, protecting the core interests of sovereign states is not just a zero-sum game in the context of cyber, but reveals the possibility of enhancing cooperation among state actors in cyberspace without sacrificing the interests of some states. In cyberspace, the interests of a sovereign state cannot be gained without respecting the interests of other sovereign states and stability of the whole cyberspace. In order to achieve growth of domestic ICT companies, for example, nation states have no choice but to cooperate with each other in the globalized market. Secondly, the core interests of sovereign states and the public core of the Internet are supplementary to each other. In late 2017, the Global Commission on the Stability of Cyberspace issued a call to protect the public core of the Internet, which is believed to be significant to the stability of cyberspace. Elements of the public core here are defined as including Internet routing, the domain name system, certificates and trust, and communication cables. Based on the definition of core interests of sovereign states, the interests comprise nation states' commitments and obligations to the public core of the Internet.

Meanwhile, it's quite clear that there are two different understanding of the nature of the Internet and cyberspace produced by the spread of the Internet in a post-Cold War world: One version, represented by the IGF-BPF submission, is based on "global public good approach" and clearly implies that part of the Internet is "by nature" outside of state sovereignty. This version of understanding could also be described as the production of cyber-libertarian ideology which came from "A Declaration of the Independence of Cyberspace" (Jacob Silverman, 2015). The other version, in a more pragmatic (or, in other words, realistic) way, is the global cyberspace wherein nation states play a basic role; the public core of the Internet will be rootless if it does not acknowledging the role of state actors and accepting the framework of sovereign states' interests. From the structural perspective of cyberspace stability that has been described, unequal distributions of rights and obligations among state and non-state actors may do special harm to cyberspace stability. However, defining the core interests of sovereign states finds a way of promoting equality among sovereign states in cyberspace through redistributing their rights and obligations in a standardized way.

Last but not the least, it makes the pursuit of cyberspace stability a pragmatic and practical process by integrating the normative and operational levels. Coordinating the core interests of sovereign states not only clarifies the common norms that should be respected and accepted by nation states but also provides a guide to specific behavior principles for nation states in cyberspace.

OPERATIONAL FRAMEWORK FOR THE STABILITY OF CYBERSPACE

On the basis of redefining stability of cyberspace and proposing the concept of the core interests of sovereign states, enhancing the stability of cyberspace is still a difficult process that can only be achieved through exploring concrete measures. The central missions include promoting actors in cyberspace, both state actors and non-state actors, to accept the norms about rights and obligations required by the core interests of sovereign states, and to form institutions and procedures to guarantee the implementation of the norms.

In anarchy, actors in cyberspace (especially the state actors) will not always abide by the norms stemmed from the core interests of sovereign states. Though self-interests are thought of as the starting point for nations to take actions in global politics, the proposed norms of the core interests of sovereign states differ from the concept of self-interest to some extent by requiring state actors to constrain their own actions and take more responsibilities for the interests of private sectors and individuals other than that of state regimes both domestically and internationally. In this situation, actors like international organizations can play a significant role in promoting the legalization of the norms worldwide with the aim of creating a global environment that state actors have to determine and justify their own behaviors in cyberspace according to the norms. On one hand, international organizations including Global Commission on the Stability of Cyberspace can act independently as a platform for knowledge creation, accumulation and sharing with regards to specific norms and rules in cyberspace. On the other hand, norms cannot be practiced without participation of nation states so that it is feasible for international organizations to hold dialogues among nation states about the topic of cyberspace stability, aiming at collecting nation states' public support to the norms and rules. States and international organizations can also cooperate in conducting a set of institutions and procedures to encourage normative behaviors and punish the actions that violate the norms and rules and pose threats to the stability of cyberspace.

Specifically, the primary step is to formulate norms for the global cyberspace that are explicit, detailed and practical. Among the complex tasks that have to be accomplished, the primary work of knowledge creation led by international organizations is to define "responsibility" of state actors in cyberspace, and describe what a responsible state actor in cyberspace looks like. According to the concept of core interests of sovereign states, all the nation states in the world share common obligations of protecting the interests of diverse actors within the territory and undertaking the responsibility of respecting the national security of other countries, and contributing to the public core of the Internet. Non-territorial actors represented by iCANN, IETF, W3C and so on, could launch their activities inside certain borders which heavily depend on their relationship with one or more state actors.

On the basis of the value of actors' responsibility, norms and rules about the stability of cyberspace should contain a set of evaluation criteria that can be used to judge whether nation states meet the requirements about their responsibilities in cyberspace. The criteria are composed of several specific standards so that nation states' behaviors and contributions, both domestic and international, to the stability of cyberspace can be evaluated and compared with each other. Learning from existing indexes, like the cybersecurity index produced by international organizations, a new index can be created to serve the evaluation so as to improve the attractiveness of the norms. Furthermore, rules about how states and non-state actors should react to threats to the core interests of sovereign states are also an important part of the norms for cyberspace stability. The legalized procedures that are to be formulated and implemented for the rules should clarify the permissible situations in which nation states can take defensive actions through international channels or even moderate retaliation according to certain international regulations. It should also be clearly regulated about the situations and approaches for international organizations or the international community to take common actions to deal with threats to the stability of cyberspace. For the creation of norms and rules on these aspects, we suggest establishing a workshop led by Global Commission on the Stability of Cyberspace to convene experts and conduct research on glossaries including "cyberspace security", "cyberspace governance” and “cyberspace stability”. This workshop will mainly rely on the academic communities composed of researchers and experts rather than officials from the governments. Moreover, the main job is to take the first step toward stability via building common knowledge about the know-how of the strategic stability in cyberspace.

Then, a knowledge base can be built to collect a variety of threats to the stability of cyberspace. All of the experts can select the common threats and add them into the knowledge base just like the operation of Wikipedia. Experts from different countries will engage in countermeasure brainstorms and bring the unsolved problems back in order to have further discussions at the state level. If the state-level measure is effective, it can be recorded in the knowledge base and spread worldwide.

The next step is to design and operate international institutions, which have better legal positions via representing more state actors whose technical capacity is quite weak, that urge actors in cyberspace to comply with the norms and rules and also allow them to protect their own interests normatively. In fact, the aforementioned contents of norms and rules have implied that international institutions in this regard can be developed on at least two aspects: one is an evaluation and supervision regime in which state actors’ behaviors and their impact on stability of cyberspace can be reviewed; the other is a reaction regime in which both state actors and non-state actors can take actions accordingly to maintain core interests of sovereign states and the stability of cyberspace. For the former one, apart from the measure of an index that has already been proposed, an effective evaluation regime should be conducted through combining evaluation of nation states’ behaviors led by international organizations and self-evaluation and comments issued by nation states. This combination can make the evaluation regime both a constraining force on states’ behaviors as well as an opportunity for discussion of norms and practices among nation states. The reaction regime should be established in the framework of United Nations to guarantee its legitimacy, with the help of specialized international organizations on cyber issues. This regime can contain three types of regulations in the face of threats to the stability of cyberspace. First is regulation about the threat situations in which nation states can act automatically to defend against the threats. What should be expounded by the regulation is that in certain situations, comprehensive measures – not only counterattacks in cyberspace but also diplomatic actions - can be taken appropriately by nation states to protect their core interests against cyber attackers. This can add to the effectiveness of legitimate defense while helping limit the risk of conflict escalation and an arms race in cyberspace.

The second type of regulation provides a channel for nation states to appeal to authoritative international organizations asking for arbitration or collective action of the international community to cope with threat sources in the world. Of course, it would face the risk of paralysis by lack of agreement, but the UN chapters would also provide the benefit since one of its foundations is to respect the equality of sovereignty. Compared to the risk, it would bring more benefits by decreasing the unnecessary concern of those weak actors on how to ensure the security of their critical interest via accepting the regulation.

Last but not least, international organizations like the United Nations should have the authority to judge, according to certain procedures, whether the stability of cyberspace and key interests of certain actors are severely threatened by some actors, and in these situations, criticisms and collective actions toward the threat sources in cyberspace are likely to be effective solutions for international organizations to enhance the stability of cyberspace.

REFERENCES

1. Gartzke, Erik. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” *International Security* 38, no.2 (Fall 2013): 41-73.

2. Gartzke, Erik, and Jon R. Lindsay. “Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace.” *Security Studies* 24, no.2 (2015): 316-348.

3. 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.

4. Huang, Zhixiong, ed. *On Cyber Sovereignty: Jurisprudence, Policy and Practice*. Beijing: Social Sciences Academic Press, 2017.

5. Information Technology & Innovation Foundation. “Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?” May 2017. http://www2.itif.org/2017-cross-border-data-flows.pdf.

6. International Security Advisory Board. “Report on a Framework for International Cyber Stability.” July 2, 2014. https://www.state.gov/documents/organization/229235.pdf.

7. Kramer, Franklin D. “Achieving International Cyber Stability.” Atlantic Council, September 2012. http://www.atlanticcouncil.org/images/files/publication_pdfs/403/kramer_cyber_final.pdf.

8. Kello, Lucas. “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft.” *International Security* 38, no.2 (Fall 2013): 7-40.

9. Macak, Kubo. “From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers.” *Leiden Journal of International Law* 30, no.4 (2017): 877-899.

10. Mazanec, Brian M., and Bradley A. Thayer. *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace*. London: Palgrave Macmillan, 2015.

11. Nye, Joseph S. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no.3 (Winter 2016/17): 44-71.

12. Ren, Lin. “Information Transmission Mechanism in the Cyber Era and Its Challenge to the Traditional Strategic Interaction.” *World Economics and Politics* 11 (2014): 73-90.

13. Schmitt, Michael N. ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press, 2017.

14. Shen, Yi, and Jiang Tianjiao. “Offence-Defense Balance in Cyberspace and a Proposed of Cyber Deterrence.” *World Economics and Politics* 2 (2018): 1-21.

15. United Nations General Assembly. “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” June 24, 2013.
http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

16. Van der Meer, Sico. “Enhancing International Cyber Security: A Key Role for Diplomacy.” *Security and Human Rights* 26, no.2-4 (2015): 193-205.

17. Zeng, Jinghan, Tim Stevens, and Yaru Chen. “China’s Solution to Global Cyber Governance: Unpacking the Domestic Discourse of ‘Internet Sovereignty’.” P*olitics & Policy* 45, no.3 (2017): 432-464.

MEMO 1
PROMOTING AN INTERNATIONAL SECURITY ARCHITECTURE FOR CYBERSPACE

|

PRE-NORMATIVE APPROACHES TO BUILDING CONSENSUS

Ms. Elana Broitman, Director, New America NYC

Ms. Mailyn Fidler, Fellow, New America's Cybersecurity Initiative

Mr. Robert Morgus, Senior Policy Analyst with New America's Cybersecurity Initiative

MEMO №1

INTRODUCTION

This paper addresses the question of how the international community can make more progress on widening, broadening and deepening international consensus on the architecture of cybersecurity at a time when reaching formal agreement appears to be stalled. The broadly held view is that despite some progress within the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) process over the course of over twelve years, the nadir in trust among nation-states with significant cybersecurity capabilities has negative implications for getting to a treaty.

The failure of the 2017 GGE to achieve consensus was only one of many signs that time is not ripe for reaching a global international cybersecurity agreement. The continued dissonance between the United States' position of advocating for Russian and Chinese[2] adherence to the Convention on Cybercrime, commonly known as the Budapest Convention, on the one hand, and the Russian and Chinese approach to framing cybersecurity as information security, has not diminished. Yet cyberattacks have grown more serious in their reach and impact, prompting the need to continue to move forward.

Given these dynamics, this memo advances the concept of a "pre-normative" approach of continuing, widening and deepening a commitment to improved cybersecurity through continuous contact, practical measures, capacity building, and sector-based incremental agreements that maintain and increase areas of consensus, preparing the ground for a formal global agreement when a window of opportunity opens. The particular mechanisms for such "pre-normative" work are not new, but what this memo suggests is that the more practical and technical such measures, the more likely they are to gain momentum and help expand formal and inferred consensus.

With this in mind, the document first explores "pre-normative" theory, followed by a review of sample case studies in parallel pre-normative tracks.

PRE-NORMATIVE THEORY AND DISCUSSION

"Norms" traditionally refer to comprehensive treaties and agreements, which tend to move slower than the advancement of technology, and rely on political and policy convergence that has not been found among the key global stakeholders in cybersecurity.

In contrast to classic treaty making, "socialization, persuasion, and ideation"[3] have become increasingly important norm setting levers. To paraphrase Joseph Nye's idea of "soft power," "the ability to affect others by attraction and persuasion"[4] establishes conditions for normative enforcement that are critical to realizing those norms in practice. Professors Nye and Robert

[2] For more fluid sentence flow, this memo uses Russia rather than the formal name of the country, Russian Federation, and China rather than People's Republic of China.

[3] Anne-Marie Slaughter and David Zaring,"Network Goes International: An Update," *Annual Review of Law & Social Science Vol. 2*, No. 2007-12 (February 2007): 214, https://www.annualreviews.org/doi/pdf/10.1146/annurev.lawsocsci.1.041604.120026.

[4] "How Sharp Power Threatens Soft Power: The Right and Wrong Ways to Respond to Authoritarian Influence," Snapshot, Foreign Affairs, last modified January 24, 2018, https://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power.

Keohane identified a trend of international norm building through "contacts, coalitions, and interactions… not controlled by the central foreign policy organs of governments."[5] These soft norms are not replacing intergovernmental agreements, but have gained importance in leading the way to building awareness and an impetus for eventual agreement among important stakeholders. Thus the "pre-normative" approach is a combination r of different pathways toward building a comprehensive formal agreement.

Since Nye's early work on this topic, a number of scholars have noted the importance of incremental approaches to developing governance. As Anne-Marie Slaughter has explained, political science, environmental and trade policy work have examples of structured cooperation among informal networks of multiple stakeholders, providing an opportunity for greater cooperation and even "law-making."[6] This can take shape in a number of ways. Scholars have noted examples of "local problem-solving experiments"[7] that support formal normative development. Also notable are working solutions among government agencies that do not represent the foreign policy interests of states, but rather work in cohorts framed by areas of responsibility, such as law enforcement, banking and environmental work. Such cohorts are noted for being capable of shaping "soft law agreements" that produce global governance.[8]

There has also been a veritable explosion of international bodies and convenings of civil society, academia, and industry joining government representatives. Many work on policy development and best practices. These structures are often more nimble, less constrained by large bureaucracies and rules, and in a position to more easily incorporate multiple stakeholders in decision making. They help support implementation and adherence without which agreements don't truly become norms. As Slaughter notes, "That problems of governance have become increasingly global is a truism. But it is worth remembering that globalization is not the result of an agreement by important heads of state but rather is something that has resulted from the increasingly global outlook of" governments, civil society, the corporate sector and grassroots involvement fed by more diverse and constant media coverage.[9]

The likelihood is that a series of incremental, parallel approaches - both formal and informal - must be tested in order to pilot and drive consensus. Rather than relying on a single initiative, the goal of this approach is to leverage a variety of mutually supportive opportunities to build consensus and trust, and couple this with a public education effort that creates constituent

[5] Joseph S. Nye and Robert O. Keohane, "Transnational Relations and World Politics: An Introduction." International Organization 25, no. 3 (1971): 329-49. http://www.jstor.org/stable/2706043.

[6] Slaughter and Zaring, *Network Goes International*, 215.

[7] Ibid., 219.

[8] Galbraith, Jean & Zaring, David, "Soft Law as Foreign Relations Law," Cornell Law Review, Volume 99, Issue 4 May 2014 pp 753-754, http://cornelllawreview.org/files/2014/05/99CLR735.pdf.

[9] Anne-Marie Slaughter and David Zaring, "Network Goes International: An Update," Annual Review of Law & Social Science Vol. 2 [December 2006]. The centerpoint for most global issues is the scaling mechanisms and replicating solutions across vastly different communities, see Anne-Marie Slaughter, *The Chessboard and the Web: Strategies of Connection in a Networked World* [New Haven: Yale University Press, 2017], Chapter 6.

support for new practices and standards.[10] The goal of this model is to prepare the groundwork for a formal global cybersecurity agreement when the political opportunity is ripe.

While this memo advances the notion of multiple approaches, it also highlights certain traits that offer particular strengths in supporting normative development at a time of increased sensitivity:

Confidence and Capacity Building Measures build trust, socialize normative principles and develop a constituency that can better support agreements when political opportunity arises.

- While agreements are harder to achieve, incremental agreements may be possible even at this stage because their narrow scope can gain consensus easier. Incremental agreement test norms and can lead to broader adherence by a larger set of stakeholders as long as they are not framed on the basis of political or subjective distinctions among countries.
- In all these approaches, multi-stakeholder participation is important for both consensus development and implementation.
- Memorializing principles, best practices and incremental agreements can remind stakeholders of areas where consensus exists and thus expedite future negotiations.

The next section distills lessons from case studies in cybersecurity and other domains, and their potential contribution to building the cybersecurity architecture.[11]

PRECEDENTS FOR CONSENSUS DEVELOPMENT IN CYBERSECURITY AND ANALOGOUS AREAS

A. CONFIDENCE AND CAPACITY BUILDING MEASURES:

While formal agreements can stalemate over entrenched policy positions, confidence building measures (CBMs) can lead to breakthroughs, and capacity building programs can deepen constituencies that help break through political deadlocks. These measures create more transparency, promoting trust among key stakeholders - important for fruitful negotiations. They operationalize good practices that have the potential to become formal "norms," and build a constituency for normative development when the political and diplomatic ground is ripe for such work. Even the 2015 GGE consensus document recommended a series of CBMs and capacity-building recommendations.[12]

[10] Paul Costello, "Creating Inclusive Policies Through Storytelling," German Marshall Fund of the United States, 2017, last modified February 8, 2017, http://www.gmfus.org/blog/2017/02/08/creating-inclusive-policies-through-storytelling.

[11] The Global Commission has briefing papers providing a catalog of diplomatic initiatives. Such work is also available from other bodies such as UNIDIR and Carnegie, as well work describing the Bildt Commission, ITU's work, efforts to build on the Budapest Convention, and others. This paper will assume a knowledge of such mapping, and thus will focus on examples of interesting theoretical approaches to diplomatic work, as well as the confidence and capacity building measures that would further and complement such work.

[12] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," Seventieth Session, A/70/172, p. 9-13, last modified July 22, 2015, http://undocs.org/A/70/172.

Technical Cooperation Builds Trust

One of the most effective examples in cyberspace has been the Asia Pacific Computer Emergency Response Team (APCERT) where Computer Security Incident Response Teams (CSIRTs) in the Asia Pacific region coordinate incident response and other activities. The very fact that it has doubled in size from its origins to encompass 31 teams from 21 economies is a testament to its usefulness for many countries.[13] According to Yurie Ito, former Chair of APCERT, the "members have built trust and operational collaboration across regions with significant cultural differences . . . [and despite] different approach[es] to governmental control of information and the related authority over ISPs to block traffic."[14]

Indeed APCERT's membership includes approaches to the Internet as diverse as China, on the one hand, and Australia and Japan, on the other. Yet despite these differences, for fifteen years the CSIRTs have managed to work across boundaries to help each other address cyber incidents. They do not get into the more sensitive questions of attribution, but they do share information and best practices, they mutually assist each other, and they collaborate on research and training.[15] As Ito has pointed out, these collaborations have led to a realization that their security depends on each other. This very practical acceptance of inter-relationships lends itself to an appreciation for the benefit of norms in the cyber arena. Even if the normative support develops around narrow areas on which the CSIRTs cooperate, such cooperation provides the basis for expansion into other parts of cybersecurity over time.

The APCERT confidence building has lent itself to a normative initiative in spite of broader strains in international relations. In 2005, China's, Japan's, and South Korea's information technology ministers signed a Memorandum of Understanding to build a framework of information sharing and cooperative incident-handling procedures to control cyberattacks and mitigate the consequences of these activities (the "CJK Initiative").[16] Despite the diplomatic disagreements between China, Japan and South Korea, and the fact that hacking has been utilized as a national security tool between the countries, the three share a concern that internet attacks could lead to more significant crises. This example shows how a history of practical collaboration helped develop the trust and dialogue that led to a normative agreement despite broader security and diplomacy disagreements. Their CSIRTs' work together helped highlight the risks they all shared if cyberattacks were to continue unabated. Interestingly Ito believes that the CBMs depended not only on the exercises the CSIRTs conducted, but also on the regular in-person interactions that helped build bridges among APCERT members.[17]

APCERT is a leading example of depoliticized technical cooperation leading to normative opportunities, but it need not be the only one. While more nascent than its Asia Pacific

[13] Asia Pacific Computer Emergency Response Team, "Member Teams," APCERT Structure, accessed April 20, 2018, https://www.apcert.org/about/structure/members.html.

[14] Yurie Ito, "Making the Internet Clean, Safe and Reliable: Asia Pacific Regional Collaboration Activities," *Cybersecurity Summit (WCS), 2011 Second Worldwide*, IEEE, 2011. Available at https://ieeexplore.ieee.org/document/5978796/.

[15] See Asia Pacific Computer Emergency Response Team, "Mission Statement," About APCERT, accessed April 20, 2018, https://www.apcert.org/about/mission/index.html.

[16] Ito, ibid.

[17] Interview with Yurie Ito.

counterpart, AfricaCERT presents a similar appreciation by the African network operators to share best practices, develop principles and support capacity in African countries to maintain stability and security of the Internet. There may well be an opportunity to work with AfricaCERT to support its deepening of confidence building measures.

The confidence building approach has likewise been endorsed by broader groups. For example, the Organization for Security and Co-operation in Europe (OSCE). The OSCE not only established an informal working group (IWG) on Confidence Building Measures to Reduce the Risk of Conflict Stemming from the Use of ICTs, but has also adopted sixteen CBMs.[18] It is too soon to know how successful the OSCE IWG will be. Implementation, after all, will be voluntary, and thus hard to predict. Moreover, observers agree that some of the goals, such as states' agreement to refrain from certain destabilizing activities, will be difficult.[19]

But the fact that cooperative and transparency measures are broadly understood to serve as important pillars for increasing cyber stability. At the November 2017 OSCE Chairmanship Conference on Cybersecurity, the chair endorsed capacity building and CBMs in his opening remarks, "Faced with these challenges, we need to come together to do three things: work towards a common understanding of the rules for responsible state behaviour in cyberspace; promote confidence and trust between states; and strengthen our efforts to increase cyber resilience by promoting capacity building."[20] Even the Russian representative gave a nod in this direction, saying "While the UN is the leading organization for discussing the promotion of cyber stability between states, the OSCE's unique role in settling incidents related to the use of ICTs needs to be strengthened."[21]

The OSCE work is mirrored by similar activities[22] in the ASEAN Regional Forum (ARF) and the Organization of American States (OAS).[23] There is a clear recognition of the importance of both capacity and confidence building for cybersecurity normative development in these different regional organizations.

[18] OSCE Permanent Council, "Initial set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies," Decision No. 1106, last modified December 3, 2013, https://www.osce.org/pc/109168?download=true.

[19] Patryk Pawlak, "Chapter 7: Confidence-Building Measures in Cyberspace: Current Debates and Trends." International Cyber Norms: Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn, 2016, https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_Ch7.pdf.

[20] Michael Linhart, Austrian Deputy Foreign Minister, speaking on behalf of his country's chairmanship role. "Common Understanding of Rules for Responsible State Behaviour in Cyber Space Needed,Say Participants of OSCE Chairmanship Conference on Cybersecurity," Press Release, Organization for Security and Cooperation in Europe, last modified November 3, 2017, https://www.osce.org/chairmanship/354676.

[21] OSCE Secretariat, "Common Understanding of Rules for Responsible State Behaviour in Cyber Space Needed, say Participants of OSCE Chairmanship Conference on Cybersecurity," Press Release, Organization for Security and Co-Operation, last modified November 3, 2017, https://www.osce.org/chairmanship/354676.

[22] These efforts have been catalogued by previous papers so this memo will not go into detail into the various proposals. The point for raising them here is to note that the regional efforts are complementary to each other.

[23] ASEAN Regional Forum, "Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security," last modified July 13, 2012, https://ccdcoe.org/sites/default/files/documents/ASEAN-120712-ARFStatementCS.pdf..

What is important to deepening the impact of any of these is to operationalize communication channels, establish technical collaboration such as among incident response systems, and make interactions as regular and frequent as possible.

Building and Highlighting Capacity

Countries can be reluctant to support new norms if they do not see the potential benefit for them of bearing the cost of implementation or in some cases see political risk in endorsing and implementing new norms. The gap in capacity is particularly wide in the field of cutting edge technologies, making low capacity an obstacle to cybersecurity norm building.[24] States may not adequately appreciate the risk to their economy or national security from a cyber event, they may perceive risk abatement as overly costly, or consider the absence of cyber rules an asymmetric advantage. Tikk and Kerttunen suggested as much in calling for a "*Cyber Marshall Plan,* building robust national capacities and unprecedented transfers of ICTs … [to create] a climate of wealth, health and security."[25]

In an analogous sector, climate change, as countries became more economically diverse, the potential benefit from leveraging new energy technologies began to rival the liability of curbing reliance on polluting fuel sources. Some of this rebalancing was thanks to capacity building by the UN and other bodies.[26] The commitment to remain in the Paris Agreement was reinforced by a variety of local and philanthropic coalitions dedicated to supporting the agreement. And the data sharing exposed links between better energy policies and economic benefits, helping to motivate stakeholders to adhere to the normative contract. Just to name one example among several, the C40 Cities initiative has invested both in capacity building and in building maps and other presentations linking measures of clean air benefits to energy sources, visibly demonstrating to mayors the importance of adhering to climate norms.[27]

Similarly in the cybersecurity sector, the United Nations Office on Drugs and Crime (UNODC) developed a cybercrime training for El Salvador.[28] According to UNODC, such work not only has the benefit of raising local capacity for implementing cyber commitments, but also develops local institutional ability to collaborate across borders, and an appreciation of, and thus demand for,

[24] Resolution A/72/251 177 on the Impact of exponential technological change on sustainable development and peace passed on December 22, 2017 is clearly based on the recognition that technology capacity is uneven, yet important for sustainable development.
[25] Eneken Tikk and Mika Kerttunen, "Cyber Treaty is Coming," Publications, Cyber Policy Institute, accessed April 20, 2018, http://cpi.ee/wp-content/uploads/2018/02/Cyber-Treaty-is-Coming-Tikk-Kerttunen.pdf.
[26] UN Sustainable Goal 13 is "Take urgent action to combat climate change and its impacts."
[27] "C40 Research, Measurement and Planning," C40 Cities, accessed May 5, 2018, http://www.c40.org/research.
[28] "UNODC Continues Strengthening El Salvador Capabilities for Fighting Cybercrime," Central America and the Caribbean, United Nations Office on Drugs and Crime, accessed October 20, 2017, https://www.unodc.org/ropan/en/unodc-continues-strengthening-el-salvador-capabilities-for-fighting-cybercrime.html.

cyber norms. Interestingly UNODC's project reinforces the Salvador Declaration,[29] helping to build adherents to a soft normative document.

Outside the UN, a nonprofit initiative, CyberGreen, maps the risks to the cyber ecosystem for national CSIRTs.[30] As economies become more robust and Internet dependent, data that demonstrates economic consequences from cyber risks can be meaningful for creating local impetus for cyber agreement. Inside the UN, also the UNODC has reviewed the state of cybercrime and has been charged with further work on the topic through an intergovernmental open-ended expert group.[31] This work could well prove to be useful to deepening and shaping countries' appreciation of the need for cyber norms.

What is particularly attractive about interactive, current data maps such as CyberGreen's and presentations of impact measures such as C40 Cities' is their focus on actionable data in formats that highlight the connections in ways more likely to gain policy officials' attention. Moreover the public facing nature of their websites also provides a tool for civil society constituencies to press for greater action from their governments.

Investment in more capacity building and user-friendly data sharing - particularly when reinforcing agreements or declarations of consensus - can help drive support for cyber norms among a greater number of countries, helping break through inaction on formal measures.

Conferences Most Useful When Tied to CBM and Capacity Building

Among those interviewed for this memo, many note the importance of creating opportunities to bring together important stakeholders, share best practices and spark ideas and develop like-minded collaborations. While there are a number of cybersecurity relevant fora that play this role,[32] the most tangible impact is associated with those that advance specific, practical measures that build consensus.

To analyze this distinction, it is worth examining the five Global Conferences on CyberSpace (GCCS) to date that have comprised the "London Process."[33] As a conference, the London Process

[29] United Nations,"Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World," Twelfth United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.213/L.6/Rev.2, (April 2010), https://undocs.org/A/CONF.213/L.6/REV.2.

[30] "About," CyberGreen Institute, accessed April 21st, https://www.cybergreen.net/.

[31] UNODC has published a 2013 Comprehensive Study on Cybercrime. United Nations Office on Drugs and Crime, "Comprehensive Study on Cybercrime," United Nations, February 2013, V.13-80699, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. See more information about the open-ended group at "Open-Ended Intergovernmental Expert Group to Conduct A Comprehensive Study of The Problem of Cybercrime," United Nations Office on Drugs and Crime, accessed May 5, 2018, http://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-to-conduct-a-comprehensive-study-of-the-problem-of-cybercrime2018.html.

[32] There are a few examples of different types of cybersecurity fora. While the paper reviews compares some public examples, there are also fora like the MIT conference that are smaller and less public, but which provide useful opportunities for sharing of ideas, which can be further shared at other opportunities. Moreover the Secretary General appears to be appointing a high level group, but it is too early to know how the group will do its work.

[33] "A Policy Maker's Guide To The Global Conference on Cyberspace 2017," Access Now, accessed April 29, 2018, https://www.accessnow.org/cms/assets/uploads/2017/11/A-Policy-Makers-Guide-to-GCCS-2017-digital-v.pdf.

already had the attribute of government sponsorship, but multi stakeholder participation. Yet it was not able to deliver on its ambitious goal of helping the global community develop “voluntary and non-binding ‘rules of the road’ for cyberspace.”[34] Instead, the London Process found its footing at the 2015 Hague meeting, launching the Global Forum on Cyber Expertise (GFCE).[35] With the idea that better cyber capacity produces more interest in good cyber hygiene, the Forum is meant to identify capacity needs and help match them to responsive projects. At its May 2017 meeting, GFCE participants described a variety of initiatives from building out the capacity of countries to implement the Budapest Convention to harmonizing an understanding of cyber threats.[36] The GFCE made a further contribution by working on impact assessment, which can help identify and prioritize best practices and provide the data necessary to support investment in cyber capacity.[37]

As described in the section on CBMs, the tangible deliverable that the GFCE represents makes the London Process more meaningful to a broader group of stakeholders. As a platform that supports capacity building, the GFCE can increase the number and diversity of stakeholders interested and able to participate in good cyber practices and help forge relationships among them, setting the stage for broader normative support.[38]

This is not to say that fora whose goal is mainly to share ideas are useless. Many praise the UN’s Internet Governance Forum (IGF), for example, for providing both global and regional opportunities to air ideas and even differences, and to spark common understandings. These activities lend themselves to relationship building and sharing of good practices that are ultimately necessary to normative development. But if one were to highlight the opportunity to make the most far-reaching impact, it is when the meetings conclude with specific measures that can deepen and broaden consensus.

In contrast it is important to note the type of conference that does not contribute to consensus building because its neutrality is undermined. The Conference of the International Information Security Research Consortium held in Garmisch, Germany has lost traction since its launch in 2007 by the Russian Institute of Information Security Issues at Moscow State University. With its early meetings scheduled during the attempted reset between the U.S. and Russia, attendance was more robust and potential for greater understanding may have been possible.[39] The forum

[34] Ibid., p. 5.

[35] “Launch Global Forum on Cyber Expertise in The Hague,” Netherlands National Government, last modified April 4, 2015, https://www.government.nl/latest/news/2015/04/16/launch-global-forum-on-cyber-expertise-in-the-hague.

[36] See GFCE Secretariat, GFCE Annual Meeting 2017, Global Forum on Cyber Expertise, 2017, file:///C:/Users/sanchezk/Downloads/Report+GFCE+Annual+Meeting+2017.pdf.

[37] Vladimir Radunovic of the DiploFoundation presented on the GFCE effort “to produce [a] set of global good practices, [based] on rigor and empiricism in the identification of what works and what doesn’t.” See Robert Morgus, “Show me The Numbers: Reflections from The Global Forum on Cyber Expertise’s Annual Meeting,” New America, last modified June 13, 2017, https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/show-me-da-numbers-reflections-global-forum-cyber-expertises-annual-meeting/.

[38] Council on Foreign Relations, “The Global Forum on Cyber Expertise: Its Policy, Normative, and Political Importance,” Net Politics & Digital and Cyberspace Policy Program, last modified April 28, 2015, https://www.cfr.org/blog/global-forum-cyber-expertise-its-policy-normative-and-political-importance.

[39] Andrew E. Kramer and John Markoff, “In Shift, U.S. Talks to Russia on Internet Security,” *The New York Times*, last modified December 12, 2009, https://www.nytimes.com/2009/12/13/science/13cyber.html; David Talbot, “Russia’s

provided one of the few less formal opportunities for Russian government officials to interact with their counterparts and non-governmental stakeholders. But given the association of the Garmisch forum with Russia's effort to establish its position in cyberspace, attendance has diminished as Russia has become associated with aggressive methods on and off the Internet.

UN can best advance norms through capacity building

While the UN is most often discussed as a body where formal agreements are shaped, even the UN cannot productively play this role at a time of strained diplomatic relations and divergent national policy perspectives. Normative work may continue at the UN General Assembly. However the ability to pass non-binding resolutions at UNGA despite objections by Member States with the deepest cybersecurity capability does not change the key countries' positions on what they would accept in binding agreements.

Thus this memo considers the UN's key contribution at this time to be confidence and capacity building. The UN's global platform allows it to move best practices around different geographies. A successful cyber capacity program from one area can support capacity building in another country, with the added value of building networks across boundaries among stakeholders who endorse good cyber hygiene. The UN is singularly the global institution that can span across geographies and levels of development. It is quite useful for the UN to remain engaged and focus on pre-normative opportunities like capacity building.

B. INCREMENTAL AGREEMENTS

Whereas the practical measures described in the last section have a history of developing trust and interest in supporting norms, actual agreements that produce tangible commitments would be a significant step to narrowing ungoverned spaces. While the political alignment necessary for a comprehensive cybersecurity agreement is lacking, the way forward may well be through narrowly focused agreements because those can be reached in a more reasonable amount of time and with greater potential for compliance. Professor Nye has endorsed the "like-minded states" approach to norm development, which could be expanded at a later stage to include more actors.[40] The current U.S. administration also endorsed this approach, particularly since the 2017 UN GGE.[41]

Cyber Security Plans," *MIT Technology Review*, last modified April 16, 2010, https://www.technologyreview.com/s/418495/russias-cyber-security-plans/; John Markoff, "Step Taken to End Impasse Over Cybersecurity Talks," *The New York Times*, last modified July 16, 2010, https://www.nytimes.com/2010/07/17/world/17cyber.html.

[40] Joseph S. Nye, "The Regime Complex for Managing Global Cyber Activities," Global Commission on Internet Governance Paper Series, No. 1, May 2014, https://dash.harvard.edu/bitstream/handle/1/12308565/NyeGlobalCommission.pdf?sequence=1.

[41] Shaun Waterman, "White House Cyber Czar Says Push for Norms will Move to Small Group of Allies," Government, CyberScoop, last modified July 11, 2017, https://www.cyberscoop.com/rob-joyce-white-house-cyber-norms/. Moreover the utility of this approach is underlined by the flipside of "non like-minded" states, the U.S. and China, having a hard time enforcing compliance with their 2015 bilateral position on cyber espionage.

This approach has had a number of supporters. In addition to Professor Nye's work, the Council on Foreign Relations' (CFR) International Institutions and Global Governance has recommended that a like-minded group of ten democracies or "D10" work on issues from security to human rights.[42] Likewise, a European Union Institute for Security Studies paper laid out a few of the merits of this approach, with the upside being the ability to reach agreement and to monitor compliance.[43]

Yet forming agreements with only like-minded coalitions runs the risk of divisiveness and parochialism. "The forming of a 'coalition of the willing' (that draws a line between different approaches) may force others to unnecessarily pick sides – ultimately defeating the purpose of the normative endeavour."[44] Even the authors promoting the D10 notion recognized the potential lack of legitimacy of "exclusive" clubs and of a dynamic of "us versus them," which could create new problems.[45] Some of this could be alleviated by supporting a series of parallel like-minded agreements so that no one of them is elevated to being an exclusive "insiders' club."[46] But as the ability to support and network among them is likely to be constrained for any institution, a like-minded approach might do better by focusing on "what" it is governing, rather than "who" is among the signatories.

Tangible, sector-specific issues

A useful way to think about making progress when caught between conflicting ideological approaches to cybersecurity is to focus on specific, tangible issues important to strengthening cyber hygiene. "Thematic coalitions"[47] are harder to criticize for being exclusive clubs. Rather they build signatories or members around common interests, and new members are welcome if they are relevant to the theme.[48]

[42] Ash Jain, "Like-Minded and Capable Democracies: A New Framework for Advancing a Liberal World Order," Council on Foreign Relations Working Paper, last modified January 3 2013, file:///C:/Users/sanchezk/Downloads/IIGG_WorkingPaper12_Jain.pdf.

[43] Jakob Bund and Patryk Pawlak, "Minilateralism and Norms in Cyberspace," Issue Alert, European Union Institute for Security Studies (EUISS), September 2017, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert%2025%20Cyber%20norms_0.pdf.

[44] Ibid., 2.

[45] Ash Jain, *Like-Minded and Capable Democracies: A New Framework for Advancing a Liberal World Order*, 16.

[46] For example, China's International Strategy of Cooperation in Cyberspace, while preferring a UN-led approach, makes room for additional sub-group models. Tian Shaohui,"Full Text: International Strategy of Cooperation on Cyberspace," Xinhuanet, accessed April 23, 2018, http://www.xinhuanet.com/english/china/2017-03/01/c_136094371_4.htm.

[47] A term used in Eneken Tik's & Mika Kerttunen's "Cyber Treaty is Coming: Что делать?" Cyber Policy Institute, 2018, http://cpi.ee/wp-content/uploads/2018/02/Cyber-Treaty-is-Coming-Tikk-Kerttunen.pdf.

[48] A thematic approach that would set this version of "like-minded" apart from other groups that call themselves "like-minded" such as the Like Minded Developing Countries group at the UN that includes members such as Syria, and the Like Minded Group (LMG) of 52 countries at the UN coordinates activities at the UN Human Rights Council. See blog post of Amr Essam,"The Like Minded Group (LMG): Speaking Truth to Power," Universal Right Group, last modified May 10, 2016, https://www.universal-rights.org/tag/lmg.

The trade arena provides an apt analogy as regional free trade agreements (FTAs) grew in volume once global discussions stalled.[49] A number of states appeared unwilling to adequately compromise in the major world trade rounds, probably because they did not see enough benefit to their smaller economies of making such sacrifices.[50] Yet regional and other narrowly focused arrangements proliferated. There has been some debate as to whether the growth in regional trade agreements was a substantial factor in moving toward global negotiations, but what appears to be the case is that (a) regional agreements grew to supra-regional as expanding numbers of countries joined, and (b) that along with the growth of the FTAs was a deepening appreciation in less developed economies of the link between compromises and eventual economic benefits.[51]

These aspects of regional agreements are important lessons for cybersecurity. Like FTAs, correctly structured narrow-focus cybersecurity agreements should be able to attract additional signatories. The agreements must be crafted such that eventually broader numbers of signatories can accept the compromises reached. They must also be crafted to model good rules of behavior. Finally if the initial signatories are able to evidence economic or security benefits tied to their implementation of the agreements, there is likely to be demand on the part of more signatories to join.

In the cybersecurity realm, the case was made for focusing cybersecurity commitments on the stability of financial data flows. There are a couple of factors that make this an interesting case to consider. First the global nature of financial institutions makes many different countries vulnerable to an attack on any one large bank.[52] Second financial data integrity has long been protected by many national governments, providing a working precedent for reaching a cyber agreement.[53] Third there are working mechanisms: the G20 has the standing to promulgate such a commitment, and the Financial Stability Board[54] could be the vehicle to implement it in detail,

[49] In a presentation by Japanese trade bodies, the option of focusing on a specific subset of issues was lauded as a benefit of the FTA. Michitaka Nakatomi, "Plurilateral Agreements: A Viable Alternative to The World Trade Organization?," Asia Development Bank Institute, No. 439, October 2013, https://www.adb.org/sites/default/files/publication/156294/adbi-wp439.pdf.

[50] See discussion in Jeffrey J. Schott, "Free Trade Agreements: Boon or Bane of the World Trading System?" In *Free Trade Agreements: US Strategies and Priorities*, edited by Jeffrey J. Schott, pp. 3-33, Peterson Institute for International Economics, 2004.

[51] Ibid. See also Shujiro Urata, "Globalization and the Growth in Free Trade Agreements," Asia Pacific Review, Vol. 9, No. 1, (May 2002), http://www.wright.edu/~tdung/Globalization_and_FTA.pdf.

[52] Interview with Tim Maurer, Co-Director and Fellow of Carnegie Endowment's Cyber Policy Initiative. Moreover, defined as a critical infrastructure by President Obama, the financial sector already rises to the level of significant interest for U.S. policy makers.

[53] See G20 Research Group, "Communique: G20 Finance Ministers and Central Bank Governors Meeting," Federal Ministry of France (March, 2017), http://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Schlaglichter/G20-2016/g20-communique.pdf?__blob=publicationFile&v=7.

[54] Interestingly for the argument in the last section of this memo that compilations of agreements and principles support consensus building, the FSB creates such a compendium in the financial sector. "The Compendium of Standards," Financial Stability Board, accessed April 25, 2018, http://www.fsb.org/what-we-do/about-the-compendium-of-standards/.

together with the relevant standard-setting bodies, the private sector, law enforcement, and Computer Emergency Response Team (CERT) communities.[55]

This idea leverages the FSB's existing responsibilities designed in response to the global financial crisis. The institution has in fact been able to drive consensus in financial regulations, with member states implementing the standards, as well as cooperation from non-member states. The FSB has already taken stock of the cybersecurity attacks on the financial system and the measures taken by members to protect financial institutions.[56] It appears poised to potentially go further in developing a set of standards for financial sector cybersecurity. Given the vulnerability of a great variety of countries, including both Russia and the U.S., from financial cybercrimes, the financial sector may well provide the "like-minded" arena for development of a discrete agreement.[57]

Whether or not one settles on the financial sector, it is particularly useful to focus on a sector outside of the security context. If the goal is to expedite the ability to reach an agreement a number of stakeholders can sign and implement, it is useful to leverage existing technical collaborations and relationships (bank regulators, for example) that do not appear to impinge on the most sensitive sovereignty questions for nations. In fact if the sector has global spillover - as when more countries began to appreciate how global trade patterns impacted their economies - there is likely to be more appreciation of how the international pact can advance national interests.

Dual Illegality

Another way to think about narrowly focused agreements is to focus on activities that are historically and fundamentally illegal in the systems of different countries - even of adversaries. In such case a "like-minded" agreement can emerge as an articulation of shared implicit norms. States, for example, have agreed on the need to protect children online, developing a type of cybersecurity safe zone.[58] The U.S. Federal Bureau of Investigations (FBI) and the Chinese Ministry of Public Security have begun to cooperate in investigations of online child pornography. Along with over forty other nations, China joined the FBI's Innocent Images International Task Force,

[55] Tim Maurer, Ariel Levite, and George Perkovich, "Toward a Global Norm Against Manipulating the Integrity of Financial Data," Carnegie Endowment for International Peace, last modified March 27, 2017, http://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403.

[56] "FSB Publishes Stocktake on Cybersecurity Regulatory and Supervisory Practices," Press Release, Financial Stability Board, last modified October 13, 2017, http://www.fsb.org/wp-content/uploads/BdF-Financial-Stability-Review.pdf.

[57] Tim Maurer, Ariel Levite, and George Perkovich, *Toward a Global Norm Against Manipulating the Integrity of Financial Data*.

[58] The United Nations has adopted an optional protocol to the U.N. Convention on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography 2000 (Sex Trafficking Protocol), Volume 2171, A-27531, http://www.ohchr.org/Documents/ProfessionalInterest/crc-sale.pdf. The Preamble expresses concern over "the growing availability of child pornography on the Internet and other evolving technologies." See Cris R. Revaz, *The Optional Protocols to the UN Convention on the Rights of the Child on Sex Trafficking and Child Soldiers*, 9 Human Rights Brief 13 (Fall 2001). Also reference the International Conference on Combating Child Pornography on the Internet (Vienna, 1999).

which provides training, including on legal principles.[59] It should be noted, however, that differing implementation can undermine the agreement in practice. In 2017, the FBI reportedly broke into a number of overseas computers in pursuit of a major child porn law enforcement operation.[60] It is not clear whether what appears on its face to be unauthorized access may have caused a deterioration in the good working relationships among the U.S. and countries like Russia and China even where they agreed in principle. This example points to the prudence of anticipating implementation parameters in order to support the agreement in practice.

Leveraging Existing Security Regimes

Cybersecurity policy makers have also begun to try to use existing security arrangements to develop more oversight of offensive cybersecurity tools. Norms and laws will only constrain the behavior of actors who agree to be constrained by norms and laws. Rogue actors—whether rogue nation states, proxy actors on behalf of nation states, or non-state actors—will not necessarily adhere to an international normative or legal regime.[61] For these actors, norm and law enforcement is crucial. However, the relative ability of actors to obfuscate their actions and cast doubt over their own culpability means that more must be done to interdict these actors' process of procuring, developing, or otherwise obtaining offensive cyber capability. With these considerations in mind, the arms control approach seemed to have merit. Yet it has been hard to adapt to cybersecurity.

Over the last few years, the international community has worked to negotiate Wassenaar agreement coverage of intrusion software.[62] It is understandable why the Wassenaar arrangement presented an interesting opportunity: after all it is an arms control regime that has a number of very different adherents including both the U.S. and Russia, and has worked well to add transparency to arms transfers. But when intrusion software was added to Wassenaar control lists in 2013,[63] both academics and companies decried the overly inclusive definitions that had the unintended impact of stymieing cyber defensive capabilities.[64] Exemptions were soon negotiated in December 2017, but regulatory implementation is still to come with potential

[59] "FBI, China Team Up vs Child Porn," SciTech, *GMA News Online* October 12, 2011, last modified http://www.gmanetwork.com/news/scitech/content/235085/fbi-china-team-up-vs-child-porn/story/.

[60] Joseph Cox, "The FBI Blindly Hacked Computers in Russia, China, and Iran," *The Daily Beast*. November 8, 2017.

[61] Robert Morgus, Max Smeets, Trey Herr, "Countering the Proliferation of Offensive Cyber Capabilities," 163.

[62] The Wassenaar Arrangement was established to contribute to regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies. See "Dual-Use Trade Controls," European Commission, accessed April 26, 2018, http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/index_en.htm.

[63] "Summary of Changes: List of Dual-Use Goods & Technologies and Munitions List," The Wassenaar Arrangement, last modified December 4, 2013, https://www.wassenaar.org/app/uploads/2015/06/Summary-of-Changes-to-Control-Lists-2013.pdf.

[64] Shaun Waterman, "The Wassenaar Arrangement's Latest Language is Making Security Researchers Very Happy," Government, CyberScoop, last modified December 20, 2017, https://www.cyberscoop.com/wassenaar-arrangement-cybersecurity-katie-moussouris/.

confusion among implementing regimes.[65] Thus as of the date of this memo, the early lessons of Wassenaar is that analogous regimes may simply be too cumbersome for cybersecurity controls where matters of intent and attribution can be the difference between "black" and "white hat" activities.[66]

A more fluid approach that some cyber stakeholders have shown interest in is the arrangement for monitoring and interdicting weapons of mass destruction modeled after the Proliferation Security Initiative (PSI).[67] While transposing existing, environment-specific models onto novel security environments should be approached with caution, there are several lessons that can be drawn specifically from the PSI that may be relevant to addressing the proliferation problem.

PSI's non-legally-binding approach, focusing on cooperative activities, is akin to a technical cooperation mechanism like APCERT. Rather than a legal agreement with responsibilities and sanctions attached, the PSI is a set of principles designed to build stronger WMD interdiction cooperation. Scholars have suggested that PSI offers a "plurilateral" approach to cooperation.[68] This background suggests that while arms control agreements may be difficult to adapt to a field like cybersecurity where the same tools are often both benign and weaponized, a cooperative rather than binding arrangement may present near-term opportunities less fraught with risks for the stakeholders who raised alarms over use of the Wassenaar arrangement.

C. CIVIL SOCIETY LED AND MULTI-STAKEHOLDER INVOLVEMENT

While ultimately only governments can agree to international agreements that sanction bad behavior, civil society has, in a number of instances, led consensus building and pressured governments to develop an international agreement. Civil society and private sector can often act more nimbly than governments, helping to set the agenda that forces governments to address the issue. The challenge is that the "driver" of the agenda must not appear to have a financial stake in the outcome, or it will not have the legitimacy needed to shape the agenda.

Private Sector Resources

In the cybersecurity context, this approach can be particularly useful because the research and development, expertise and deployment of cybersecurity tools principally reside in the private sector. Companies provide important practical insights in understanding how particular norms

[65] Garrett Hinck, "Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research," Cybersecurity, Lawfare, last modified January 5, 2018, https://lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research.

[66] As Morgus, Smeets and Herr noted, applying analogies like Wassenaar or the Weapons of Mass Destruction (WMD) regime is problematic and presents new problems when trying to adapt it to the cyber environment. See Robert Morgus, Max Smeets, and Trey Herr to Global Commission on the Stability of Cyberspace, "Countering the Proliferation of Offensive Cyber Capabilities," *GCSC Issue Brief No. 1*, Memorandum No. 2 (November 2017), 161.

[67] "Proliferation Security Initiative, " Bureau of International Security and Nonproliferation (ISN), U.S. Department of State, accessed April 27, 2018, https://www.state.gov/t/isn/c10390.htm.

[68] Duncan B. Hollis and Matthew C. Waxman, "Promoting International Cybersecurity Cooperation: Lessons from the Proliferation Security Initiative (PSI)," Temple International & Comparative Law Journal, No. 2018-03, (Forthcoming, 2018).

might be developed, and what risks they might carry. Without them at the table, normative discussions would lack important information and levers for normative adherence. For a good example of this, please review the Wassenaar discussion above where the lack of such involvement forced a backtracking on language adapting the Wassenaar arrangement to cyber technology, as well as the 2012 World Conference on International Telecommunications (WCIT) where text suspected of undermining the multi-stakeholder approach to Internet governance was not adopted reportedly because of business community concerns.[69]

Clearly important private sector stakeholders are interested and have stepped forward forcefully to engage in cyber normative discussions. Microsoft's proposal of a Digital Geneva Convention is an example of one of the most significant global ICT companies raising the call for normative development.[70] In a different type of example, Siemens and eight other global companies signed a Joint Charter on Cybersecurity, which includes ten areas in which governments and companies should take action to support greater cybersecurity.[71] Both the Siemens and Microsoft efforts include ideas for both government and corporate responsibility, and that in itself, is important as a marker that multiple sectors must be involved for norms to align and to be implemented. Whether or not a new convention is needed - or ultimately adopted - the fact that global technology companies are ready to commit resources to supporting a global consensus should add impetus to normative development.

Civil Society as a Driver

In past contexts normative breakthroughs were driven by civil society seized with the threat posed by certain weapons. Thus, treaties on Landmines and Cluster Munitions, respectively, were first driven by civil society. In 1992, coalitions of national and international non-profits and dedicated individuals across human rights, refugees, development and humanitarian fields, began a concerted effort to address the scourge of landmines. Their dedicated and consistent data development and advocacy resulted in a 1995 treaty that is still observed today.[72] A similar network of groups and activists began in 2003 to agitate to end the use of cluster munitions, delivering a treaty in 2008.[73] More recently civil society groups —from the Campaign to Stop Killer

[69] Wolfgang Kleinwächter,"WCIT and Internet Governance: Harmless Resolution or Trojan Horse?" CircleID, last published December 27, 2012, http://www.circleid.com/posts/20121217_wcit_and_internet_governance_harmless_resolution_or_trojan_horse/.

[70] See Brad Smith's Keynote Address, *Protecting and Defending Against Cyberthreats in Uncertain Times*, at the RSA Conference 2017.

[71] "Charter of Trust," Cybersecurity, Siemens, accessed April 23, 2018, https://www.siemens.com/global/en/home/company/topic-areas/digitalization/cybersecurity.html.

[72] "The ICBL," Who We Are, International Campaign to Ban Landmines, accessed April 24, 2018, http://www.icbl.org/en-gb/about-us/who-we-are/the-icbl.aspx; "NGOs and the International Campaign to Ban Landmines," Global Policy Forum, accessed April 26, 2018, https://www.globalpolicy.org/ngos-and-the-international-campaign-to-ban-landmines.html.

[73] "Nations Sign Cluster Bomb Treaty," *BBC News*, last modified December 3, 2008, http://news.bbc.co.uk/2/hi/europe/7762031.stm; Thomas Nash, "Civil Society and Cluster Munitions: Building Blocks of A Global Campaign, Palgrave Macmillan, Global Civil Society (2012), https://link.springer.com/chapter/10.1057/9780230369436_8.

Robots, to the Partnership on AI, and many others —have arisen to call for ethical norms that would govern cutting edge technologies.[74]

Some analysts have theorized that cyber security agreement will be reached only when a truly catastrophic event occurs that drives home the stakes in not having an agreement. To build a cyber campaign akin to "killer robots," civil society would likely need to focus on a specific catastrophic cyber risk such as incapacitating life-saving critical infrastructure, or triggering a physical threat to human safety such as a nuclear power plant melt down. These are catastrophic consequences that concentrate the ire and resources of a civil society community.

In the absence of such an event, the importance of civil society is in sharing knowledge and building constituencies that support and advise normative development, and help ensure adherence and implementation. For example in the climate arena, cities and civil society have taken leadership in order to continue to make progress when international agreement stalled, and to deepen it when it happens. Thus the 40 Cities Initiative,[75] America's Pledge,[76] and others have been able to seed good climate initiatives and continue pledges in support of the Paris Climate Agreement thanks to civil society and sub-national governments rallying to respond to the U.S. pulling out of the agreement.[77]

Similarly civil society can help broaden and deepen constituencies for cyber norms, and can best support these efforts if included in discussions, capacity building and even collaborative activities among key stakeholders. Thus, for example, efforts to develop greater understanding of a cyber risk would do well to include not only government experts, but also substantial participation by civil society, which can help develop the research, contribute diverse points of view, and communicate results to build public support.

D. MEMORIALIZING NORMATIVE DEVELOPMENT

The work described above is occurring in many fora, with disconnected actors often retreading some of the work already completed in other contexts. Similar best practices are disconnected, and lessons learned not shared, limiting their impact. Cataloging and publishing agreements, principles and best practices helps to raise awareness, educate stakeholders and acknowledge and reinforce the normative progress that has occurred.[78] Databases highlight similarities among

[74] The Campaign to Stop Killer Robots was launched in 2013 by an international coalition of five international NGOs, a regional NGO network, and four national NGOs that work internationally; their work is focused on preemptively banning fully autonomous weapons. The Partnership on Artificial Intelligence to Benefit People and Society, or the Partnership on AI for short, was created in 2016 by founding partners Amazon, Apple, DeepMind, Google, Facebook, IBM, and Microsoft to establish best practices and guidelines for artificial intelligence systems.

[75] "History of the C40," History, C40 Cities, accessed April 22, 2018, http://www.c40.org/history.

[76] "America's Pledge," Bloomberg Philanthropies, access May 5, 2018, https://www.bloomberg.org/program/environment/americas-pledge/#overview.

[77] Regan, Michael D., "U.S. Cities States Pledge Support for Climate Accord." *PBS News Hour, (online)* November 11, 2017.

[78] Technical norm setting organizations such as NIST in the U.S. or IEEE globally use the method of building databases of information as a tool for nudging along agreement. An argument can be made that breaches in behavior or the falling apart of consensus at later dates raises the question of whether an implicit norm actually exists. But given that breaches occur even with formal agreement, there is nevertheless a benefit to reinforcing that consensus has been

positions of different subgroups, reinforcing the breadth of agreement on certain fundamental principles and making it less likely that past agreements will be reopened. They also help minimize the waste of duplicative work by presenting the agreements reached to date.

But who compiles, supports and makes decisions on what is appropriate to include? On the one hand, the UN's global role may make it particularly well-suited to housing such a compilation. Such a database can include the output of previous consensus, such as the pre-2017 GGEs,[79] as well as work accomplished in the First Committee, and the Second and Third Committees.[80] UNIDIR[81] and ITU[82] reports on the state of cybersecurity, as efforts such as the open-ended intergovernmental expert group can also be included for a comprehensive look at UN based cyber developments.

On the other, the UN may be constrained from including credible and substantial criticisms of contributions by Member States. For this reason there is a benefit to complementary catalogs, with the UN serving as a global database of major agreements, best practices, UN resolutions and consensus documents such as the GGEs, while a non-governmental body compiles an annex that can include significant disagreements in positions in order to accurately portray the state of cybersecurity discussions.[83]

Civil society has already begun to develop such work. The Carnegie Endowment has a Cyber Norms Index,[84] for example, provides an interactive tool to compare existing expressions of standards of appropriate behavior in cyberspace across the globe. This search tool enables the user to compare specific language in multilateral outcome documents either by category or keyword. The Index contains both established law as well and aspirational measures in development. it even includes confidence- and transparency-building efforts as well as ongoing

reached and not undone. For counter arguments, see Elaine Korzak, "UN GGE on Cybersecurity: The End of an Era?" The Diplomat, last modified July 31, 2017, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

[79] Endorsement by the G20 in 2015 seems to have established the prior GGEs' work enough to warrant cataloging those accomplishments. Joseph S. Nye, "How Will New Cybersecurity Norms Develop?" Project Syndicate, last modified March 8, 2018, https://www.project-syndicate.org/commentary/origin-of-new-cybersecurity-norms-by-joseph-s--nye-2018-03; Arun M. Sukumar, "The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?" Cybersecurity, Lawfare, last modified July 4, 2017, https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

[80] While the First Committee is noted as having jurisdiction in this area, the others focusing on development and human rights likewise add valuable perspectives to round out the database.

[81] Dr. Camino Kavanagh, "The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century," United Nations Institute for Disarmament Research, accessed April 24, 2018, http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf.

[82] "Global Cybersecurity Index (GCI) 2017" International Telecommunication Union, accessed April 20, 2018, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

[83] For example, Citizen Lab's criticism of the Shanghai Cooperation Organization's Code of Conduct may be impossible for the UN to include, but is an important part of memorializing the state of cybersecurity discussions. "An Analysis of the International Code of Conduct for Information Security," Free Expression Online, The Citizen Lab, last modified September 28, 2015, https://citizenlab.ca/2015/09/international-code-of-conduct/.

[84] "Cyber Norms Index," Publications, Carnegie Endowment for International Peace, accessed April 23, 2018, http://carnegieendowment.org/publications/interactive/cybernorms.

processes or outline future processes. There is merit to this broad grouping, but also a risk in encompassing too many underdeveloped "norms" that cannot provide a firm basis of agreement.

Regardless of the model, the point is that cataloging settled consensus and best practices - probably through a formal global database, with an annex that can include disagreements and critiques - would advance cybersecurity norm development by reinforcing settled consensus and focusing future work on the gaps in agreement.

SUMMARY

Given the ideological and diplomatic obstacles to reaching a formal and comprehensive cyber agreement in the near term, the most productive current option is to create and deepen support for cyber norms, build trust among stakeholders, maintain forward momentum, and narrow the ungoverned areas or ones lacking consensus so that when the political opportunity is ripe, ground has been laid for formal normative development. In reviewing pre-normative case studies in both cybersecurity and other arenas, what becomes evident is that the breadth of issues and obstacles in constructing a normative architecture for cybersecurity demands a number of complementary entry points that can mutually reinforce each other. But in considering how to structure such approaches, practical, technical measures have the best chance of advancing norm building.

First, given the ideologically fractionalized nature of the cybersecurity debate, technical cooperation has the best opportunity of escaping the politicization that has deadlocked normative discussions. By avoiding areas of sensitive disagreement, collaborations designed for practical problem solving can continue making advances in the near term. By doing so, they deepen cross-border relationships and advance good cyber practices that can incentivize and build toward normative development.

- *There is a growing appreciation of the benefit of confidence building among many regional bodies. The successful history of APCERT, along with the endorsement of CBMs among a variety of actors, provides an opportunity to invest in technical cooperation within regional bodies. Policy makers could consider calling for deeper investment by the relevant bodies in practical, technical cooperation among cybersecurity stakeholders.*

Second, building cyber capacity helps to develop the ability of diverse countries to support cyber norms. Such capacity building, particularly if coupled with data sharing on the impact of cyber incidents, builds a constituency for such norms by demonstrating their value for those countries' economies and security. Such efforts are at an early stage, but as seen in other contexts, they can likewise help build an understanding of the importance of cyber norms.

- *More investment can build up the capacity building field. Furthermore it is helpful to link such efforts to existing commitments so that the capacity building directly reinforces the normative consensus. Policy makers could consider calling for such investment, as well as highlighting data mapping to make the case for cyber norms for decision makers.*

Third while there is a benefit to utilizing narrowly framed agreements because they can be reached much earlier than global ones, such agreements are much more likely to develop beyond the initial list of signatories if their focus is based on sector or substantive considerations instead of a "club" of friendly states. The memo points out the trade example as one where a regional treaty was able to gain adherents over time. Likewise the financial sector has mechanisms that enjoy compliance among non-members. These narrowly defined mechanisms likely grew in size because they offered a practical benefit for the signatories, presented a benefit for others, and were not designed to preference some countries over others.

- *The recommendation based on these consideration is to shape any like-minded approach around specific sectors and develop the group of like-minded members based on their shared approach to the sector rather than what might be seen as a subjective measure of "friends versus others." Policy makers could explore a cybersecurity regime focusing on a particular sector, inviting experts from that area and collaborating with the traditional institutions in the sector to architect principles for a potential like-minded agreement.*

Throughout all these efforts, it is important to include a variety of stakeholders not only for better normative design, but also to ensure that they are respected and implemented. Without the private sector, normative discussions may be derailed, and certainly cannot take advantage of the latest in research and development. Without civil society, important levers for expanding consensus are undermined.

- *Both in technology governance and in other security precedents, multi stakeholder models have proven to be important for driving and developing consensus.*

Finally, while catalogs do not advance new norms, they reinforce existing consensus and allow negotiations to launch from a more advanced point by reminding us of established agreements.

- *The benefit of databases is less significant than of the other approaches highlighted above. Nevertheless the history of duplicative work and reopening of settled consensus shows the value of a comprehensive, searchable catalog (or several complementary ones).*

Recent experience in both cybersecurity and other contexts shows that practical incremental approaches can help loosen the logjam created by warring theoretical principles at a low point in diplomatic relations between key countries. There is an opportunity to design and invest in CBMs, capacity building and even narrowly framed agreements in ways that reinforce the power of each of them. This pre-normative approach promises to seed support for and understanding of cyber norms, which are important preconditions for ultimately negotiating a treaty.

MEMO 2
CONCEPTUALIZING AN INTERNATIONAL SECURITY REGIME FOR CYBERSPACE

Ms. Elonnai Hickok, COO, The Centre for Internet and Society, India

Mr. Arindrajit Basu, Consultant, The Centre for Internet and Society, India

MEMO №2

INTRODUCTION

Policy-makers often use past analogous situations to reshape questions and resolve dilemmas in current issues. However, without sufficient analysis of the present situation and the historical precedent being considered, the effectiveness of the analogy is limited.[85] This applies across contexts, including cyber space. For example, there exists a body of literature, including The Tallinn Manual[86], which applies key aspects (structure, process, and techniques) of various international legal regimes regulating the global commons (air, sea, space and the environment) towards developing global norms for the governance of cyberspace.

Given the recent deadlock at the Group of Governmental Experts (GGE), owing to a clear ideological split among participating states, it is clear that consensus on the applicability of traditional international law norms drawn from other regimes, will not emerge if talks continue without a major overhaul of the present format of negotiations.[87] The Achilles Heel of the GGE thus far has been a deracinated approach to the norms formulation process.[88] There has been excessive focus on the content and the language of the applicable norm rather than the procedure underscoring its evolution, limited state and non state participation, and a lack of consideration for social, cultural, economic and strategic contexts through which norms emerge at the global level. Even if the GGE process became more inclusive and included all United Nations members, strategies preceding the negotiation process must be designed in a manner to facilitate consensus.

There exists to date, no scholarship that traces the negotiation processes that lead to the forging of successful analogous universal regimes or an investigation into the nature of normative contestation that enabled the evolution of the core norms that shaped these regimes. To develop an effective global regime governing cyberspace, we must consider if and how existing international law or norms for other global commons might also apply to 'cyberspace', but also transcend this frame into more nuanced thinking around techniques and framework that have been successful in consensus building. This paper focuses on the latter and embarks on an assessment of how regimes universally maximized functional utility through global interactions and shaped legal and normative frameworks that resulted, for some time, at least, in a broad consensus.

[85] Richard E Neustadt and Ernest R May, *Thinking in Time : The Uses of History for Decision-Makers*, 1st FreePress pbk. ed. 1988 (New York : Free Press, 1988), accessed 6th May 2018, https://trove.nla.gov.au/version/44808522.

[86] Michael SchmittSchmitt. Tal*linn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge: Cambridge University Press, 2015.

[87]Eneken Tikk and Mika Kenttunen. "The Alleged Demise of the UN GGE: An Autopsy and Eulogy." 2017. Accessed May 1, 2018. http://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf

[88] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110, no. 3 (July 2016): 427.

METHODOLOGY

DEFINING CYBER SECURITY

To embark on investigating an international security architecture, we must first arrive at a workable definition of cyber security. While arriving at a definition has been the objective of many scholarly works, a single definition is yet to be formalized. The International Telecommunications Union came up with a broad definition, which this paper will use as a reference point.[89] ITU defined cybersecurity 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."*

Thus, we consider a global cyber security architecture from two separate but connected frames of reference. The first aspect, broadly termed 'cyber hygiene' comprises of the technical aspects of cyber security, as outlined in the ITU's definition, which includes developing safeguards to prevent computer infrastructure from risk and the sharing and co-ordination of best practices among the various concerned stakeholders. The second aspect of this architecture , which this paper will largely focus on is the development of a shared understanding on the nature of cyberspace, strategies for ensuring its continued stability and the key actors that play a role in shaping this framework. This aspect will require far more time and co-operation to arrive at a mutually acceptable understanding acceptable to most, if not all key stakeholders. Progress on these two aspects of the cyber security architecture can occur simultaneously-with technical solutions being developed in the short run, while the agreement at large is in the making.

OBJECTIVE

The objective of this report is to undertake an investigation into the procedural history of the negotiations that lead to the formation of four analogous functional regimes and assess how the processes of contestation around certain organising principles lead to an outcome of negotiated normativity. The regimes considered are:

1. The Law of the Seas and its the formation of the United Nations Convention on the Law of the Sea and its constituent Organisations-the International Sea-Bed Authority and the International Tribunal on the Law of the Sea
2. The evolution of the norm outlawing the Use of Force and the Development of International Humanitarian Law
3. International Trade Law leading to the General Agreements on Tariffs and Trade and the formation of the World Trade Organisation and
4. The evolution of the Paris Agreement.

[89] ITU. 2009. *Overview of Cybersecurity. Recommendation ITU-T X.1205.* Geneva: International Telecommunication Union (ITU). accessed April 30, 2018, http://www.itu.int/rec/T-REC-X.1205-200804-I/en

The background report will dissect the first two regimes in detail in chapters 2 and 3 and chapter 4 will highlight additional learnings from the trade and environmental regime. Chapter 5 will highlight the progress made in the cyber-security negotiations thus far. In doing so, it will reflect on some of the existing cyber norms, initiatives and proposals. The recommendations section in Chapter 6 will use key learnings of this investigation to propose how the norms formulation process in cyberspace could be reformed.

These regimes have been chosen for three similarities with current negotiations on cyber governance. First, they deal with the regulation of an area that offered some form of functional utility for all participating nations. Second, much like the present regime seeking to govern cyberspace, each of these regimes are the product of contestation between regional or strategic state groupings. Third, some of these regimes have led to the evolution of a central governing body or a dispute settlement mechanism. Most of these regimes have also been strained with increasing political disagreement and lower exit barriers in the past decade. Rather than viewing this development as a reason to exclude these regimes from our assessment, this report will consider the reasons that led to these recent fetters and assess the take aways these might have for cyberspace governance.

CHAPTER 1: THEORETICAL UNDERPINNINGS

In order to inform our assessment of each regime and subsequent recommendations, this chapter summarises the predominant theories on regime formation and parliamentary diplomacy that may aid the evaluation of the regimes considered in the following chapters.

CO-OPERATION AND CONTESTATION

Cyberspace and the prospect of the cyber-weapon has revolutionized traditional understandings of organizing principles of global governance in what Lucas Kello terms three degrees of cyber-revolution.[90] Third order cyber-revolution has altered the language and orientation of power through a weapon, whose transitory nature[91] makes it difficult to test and dissect it through traditional means. The cyber-weapon has thus not only systematically disrupted existing relationships between states but also altered the rules and norms that regulate their conduct. Second order revolution or systemic revision occurs when a cohort of outliers such as a whimsical dictator uses the cyber weapon to challenge the edifice of the global political framework.[92] Finally, first order revolution or systemic change refers to a drastic change in the main actors themselves with private actors entering the fray.[93] A traditional attack could easily be detected and acted against, thereby reducing the operations of non-state actors to small scale guerilla tactics which could not threaten the state driven edifice of conventional order. The unbound nature of the cyber weapon offers tantalizing prospects both for established actors in the international system

[90] Lucas Kello, *The Virtual Weapon and International Order* (Yale University Press, 2017) 86.

[91] Max Smeets " A matter of time: On the transitory nature of cyberweapons", *Journal of Strategic Studies*, (2017) 7.

[92] Kello 90.

[93] Kello 92.

who want to preserve power and for disruptors who want to use the weapon as a hitherto unforeseen avenue of gaining global influence.[94]

Even though the precise definition of a regime is contested, a widely accepted definition is "norms, rules and decision-making procedures around which actors' expectations converge in a given area of international relations."[95] A functioning regime creates a convergence of expectations and lays down acceptable standards of behaviour which may foster a general sense of obligation.[96] Regime theory considers states as principal actors in the international arena and argues that states pursue absolute gains through international co-operation while realists believe that hegemons want to pursue relative gains to maintain the existing power imbalances in their favour.[97] Regimes function often in the absence of authoritative central institutions and instead rely on the convergence of interests among states.[98]

Any international regime that attempts to regulate cyberspace must consider these unique characteristics while bearing in mind its élan vital as a borderless construct accessible to and therefore strategically important for modern communication, trade and the building of relationships. Regime theory has broadly been inspired by the theory of collective action that explains outcomes as the integration of party interests through co-operation or co-ordination. Arriving at an universal regime requires what are known as 'transaction costs' due to the need to coordinate among multiple actors.[99] Thus, in certain cases unilateral or bilateral bargaining may be more strategic unless the subject matter of the negotiations has an inherently entangled value and exhibits traits of the global commons, which means that there is a shared interest in its stability.[100]

The most renowned understanding of international co-operation has been put forward by Robert Axelrod in his theorization of an iterated prisoner's dilemma.[101] If players were to engage with each other only once in a simultaneous game, the optimal strategy for each player would be to 'defect'- that is, block the negotiations on a certain point.[102] However, if the game is repeated over an unidentified period of time, as in the case of international negotiations,the incentive structure changes as states that block one aspect of the negotiation may be punished by other states which retaliate by stonewalling other points of contention that are of value to the defector. Thus,

[94] Kello 92.

[95] Stephen D. Krasner, ed., *International Regimes*, Cornell Studies in Political Economy (Ithaca, NY: Cornell University Press, 1983), 2.

[96] Anu Bradford, "Regime Theory," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, February 1, 2007), 1, accessed April 30, 2018, https://papers.ssrn.com/abstract=2770647.

[97] Bradford, 5.

[98] Bradford, 5.

[99] John A. C. Conybeare, "International Organization and the Theory of Property Rights," International Organization 34, no. 3 (1980): 209–313.

[100] Four attributes of commons may be described as (1) Economic value which gives people a reason to capture them, (2) Indivisible or 'in joint supply', (3) Usable by and of interest to all players and 94) Non-excludable and non-rivalrous Francis T. Christy, "Marine Resources and The Freedom of The Seas," Natural Resources Journal 8, no. 3 (1968): 425.

[101] Robert Axelrod, *The Evolution of Co-operation* (New York, Basic Books, 1984) 174.

[102] *Ibid.*

as states interact with each other and build reputations, the negotiation of optimal outcomes are possible due to a convergence of interests in the subject matter of the negotiation at large.[103]

There are four key conditions, however, that facilitate successful cooperation.[104] First, both players must have low discount rates-that is they must care about the future in relation to the present.[105] Players who are irrational or impatient cannot fit into the paradigm of a co-operative iterated prisoner's dilemma scenario as they cannot resist the urge to cheat in round (n) rather than in round (n+1). This means that their threat to punish the other player in round (n+1) is not perceived as a credible threat by the other player. An example of this would be a 'rogue state' that is run by irrational or trigger-happy impulsive leader or a non-state actor who does not suffer reputational costs. *These states would probably not fit into the paradigm of a standard iterated co-operation game*. Second, the players must not know when the iterated game will end, which means that they will be continuously faced by the threat of punishment if they defect. Third, the payoffs from defecting must continue to be low in comparison from the payoffs available with co-operation. *Pay-offs may change over time, which may change the incentives to cooperate.* USA's withdrawal from the Paris Agreement could be seen as an example.[106] The reduced pay-offs in terms of complying with global environmental policy in comparison with the increased profit incentive of polluting and using the exit as optics to attract Trump's domestic support base acted as an ideal incentive to defect. *In cyberspace, this problem is particularly acute given the difficulties of attributing an attack, which may incentivise players to defect from agreed norms even after the regime has come into forc*e.[107] Finally, the strategies chosen by the players must be sufficiently exploitative and not too forgiving. If the response is too forgiving, the credible threat perception automatically goes down and the incentive to defect from the negotiations rises. *This would require states to operate in coalitions of like-minded states to ensure that their interests are placed on the bargaining table and are made a part of the bargain in the process.*

Trade-offs and bargaining, keeping the broader objective in mind, is undoubtedly an integral aspect of any negotiation. Therefore in order to facilitate dialogue and convergence, it is necessary for states to be entirely transparent and open about the significance of that particular issue. Once this posturing is made known to all states, trade-offs through broader packages and subpackages can commence.

[103] Douglas G. Baird, Robert H. Gertner, and Randal C. Picker. Game theory and the law. Harvard University Press, 1998., 164-72; Gibbons, Robert. Game theory for applied economists. Princeton University Press, 1992. 82-99; Indeed, the evolution of the norm of 2(4) was a product of interactions between states who jointly believed in the outlawing of war as a tool of conducting politics. The insertion of Article IV into the Outer Space Treaty, which calls for the demilitarization of Outer Space within two years of the commencement of negotiations on the Outer Space Treaty is a similar example. Both the major powers-USA and USSR recognized the immense destructive potential of using the rapidly proliferating nuclear arsenal in Outer Space and rapidly negotiated the Outer Space Treaty in order to prevent the nuclear arms race from spiralling into outer space.

[104] Jack L. Goldsmith and Eric A. Posner, "A Theory of Customary International Law," The University of Chicago Law Review 66, no. 4 (1999): 1126.

[105] Goldsmith and Posner, 1126.

[106] Demetri Sevastopulo, "US to Withdraw from Paris Pact in Blow to Obama Climate Legacy," Financial Times, June 1, 2017, accessed 6th May 2018, https://www.ft.com/content/af8c9b89-6497-39c4-9804-0bebe862bf53.

[107] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (January 2, 2015): 4–37.

ROLE OF INTERNATIONAL LAW

It is crucial to remember that law and norms are not conflicting but interrelated processes. As noted by Harvard Law Professor Lawrence Lessig, law can create, change or displace the meaning of social norms.[108] Backing from established tenets of International Law provides legitimacy to the evolution of cyber norms and can therefore influence collective expectations, and serve as a facilitative mechanism for drawing up bargaining points and charting out the path forward. The development of international legal regimes for the regulation of various global commons including outer space, the deep sea bed and the economic exploitation of marine resources has now lead to a stable normative regime that influences state practice today.[109]

The function of International Law and global governance structures is to enable coordination and co-operation in the long run and thereby develop a framework for the stable functioning of global polity. One of the major criticisms of both the project of International Law in general and the cyber norms effort to date has been the political erosion of attempts to obtain normative consensus.[110] While such criticism is valid, it overlooks an equally crucial role of the language of international law and the facilitation mechanisms of global governance structures that enable such conflict, the nature of the conflict, and ways in which conflict has been resolved in the past. Monica Hakimi argues that conflict in the short run may be beneficial for actors that seek to engage in a shared governmental endeavours as it can create nuanced discourse and careful examination of issues.[111] Initial conflict can also lead to co-operation in the long run due to the entangled dimensions of cyberspace and the vitality of its existence for nation states and the international community as it stands today.

TRAJECTORY OF NORM EVOLUTION

Finnemore and Sikkink identify three theoretical phases of norm evolution at the global level.[112] The first phase, known as '*norm emergence*', marks the recognition of the said norm by a set of critical states who have a stake in the issue at hand. After recognition, these critical states endeavour to promote this norm at the international level by generating global discourse or in Hakimi's paradigm, conflict. This phase is known as a 'norm cascade'. Finally, after concerted discourse at the international level, states internalise these norms as obligations that are binding either due to adoption in a legal code or through societal pressure.The transition from one phase to another is known as a tipping point that is catalyzed by *norm-entrepreneurs* which may be states, groups of states or non-state actors.

[108] Lawrence Lessig, "The Regulation of Social Meaning," *The University of Chicago Law Review* 62, no. 3 (1995): 943–1045.

[109] Nico Schrijver, "Managing the Global Commons: Common Good or Common Sink?," *Third World Quarterly* 37, no. 7 (July 2, 2016): 1252–67.

[110] "Getting beyond Norms: New Approaches to International Cyber Security Challenges" (C. Hurst and; Company, 2017).

[111] Monica Hakimi, "The Work of International Law," *Harvard International Law Journal* 58 (2017): 1.

[112] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (1998): 887–917.

Zartman and Berman divide the process of formal regime formation into three separate negotiating phases that broadly correspond to the three phases of Finnemore and Sikkink's analysis of norm evolution.[113] In the **diagnostic phase**, parties consider the possibilities of regime formation while sounding out like-minded parties who may act as norm-entrepreneurs and exploring the possibilities of negotiating conduct. In the **formula phase**, they jointly settle on a formula which seeks to facilitate the third phase, which is known as the **details phase** where the broad formula is refined, specific details are added and in certain cases, laws are codified.

HYPOTHESIS

This report argues that the cyber norms process thus far has seen a muddling of the three phases and an excessive eagerness to extend norms of International Law to cyberspace rather than using the language of international legal rules in consonance with negotiation strategies as a mechanism for the facilitation of contestation between concerned stakeholders.

CHAPTER 2: UNITED NATIONS CONVENTION ON THE LAW OF THE SEA

INTRODUCTION

After the failure of the second United Nations Convention on the Law of the Sea, it was clear that UNCLOS III was a conference that almost all stakeholders desired but , as will be highlighted in this paper,had to be incentivised to be brought to the negotiating table to agree on the contours of a regime that would enable universal acceptance. The negotiators at UNCLOS II had failed to reach any form of agreement on the sole norm in contention, which was the breadth of the territorial sea.[114] The motivations for pursuing multilateral agreements were different for each nation- the developed world saw this as their last chance of salvaging the exploitation of the open oceans while the newly decolonised, developing states wanted to preserve the swathes of water near their shores.[115] As highlighted comprehensively in Robert Friedheim's *Negotiating the New Oceans Regime*[116]**,** the remaining sixteen years that saw the codification of the UNCLOS remains, to date, the most complex yet perhaps one of the most successful outcomes of multilateral bargaining and co-operative regime evolution.

THE NEGOTIATION IN THREE PHASES

The diagnostic phase: This phase ended without setting an agenda for a major diplomatic conference or outlining of norms or norm entrepreneurs that could create the norm. However,

[113] William Zartman and Maureen R. Berman, *The Practical Negotiator* (Yale University Press, 1982), 102.

[114] Territorial waters is the area immediately adjacent to the shores of a nation and subject to the jurisdiction of that nation. In essence, it is within that nation's sovereign domain. At present, it is defined as 12 nautical miles from the shores of the territorial state.

[115] Alan Beesley. "The Negotiating Strategy of UNCLOS III: Developing and Developed Countries as Partners-A Pattern for Future Multilateral International Conferences." Law & Contemp. Probs. 46 (1983): 185.

[116] Robert. L. Friedheim. *Negotiating the new ocean regime*. Univ of South Carolina Press, 1993.

the Sea-Bed Committee produced a list of 150 subjects and divided them into 23 groups.[117] They also produced a list of issues. While contention was apparent among the various apparents, the diagnostic phase had clearly identified that the multilateral regime would be a universal one which would grapple with a range of issues.

The formula phase: The delegates at the third United Nations Law of the Sea Conferences in New York, Caracas and Geneva respectively were faced with two clear challenges[118]:

1. Establishment of the rules of interaction and way forward in the negotiations and
2. A formula that would take into consideration shared ideas and underpin a comprehensive treaty regime.

On point 1, they agreed that all issues would be attempted to be negotiated using consensus rather than a voting procedure that required a simple or a special majority.[119] This was because the Group of 77 - the block representing the global south could have used the voting process to create a treaty that fit its needs.[120] This would have resulted in the developed world leaving the treaty regime altogether as the pay-offs from defecting would have been greater than the pay-offs from remaining in the regime. Both the USA and USSR realized, regarding point 2, that the final outcome would have to be a package deal reflected in a 'single-negotiating text.[121] The various components of the text were negotiated by using informal sub-groups at UNCLOS.[122] The sub-groups agreed to the establishment of the 200 mile Exclusive Economic Zone, which would enable developing coastal states to exploit resources proximate to their territory in exchange for a 12-mile-territorial sea and a right of transit through straits that may be used for international navigation.[123]

The details phase: Despite the striking of relative fruitful bargains during the formula phase, working out the details of the agreement took seven years. The U.S. made many attempts to 'exit' the regime altogether.[124] Henry Kissinger's dramatic re-orientation proposed a 'parallel' system of regulating the deep sea-bed in a supposed bid to balancing the sovereignty driven monopoly of access approach taken by the Group of 77 and the unlimited licensing system which the developed states wanted.[125] However, the voice of the majority Group of 77 was not to be drowned out and they constantly opposed the U.S. proposal to legitimize open-access deep sea-bed mining.[126] This issue was discussed in Committee I under the stewardship of Jens Everson of

[117] Committee on the Peaceful uses of the seabed and Subsoil beyond National Jurisdiction, List of Issues Relating to the Law of the Sea, (A/AC.138/66).

[118] Friedlheim, 31.

[119] Friedlheim, 32.

[120] Alan G. Friedman; Cynthia A. Williams, Group of 77 at the United Nations: An Emergent Force in the Law of the Sea, 16 San Diego L. Rev. 555 (1979).

[121] Barry Newman, " The Law of the Sea is still unwritten, but Please Don't Fret," Wall Street Journal (27 Aug 1974) quoted in Friedlheim at 33.

[122] Barry Buzan. "'United we stand...': Informal negotiating groups at UNCLOS III." *Marine Policy* 4, no. 3 (1980): 183-204.

[123] James.E. Bailey III. "The Exclusive Economic Zone: Its Development and Future in International and Domestic Law." *La. L. Rev.* 45 (1984): 1269.

[124] Richard Darman. "The law of the sea: Rethinking US interests." *Foreign Affairs* 56, no. 2 (1978): 373-395.

[125] Friedlheim, 35.

[126] Williams and Friedman, 556.

Norway. Even though the final outcome had technical issues, it was a negotiation that had taken on board multiple stakeholders.[127] The G77 advisors drove the articles on the deep sea-bed which gave the seabed authority a broad-ranging variety of powers on the regulation of deep sea-bed mining.[128]

The discussions on the deep sea-bed lead to cascading of the norm demarcating this area as the 'Common Heritage of Mankind.' (CHM) Originally articulated by Maltese Ambassador at the United Nations General Assembly in 1967,[129] the concept claims that certain commons or elements that are of benefit to all of mankind must not be appropriated by states or individuals or corporate entities but be exploited under an international regime that facilitates exploitation in a manner beneficial to mankind as a whole.[130] After a thorough evaluation of the norm during debates at the LOSC Conference, This has now arguable evolved into customary international law and internalised by the international community due to the recognition of the symbiosis between equity and efficiency fostered through the principle.[131]

COALITIONS

The Group of 77 comprised of more than 120 states when the negotiations started and had a heterogenous group of members who were differentiated by region - Latin American/Caribbean/African/Asian or by special interest issues stemming from geographic disadvantages, such as being a landlocked state. Yet, they Ambassadors Koh and Jayakumar have highlighted that even among this broad coalition there was solidarity in areas where their interests converged but not so much congruence on other issues such as the Exclusive Economic Zone (EEZ), which were of relevance only to coastal states. [132]

Despite these differences, the use of the coalition had an influential impact on the negotiations. When this Group banded together on a certain issue, that was to be the 'default position' with which the other countries either had to negotiate or defect.[133] *This posed interesting strategic questions as it required the G77 to use their power of numbers to push forward their agenda and exhibit their 'voice' in the process while ensuring that their push was not aggressive enough to cause developed states to defect.*

[127] Friedlheim, 35.

[128] Danny.M. Leipziger and James. L. Mudge. "Seabed mineral resources and the economic interests of developing countries." (1976).

[129] Prue Taylor. "Common Heritage of Mankind Principle." In Klaus Bosselmann, Daniel Fogel, and J. B. Ruhl, Eds. *The Encyclopedia of Sustainability, Vol. 3: The Law and Politics of Sustainability.* 64–69. Great Barrington, MA. Berkshire Publishing.

[130] John E. Noyes, The Common Heritage of Mankind: Past, Present, and Future, 40 DENV. J. INT'L L. & POL'Y 447 (2012).

[131] Noyes 456.

[132]Tommy Koh, and Shanmugam Jayakumar. "The negotiating process of the Third United Nations Conference on the Law of the Sea." In *United Nations Convention on the law of the sea*, 1982. p. 29-134 (54).

[133] Friedlheim, 337.

NORM ENTREPRENEURS

The Asian-African Legal Consultative Committee, (now Asian-African Legal Consultative Organisation), which was set up during the Bandung Conference of the Non-Aligned Movement in 1955[134] acted as a norm entrepreneur and lobbying group for many rules that became codified to create a more equitable legal framework. At the meeting of the Working Group of the AALCC on the Law of the Sea held in Geneva in 1971, at the request of the AALCC, several delegates submitted papers highlighting the positions of their respective states on the prevailing complex issues, which could be identified as norm emergence.[135] The delegation of Kenya submitted an iconic paper on the 'exclusive economic zone' concept.[136] The delegation of Indonesia submitted a paper on 'The Concept of Archipelago' and the Malaysian delegate submitted a paper on 'International Straits'.[137] These ideas were raised before the Second Committee of the Law of the Seas Conference and treated as a cohesive representation of the perspectives of Asian and African states on these complex legal issues in the norm cascade process.[138] Following the success of these existing initiatives the AALCC worked towards the development of a cohesive legal regime that sought to regulate the deep sea-bed[139] Just after the third session of the Law of the Sea Conference in Geneva (1975), which produced the Single Negotiating Text (SNT), the AALCC prepared a detailed study of these drafts in order to further advise member states on the Law of the Sea and recraft existing norms in a manner conducive to the unique socio-economic interests of Asian and African states.[140]

ROLE FOR INTERNATIONAL LAW

There was little scope for extension of traditional principles of international law to the UNCLOS negotiations as the objective of the agreement was to modify the Grotian regime which recognised the high seas as a global commons unfettered by sovereignty and freedom for use by all.[141] The inexhaustibility of resources within the ocean and the increasing ideological dogma of post-colonial states in favour of a New International Economic Order[142] required a drastic re-

[134] Barry .Sen "*Evolution and growth of AALCC as a Forum for International Co-operation*" Asian-African Legal Consultative Committee. *Essays on international law*. Asian-African Legal Consultative Committee, 1981. 3- 21.

[135] Secretariat of the AALCC, *Report of the Twentieth, Twenty-First and Twenty-Second Sessions Held in Seoul (1979), Jakarta (1980) and Colombo (1981)* (New Delhi, 1981), 20.

[136]Sompong Sucharitkul. "Contribution of the Asian-African Legal Consultative Organization to the codification and progressive development of International Law." (2007).

[137] Kennedy Gastorn. "AALCO's Contributions to the Development of the Law of the Sea." Lecture, Wuhan University, Beijing, 2017: 7.

[138] Secretariat of the AALCC .Report of the Seventeenth, Eighteenth and Nineteenth Sessions Held in Kuala Lampur (1976), Baghdad (1977) and Doha (1978) (New Delhi, 1981,19-58.

[139] AALCC 20-25.

[140] AALCC 20-25.

[141] Hugo Grotius, *Freedom of the Seas or the Right which belongs to the Dutch to Take part in the East Indian Trade* (trans Ralph Van Deman Magoffin) (New York: Oxford University Press, 1916).

[142] The New International Economic Order ('NIEO') was officially endorsed by consensus of the UN General Assembly vide Resolution 3201 'Declaration on the Establishment of a New International Economic Order' A product of the rejuvenated era of decolonisation, the New International Economic Order sought to further principles of sovereign equality, interdependence and co-operation among all states, irrespective of the nature of their socio-economic

orientation of International Law for the regime to function rather than a mere re-orientation of existing principles that were grossly outdated.

Most claims were sought to be justified through an appeal to their acceptance as customary international law. Most of these proposals lead to greater conflict in the short run as each coalition utilised their own ideological extraction of international law to compete and ultimately synthesize with the conflict. For example,Latin American states strived to highlight a distinctively regional norm called the 'patrimonial sea'[143] which lay the edifice for discussions on an Exclusive Economic Zone(EEZ) and was used regularly by the G77 during the negotiation process.

CONTESTATION AND EXIT

The newly minted dogma of the 'New International Economic Order' acted as a prism through which the developing world viewed these negotiations and used this to re-claim sovereignty from western hegemony.[144] They used it as a tool for contestation on many issues, including the negotiation of the Exclusive Economic Zone and left this ideological concept immune from a bargaining move or trade-off. On other issues, however, there were several trade-offs forged. For example, the G77 allowed access to sea-bed minerals on the grounds of increased financial support for the International Seabed Authority or tighter production controls that would protect mineral producing states.

These trade-offs on the deep sea-bed mining provisions, in particular were not good enough for the United States.[145] The U.S. delegation returned to the Law of the Sea Conference in 1982 with an entire reconceptualization of the law on which consensus had been obtained over the course of the negotiations.[146] The U.S. return was not marked by a desire to negotiate but instead was an attempt to re-orient the negotiations in its favour by threatening exit. This did not work however and the Conference adopted the Law of the Sea Convention in April, 1982 without meeting U.S. demands. The U.S. then announced that it would not be signing the treaty in June, 1982. The U.S. exiting the negotiations did not cast a shadow on the legitimacy or enforceability of the Law of the Seas regime and the legal framework flourished nevertheless. The presence of the United States was not imperative for a regime that was designed to be multilateral. In this instance, the US played its cards wrong and misread the potential adverse effects on regime stability if it withdrew. *Given how robust the crystallized norms had become by the time UNCLOS came into force, US opinion on the treaty mattered little in the context of fervent dogma exhibited by states who wanted to re-claim their lost sovereignty.*

systems. See Giorgio Sacerdoti, " New international Economic Order," Oxford Public International Law, accessed 6th May 2018, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1542.

[143] Jorge.A. Vargas. "The legal nature of the patrimonial sea: a first step towards the definition of the exclusive economic zone." *German YB Int'l L.* 22 (1979): 142.

[144] Lawrence Juda. "UNCLOS III and the new international economic order." *Ocean Development & International Law* 7, no. 3-4 (1979): 223.

[145] James. L. Malone. "The United States and the Law of the Sea after UNCLOS III." *Law and Contemporary Problems* 46, no. 2 (1983): 33.

[146] Malone 33.

DISPUTE SETTLEMENT AND COORDINATION MECHANISM

The 1982 United Nations Convention on the Law of the Sea created the International Tribunal for the Law of the Sea as a neutral third party dispute settlement mechanism to resolve disputes between two states on any issue covered by UNCLOS. Judges are appointed on the basis of 'equitable geographical distribution' [147]As the Convention did not enter into force until 1994, the ITLOS became operational only in that year. It has so far adjudicated 23 disputes with 1 dispute pending before it at the present moment.[148] The disputes have spanned a wide range of issues, ranging from maritime delimitation to Part XV of UNCLOS that provides for compulsory adjudication but still allows states to retain a choice in the procedure they wish to adopt for resolution of the dispute. While states have generally chosen to refer their disputes to ITLOS, states have also approached the International Court of Justice or arbitration procedures due to more certainty in the former and more control over the process in the latter.[149] *This underscores the potential benefits and drawbacks of setting up dedicated dispute settlement mechanisms as opposed to relying established dispute settlement mechanisms.*

A coordination mechanism also exists under the Law of the Seas Regime in the form of the International Seabed Authority (ISA). Based in Kingston, Jamaica, it was set up to regulate mineral-related activities in the international sea-bed area, including in areas beyond the limits of national jurisdiction. As per Article 154 of UNCLOS, the Assembly of the ISA undertakes a systematic review of the functioning of ITLOS and suggests recommendations that may improve its impact. The Review of the ISA in 2016, articulated that the ISA has made significant efforts at organising and regulating activities in that area although there is still some doubt on how state entities are controlled effectively.[150] This fear is compounded by the fact that the authority largely operates behind closed doors and there is no published data on how contracts are awarded.[151] The Report suggests that there needs to be an independent and transparent regulatory body that is capable of enforcing the regulations devised by the ISA in order to ensure the efficacy of its functioning.

CONCLUSION

The UNCLOS negotiation is an example of the successful use of parliamentary diplomacy that sought to gain legitimacy by ensuring broad participation from a variety of states and taking into consideration a range of strategic concerns. Although the diagnostic phase did not generate anything substantive, it did signal to all states that any agreement regulating the seas must be based on universal consensus. In the formula phase, they agreed on voting rules for the negotiation process and decided on the outcome of the negotiations, which was to be a single

[147] "EJIL: Talk! – Election of Judges to the International Tribunal for the Law of the Sea," accessed April 30,2018, https://www.ejiltalk.org/election-of-judges-to-the-international-tribunal-for-the-law-of-the-sea/comment-page-1/.

[148] Hakimi, Monica. "The Work of International Law." *Harv. Int'l LJ* 58 (2017): 1.

[149] "EJIL: Talk! – The Hamburg Tribunal Heats Up? Is ITLOS Now in Business?," accessed April 30, 2018, https://www.ejiltalk.org/the-hamburg-tribunal-heats-up-is-itlos-now-in-business/.

[150] "*Comments by the Legal and Technical Commission on the Interim Report on the Periodic Review of the International Seabed Authority pursuant to Article 154 of the United Nations Convention of the Law of the Sea and the Comments by the Review Committee.*," 1, accessed May 1, 2018.

[151] Todd Woody, "Seabed mining can decide the fate of the deep ocean," Text, GreenBiz, September 28, 2017, accessed April 30, 2018, https://www.greenbiz.com/article/seabed-mining-can-decide-fate-deep-ocean.

negotiated text. Over a period of seven years that saw the formation of coalitions and the use of trade-offs and sub-packages, the present Law of the Seas regime was born. Norm-entrepreneurs such as the AALCC and coalitions such as the G77 banded together to press for a re-orientation of existing constructs such that the emerging economies may also benefit from the regime. There was constant reference to the participants ideological extractions of international law. The concepts of the patrimonial sea, sovereign equality and the New International Economic Order were repeatedly used as a frame of reference to facilitate discussion and consensus, in the long run. Due to the comprehensiveness of the final treaty and the large number of states that eventually came on board, exit by the United States did not matter for the survival of the regime.

CHAPTER 3: OUTLAWING THE USE OF FORCE AND THE DEVELOPMENT OF INTERNATIONAL HUMANITARIAN LAW

INTRODUCTION

International peace and stability is an entangled domain that all states have an interest in. Bearing this in mind, two separate bodies of law have crystallized to deter the possibility of the world reverting back to a continued state of barbaric warfare. The first, known as 'jus ad bellum' or the 'right to go to war' is embodied in the prohibition on the use of force in Article 2(4) of the U.N. Charter. The second, known as Jus in Bello (law in war) or International Humanitarian Law regulates conduct during warfare and is largely codified in the Hague Conventions and the Geneva Conventions and its Additional protocols. While the forms of interaction that lead to the codification of each of these bodies of law may have varied slightly, a common thread running through the development of both these bodies of law is that alongside considerations of *realpolitik* and strategic considerations - that ideas by individuals or groups of actors mattered in the development of each of these bodies of law.

NORM OUTLAWING THE USE OF FORCE

The origins and history of the main stakeholders involved in the development of this norm is captured comprehensively in Oona Hathaway and Scott Shapiro's 2017 unique history on the evolution of the norm entitled *The Internationalists.*[152]

The diagnostic phase: Before states entered the fray or the conception of the norm became a subject of discourse at multilateral fora, individuals conceptualized, theorized and re-defined the norm. Before the dawn of what Hathaway and Shapiro term 'the outlawry movement',[153] Hugo Grotius (dubbed 'The Father of International Law') defended warfare as an alternative to the Courts system for the prosecution of wrongs or restoration of rights. This remained the status quo in International Law until a Chicago-based commercial lawyer named Samuel Levinson collaborated with John Dewey, then Professor of Philosophy at Columbia University, Levinson wrote an article for *The New Republic* entitled " The Legal Status of War" where he argued that

[152] Oona Hathaway and Scott Shapiro, *The Internationalists:How a Radical Plan to Outlaw War Remade the World* (Simon Schuster, 2017).
[153] Hathaway and Shapiro, 109.

instead of working on onerous codes that sought to regulate the conduct of atrocities during warfare, war must be outlawed in its entirety.[154] *Despite the unique thought process and argumentation evident in the piece, backing at the institutional level was necessary to ensure legitimacy.*

James Shotwell, then Professor of History at Columbia University and adviser to President Wilson during the Versailles negotiations, sought to take the normative outlawing movement forward but also add to this process some 'teeth' or sanctions mechanism.[155] He corresponded with French Foreign Minister Briand and induced American Secretary of State Frank Kellogg to co-ordinate negotiations on the draft of a universal pact that would outlaw war. There were 31 signatories by the effective date.[156] Even though the Pact was unable to constrain the routine use of warfare by states and the outbreak of World War II itself, it sowed the seeds for what would become a far more all encompassing norm in the form of Article 2(4). Again, despite its irrelevance and lack of enforcement at the time, the Kellogg-Briand Pact is an example of an international norm whose emergence was utilised to frame conflict and then create consensus in the long run.

The language of the peace-pact was utilised by the Sub-Committee on International Organisation through a treaty which was originally drafted by James Shotwell in a recognition of the errors in judgment that occurred as a result of a toothless League.[157] A final proposal called "Plan for the Establishment of an International Organisation for the Maintenance of International Peace and Security" was presented to President Roosevelt of the United States and would serve as a draft for future negotiations on the regime.[158]

The formula phase: As World War II drew to a close, the British, American and Soviet delegates discussed what the contours of world order, post World-War II, would look like.[159] The enforcement of the prohibition on the use of force was an obvious inclusion given the tremendous destruction suffered even by the victors during the War. There were no incentives to defect from this co-operative equilibrium. Disagreement existed only on the enforcement of the norm. Soviet Ambassador Andrei Gromyko was adamant and would not concede on retaining veto powers for all permanent members of the UNSC even in matters that directly involved them. As a way of moving forward despite dissenting opinions, and instead of destroying all the progress made during the diagnosis phase, the delegates adopted a draft text that ultimately became the present U.N. Charter, but with an added note which clarified that the voting procedure was still under consideration.[160]

[154] Hathaway and Shapiro, 109.

[155] Harold Josephson. *James T. Shotwell and the rise of internationalism in America*. Fairleigh Dickinson Univ Press, 1974: 39-40; Hathaway and Shapiro 117-121.

[156] Hathaway and Shapiro, 122.

[157] Hathaway and Shapiro, 198.

[158] "*Plan for the Establishment of an International Organisation for the Maintenance of International Peace and Security*," December 23, 1943, FRUS,1944, Vl 1 (General), 615.

[159] Hathaway and Shapiro, 199.

[160] U.S. Department of State, Dumbarton Oaks Documents on International Organisations, 2223: 13.

The details phase: In February 1945, representatives of fifty nations and forty two non governmental groups congregated to usher in the United Nations organisation.[161] However, as president Truman mentioned in his opening address, the Conference was not a mere formality as the issue of voting procedures at the UNSC still had to be agreed upon.[162] The smaller powers resisted the use of the veto power, which struck them as being inherently inequitable. However, the voice of the major powers carried through and the veto powers were retained. The negotiation of Article 2(4) was far more simple as this norm had already been explored in great detail both in the diagnosis and formula phases and on June 26, 1945, all 50 nations present signed the UN Charter.[163]

INTERNATIONAL HUMANITARIAN LAW

The diagnostic phase: Due to progress made on the codification of the Laws of War through the 1907 Hague Conventions, there was already some agreement on the nature of the rules that would govern war, although these agreements were pragmatic considerations fostered on reciprocity rather than a desire to create a new international regime. So the diplomats who negotiated the Geneva Conventions in 1949 already had the substance ready at hand, from the Hague Conventions and from international custom, which was coupled with their collective understanding of all that had gone wrong during the atrocities of World War II. The four Geneva Conventions were *negotiated without much contestation due to the uncontroversial and aspirational nature of the norms* contained therein.[164] Right from the time of their drafting, the Conventions were not entirely relevant for a world that was fast changing with different modes of warfare and different kinds of actors, such as newly decolonized states entering the fray.[165] An update and re-orientation of the regime was needed. Norm emergence, cascade and internalization occurred relatively fast but the norms themselves were out of date and lacked specific codification which could create a robust regime protecting civilians and medical personnel during the conduct of hostilities.

Addressing this, the International Committee of the Red Cross took the initiative to press for another Conference in 1974 and had already prepared a draft treaty carving out specific obligations and legal guarantees. This draft was prepared based on the experiences of their personnel and from the criticisms of the Conferences of Governmental Experts in 1971 and 1972.[166]

The formula phase: The Conference titled the Geneva Conference on the Re-affirmation and Development of International Humanitarian law was convened in 1974 by the Swiss government

[161] Hathaway and Shapiro, 211.

[162] “Harry S. Truman: Address to the United Nations Conference in San Francisco,” accessed April 30, 2018, http://www.presidency.ucsb.edu/ws/?pid=12391.

[163] Hathaway and Shapiro, at 213.

[164] John Dwight Ingram. "The Geneva Convention is Woefully Outdated." *Penn St. Int'l L. Rev.* 23 (2004): 79.

[165] Dwight, 79.

[166] George H. Aldrich, Establishing Legal Norms through Multilateral Negotiation--The Laws of War, 9 Case W. Res. J. Int'l L. 9 (1977).

which was the depository of the original Geneva Conventions.[167] Although approximately 120 delegations are believed to have attended - the number of active participants may have been around 70. The community believed that a comprehensive agreement with broad-based state participation was required for a robust re-orientation of Humanitarian Law.[168] The first Conference was held up by procedural baggage such as whether invitations should be extended to national liberation movements- a question that was decided by a majority vote.[169] Similarly, the question of whether national liberation wars qualified as international armed conflicts was also decided by majority vote, which meant that the protections provided for in the Geneva Conventions apply.[170] This irked United States, at which point, they threatened to exit the negotiations.[171] The second session of the Conference was marked by trade-offs and compromises - a pattern which continued into the Third Session of the Conference. Compromises had to be made on certain key issues and voting on the less contentious ones.[172] A particularly contentious issue was the granting of Prisoner-of-War status for guerilla fighters given the North Vietnamese tactics used in the Vietnam War which the US was entangled in. Another point of contestation between the Western States and those lead by the Soviet Bloc was regarding the principle of proportionality. The Soviet bloc and other representatives from the third world believed that this would grant military commanders too much discretion during an armed conflict.[173] The Western States responded by claiming that proportionality did not mean abandonment of the conduct of hostilities but lay in a more realistic understanding of the extent to which the laws of war could regulate this conduct.

The details phase: *Many of the contentious issues during the formula phase were overlooked through the utilisation of vague or ambiguous language* in the final draft. The issue about guerrillas was resolved by stating that combatants must identify themselves as soon a there is 'deployment' - a convenient term because no one had an understanding of what it meant.[174] Finally, after such diplomatic wrangling for four years, Additional Protocol 1 that dealt with external armed conflicts and Additional Protocol II which dealt with internal armed conflicts were negotiated. Despite the broad array of compromises, the new conventions plugged many of the gaps left by the original Geneva Conventions. The term 'civilian' was defined for example and given a vast array of protections. In many ways, the codification tilted the balance of the laws of war towards humanitarianism from military necessity.[175] Four decades after their adoption, there are now 174 State Parties to AP I and 168 State Parties to AP II.

[167] Aldrich, 10.

[168] Aldrich, 10.

[169] Kalshoven, Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts: The First Session of the Diplomatic Conference, 5 NETH. Y.B. INT'L L. 3 (1974).

[170] Amanda Alexander, ' A short History of International Humanitarian Law' 26 EJIL 1 (2015), at 124.

[171] They ultimately did not sign. Reagan, Ronald. "Letter of transmittal." *The American Journal of International Law* 81, no. 4 (1987): 910-912.

[172] Amanda Alexander, ' A Short History of International Humanitarian Law' 26 EJIL 1 (2015), at 124.

[173] *Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, Geneva* (1974–1977), vol. 14 (1981).

[174] George.H. Aldrich. "Guerilla Combatants and Prisoner of War Status." *Am. UL Rev.* 31 (1982): 871.

[175] Antonio Cassese, 'A Tentative Appraisal of the Old and the New Humanitarian Law of Armed Conflict', *The New Humanitarian Law of Armed Conflict*. Vol. 1. Editoriale scientifica, 1979.

NORM ENTREPRENEURS

The ICRC has played a major role in the negotiation of International Humanitarian Law across decades and in several instances has been more proactive in taking initiatives than many states.[176] For example vide a memorandum dated February 15, 1945, the ICRC stated that it would initiate consultations for the purpose of drafting the Geneva Conventions and brought together governments and National Societies to gather the necessary expertise and documentation.[177] On the basis of the deliberations and conclusions reached through these informal consultations and the preparatory conferences, the ICRC formulated the four draft conventions and re-formulated them after the Seventeenth International Conference of the Red Cross that met in Stockholm.[178] They then transmitted these drafts to the Swiss government which acts as the depository of the Geneva Conventions and circulated these drafts to all countries invited to the diplomatic conference in Geneva in 1949. The drafts prepared by the ICRC were used for deliberation at the Conference and provided an edifice around which negotiations could take place. They played a similar roles in the process building up to the Additional Protocols as they recognized that a world divided in the midst of the Cold War would not easily revise the tenets of humanitarian law. Again, it prepared the draft which served as the basis for deliberations at the Conference, which was then forwarded to the Swiss government which initiated the dialogue.

CONCLUSION

The norm outlawing the use of force and the codes regulating the conduct of atrocities were both products of active engagement and facilitation by norm-entrepreneurs. In the case of the norm outlawing use of force, individuals and their ideas enabled states to come together to agree on an universal principle that to this day remains the bedrock of international relations. This reorientation happened through initial agreement through the Kellogg-Briand Pact. Even though this norm was flouted, as evidenced by the outbreak of the Second World War, it laid a formula for the post-war negotiations that resulted in the articulation of Article 2(4) of the UN Charter. The trajectory of IHL was slightly different as the Geneva Conventions were signed and internalised rapidly but were not in sync with the requirements of rapidly evolving modes and consequences of warfare. Norm entrepreneurship by the ICRC and contestation between the Western and developing world finally resulted in the Additional Protocols which have been widely signed and ratified. Much like cyberspace,the outlawing and regulation of warfare mark a domain, whose stability all states have an interest in preserving and the lessons learned from this case study have much to offer in the context of cyber negotiations.

[176] Francis Buignon. "The International Committee of the Red Cross and the development of international humanitarian law." *Chi. J. Int'l L.* 5 (2004): 191.

[177] Memorandum adresse par le Comiti international de la Croix-Rouge aux Gouvernements des Etats parties d la Convention de Genive et aux Socits nazonales de la Croix-Rouge, 27 Revue intemationale de la CroixRouge 85 (1945), quoted in Buignon 194.

[178] Seventeenth International Red Cross Conference (Stockholm, Aug 1948), Report (Swedish Red Cross 1948); Seventeenth International Conference of the Red Cross.

CHAPTER 4: LEARNINGS FROM TRADE AND ENVIRONMENT

This chapter endeavours to build on the detailed case studies and highlight some additional learnings from the trade and environmental regimes. While these regimes bear some similarities with the trajectory of regime evolution illustrated in the previous two chapters, the processes and outcomes of these regimes offer some further useful insights that work on the cyberspace regime should take note of.

GOVERNMENT PARTICIPATION

The process of developing the Paris Agreement saw participation from countries from across the world including developing and developed. In total 195 countries joined the agreement except for Syria - as it was in the middle of conflict and subject to U.S and E.U sanctions and Nicaragua - as it felt that the agreement was not robust enough.[179] In 2017, both Nicaragua[180] and Syria[181] became a signatory to the agreement. Prior to Nicaragua and Syria joining, in 2017, Donald Trump announced that the United States will withdraw from the agreement.[182] Despite exit by the U.S., experts have maintained that Trump's position will geopolitically hurt the U.S. and give countries like China the ability to become leaders in this arena.[183]

NEGOTIATION PROCESS AND STRATEGIES

The Paris Agreement was a formal 'agreement at large' in which consensus was facilitated through extensive informal processes and networking during the conference. In his article, *The Paris Agreement on Climate Change: Behind Closed Doors*, Radoslav Dimitrov highlights the important role that diplomatic tactics play in consensus building including understanding and leveraging the nuances of structure and process, micro-dynamics of negotiations, and coordination. Radoslav provides an account of the conference and how strategies such as negotiating only with actors directly relevant to issues, limiting the number of open deliberations, and presenting text in a 'take it' or leave it fashion was key in facilitating consensus.[184]

[179] Friedman, Lisa. "Syria Joins Paris Climate Accord, Leaving Only U.S. Opposed." The New York Times. November 07, 2017. accessed April 30, 2018, https://www.nytimes.com/2017/11/07/climate/syria-joins-paris-agreement.html.

[180] "Paris Accord: US and Syria Alone as Nicaragua Signs." BBC News. October 24, 2017. accessed April 30, 2018, http://www.bbc.co.uk/news/world-latin-america-41729297.

[181] "US and Syria Left Alone on Climate Accord," *BBC News*, October 24, 2017, sec. Latin America & Caribbean, accessed April 30, 2018, http://www.bbc.com/news/world-latin-america-41729297.

[182] "Statement by President Trump on the Paris Climate Accord," The White House, accessed April 30, 2018, https://www.whitehouse.gov/briefings-statements/statement-president-trump-paris-climate-accord/.

[183] "Why Abandoning Paris Is a Disaster for America," *Foreign Policy* (blog), accessed April 30, 2018, https://foreignpolicy.com/2017/06/01/why-abandoning-paris-climate-agreement-is-bad-for-america-trump/.

[184] Radoslav S. Dimitrov, "The Paris Agreement on Climate Change: Behind Closed Doors," Global Environmental Politics 16, no. 3 (July 15, 2016): 1–11.

PARTICIPATION FROM NON STATE-ACTORS

The Paris Agreement saw wide participation from governments during the conference as well as non-governmental actors – including civil society, industry, investors, state governments etc. Broadly, the UNFCCC allows for NGO participation which is facilitated through an accreditation process by the UNFCCC Secretariat. Accredited NGO's have the ability to lobby, produce formal statements, propose policy options and make presentations.[185] The participation from non-governmental actors in the Paris Agreement has been highlighted as playing an important role in placing additional pressure on governments during the negotiations, as well creating a series of successful commitments outside of those made by governments.[186] Importantly, the participation of private sectors and other key actors was not limited to the conference, and these stakeholders have continued to play an active role at the country level as governments begin to undertake policies to meet commitments.[187] It has also been noted that non-state actors can play an important role in the review process under the Paris Agreement by offering independent expertise, comparative insight, and push for the uptake of outcomes at the national level.[188]

CONSENSUS AND COMPROMISE

The Paris Agreement has been represented as being based on equal compromise and reciprocal tradeoffs. Thus every government walked away from the table with gains and compromises. For example, Radoslav provides accounts of how in the end, China did not obtain legally binding action and weaker transparency standards, yet their position on finance and mitigation was accepted. Similarly the US achieved a weaker stance on the legally binding character of national actions, but their desired standard of mandatory and progressive evolution and financial differentiation was not incorporated.[189]

RIGIDITY OF INTERNATIONAL LAW MECHANISMS

The Paris Agreement has been called out by experts as an Agreement that achieved a balance between the need for national autonomy with an international responsibility by legally requiring countries to undertake and report on actions, but leaving the exact nature of these actions up to the country.[190] Known as the common but differentiated responsibilities and respective

[185] Giese, Lucas J. "The Role of NGOs in International Climate Governance: A Case Study of Indian NGOs." (2017), accessed April 30, 2018, https://digitalcommons.csbsju.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1037&context=honors_thesis.

[186] "Building Toward Breakthrough: Energizing the Paris 2015 Climate Negotiations and Post- Paris Action Agenda through Broader Engagement." Yale Climate Change Dialogue | Yale Center for Environmental Law & Policy. July 2015. accessed April 30, 2018, https://envirocenter.yale.edu/projects/yale-climate-change-dialogue.

[187] Subnationals, Non-State Actors Are Crucial for Paris Success | UNFCCC," accessed April 30, 2018, https://unfccc.int/news/subnationals-non-state-actors-are-crucial-for-paris-success.

[188] Harro Van Asselt and Thomas Hale,. "How non-state actors can contribute to more effective review processes under the Paris Agreement." *Policy Brief (Stockholm: Stockholm Environment Institute, 2016)*.

[189] Radoslav S. Dimitrov, "The Paris Agreement on Climate Change: Behind Closed Doors," Global Environmental Politics 16, no. 3 (July 15, 2016): 1–11.

[190]Radoslav S. Dimitrov, "The Paris Agreement on Climate Change: Behind Closed Doors," Global Environmental Politics 16, no. 3 (July 15, 2016): 1–11.

capabilities – it is a principle in environmental law that emerged from the 1992 Earth Summit. The principle recognizes *"the need to evaluate responsibility for the remediation or mitigation of environmental degradation based on both historical contribution to a given environmental problem and present capabilities".*[191] Experts have noted that the flexibility of NDCs was key to the success of the Paris Agreement.[192]

The transformation of the levels of Exit and Voice available to stakeholders from the GATT to the WTO offers some interesting prospects for the study of the adequate rigidity of a legally binding agreement.[193] The GATT was initially conceptualized as a 'gentleman's club' which was primarily a *political non-binding agreement with low-levels of legal discipline and therefore lower contestation because states were less incentivised to actively contest terms that would not have strict legal consequences.* This interaction worked in a bi-directional manner as the low levels of political participation prevented consensus from developing on the thornier questions of global trade. In effect, it was reduced to a business like negotiation for the reduction of tariffs rather than an agreement at large.

The World Trade Organization, however was a multi-stakeholder initiative that sought to arrive at an agreement at large that would set legally binding obligations. Due to the interconnected nature of the world trade system, exit options are scarce because most countries are members to it. This combined with high levels of legal discipline means that there is more active contestation by various groups of countries to obtain a more equitable deal in the setting of norms. This has also lead to *regime shifting by various nations who feel that regional or mega-regional trade agreements would be more conducive to their needs than the cumbersome WTO process*.

TRANSPARENCY AND ACCOUNTABILITY MECHANISMS

In the Paris Agreement, the transparency, accountability, and compliance system established is meant to ensure positive and continuous progress towards nationally defined goals. A key way this was achieved was by placing a legally binding requirement on parties to define, communicate, and undertake a nationally determined mitigation contribution. Though parties are not legally bound to achieve defined targets, it is required that policies and goals and progress towards the same must be regularly communicated and must progressively become stronger.[194] To facilitate this accountability and transparency, the Paris Agreement puts in place technical expert reviews, a multilateral peer review process, and a standing committee on implementation and compliance.[195] The role that transparency and accountability play in the Paris Agreement have been noted as key in building trust and confidence.[196]

[191] Bonnie Smith, "Adapting the Paris Agreement," *Vermont Journal of Environmental Law*, n.d., accessed April 30, 2018.

[192] "The Paris Agreement and Beyond: International Climate Change Policy Post-2020 | Belfer Center for Science and International Affairs." Harvard Kennedy School Belfer Center for Science and International Affairs, accessed April 30, 2018, https://www.belfercenter.org/publication/paris-agreement-and-beyond-international-climate-change-policy-post-2020.

[193] Joost Pauwelyn, "The Transformation of World Trade," *Michigan Law Review* 104, no. 1 (October 1, 2005): 1–65.

[194] Radoslav S. Dimitrov, "The Paris Agreement on Climate Change: Behind Closed Doors," Global Environmental Politics 16, no. 3 (July 15, 2016): 1–11.

[195] INSIDER: An Enhanced and Effective Framework for Transparency and Accountability in the Paris Agreement | World

THE BARGAINING PROCESS

The GATT used to function on the basis of a majority vote due to its nature as a political club with relatively low levels of contestation.[197] The WTO has adopted a consensus approach to voting on major policy issues, which has stonewalled progress on various issues since 2001. While the consensus voting requirement does provide voice to developing countries, the exercise of voice is only considered relevant and legitimate if the veto is exercised in consonance with a coalition.

DISPUTE RESOLUTION BODY

The WTO Appellate Body is an example of an effective and independent judicial system that has managed to extricate itself from the political trappings of the WTO. They have resolved various controversial issues with reference to the laws codified in the founding agreements which has sometimes found them at odds with trade policy elites. However, their neutrality was understood by all ultimately and lead to the cementing of the WTO as an independent authority rather than a politically driven compromise.

CHAPTER 5: PROGRESS IN CYBERSPACE

The inextricable weaving of the Internet of Things (IoT) into commerce, social interaction and military strategy universally has rendered its nature similar to any other 'global commons. States have clearly diagnosed that an international regime is needed to govern its use and restrict its weaponization in order to ensure its continued stability and utility. However, the amorphous and ever-changing nature of cyberspace and the vastly contested perceptions of the phenomenon has stood as challenges to the international community from arriving at a formula that could precipitate shared notions of cyber governance for three key reasons.First, t*here is a cultural divide on the essence of cyberspace - as a free-flowing entity that states should patrol with as light a touch as possible and the idea of information sovereignty, which prefers strict sovereign regulation*. Second, *the unknown potential of pursuing offensive strategies in cyberspace and the limited potential of deterrence given the difficulties of attribution incentivise states to defect from the co-operative equilibrium* simply because they remain unsure regarding the quantity of pay-offs when they cheat or co-operate. This also *prevents them from displaying all their preferred strategies and outcomes at the negotiation table as that would tie their hands in case a future opportunity for strategic exploitation opened up*. The utility of cyberspace in altering or re-orienting prevailing global power asymmetries is a reality the cyber governance project must grapple with. Finally, the *increased role of non-state actors in the prevailing cyber security architecture means that state negotiators will have to understand the needs, motivations and ideologies of those operating both in the offensive and defensive realm*. The heterogeneity of

Resources Institute," accessed April 30, 2018, http://www.wri.org/blog/2015/12/insider-enhanced-and-effective-framework-transparency-and-accountability-paris.

[196] INSIDER: An Enhanced and Effective Framework for Transparency and Accountability in the Paris Agreement | World Resources Institute," accessed April 30, 2018, http://www.wri.org/blog/2015/12/insider-enhanced-and-effective-framework-transparency-and-accountability-paris.

[197] Pauwelyn 5.

actors and motivations together with the complexity of the phenomenon itself turns the regulation of cyberspace into a unique challenge for the international community.

Diagnosis Phase: In 1998, Russia proposed a treaty at the United Nations that would regulate and restrict the utilization of cyber-attacks and cyber weapons.[198] The initial proposal adapted its idea from norm proliferation in the avenue of arms control and disarmament. At the time, this proposal was opposed by the United States and found little support. Academic discourse on the development of an international cyber security convention was also discarded as impractical and failed to gain traction within the United Nations.[199]

Further research on the *utilization of non-binding norms and confidence building measures as an alternative to the development of a full-fledged treaty regime lead to an alternate approach within the international community.*[200] The approach drew from the norms based approach in regimes such as the Missile Technology Control Regime and helped shape the UN-GGE process. The GGE was set up in 2004 and comprised of independent experts from 15 states. This group was initially meant to advise the UN on promoting peace and stability in cyberspace. While the first UN-GGE was not able to finish a report, the second GGE was more fruitful and ended up releasing a report in 2010. The third GGE which presented its report in 2013 agreed on a set of founding norms for the governance of cyberspace.[201] The document basically stated that international law, state sovereignty and human rights were applicable to the governance of cyberspace. The report also stated that states must not use non-state proxies to commit cyber- attacks on other states or allow non-state actors to use their territory for the launching of cyber-attacks.

MAKINGS OF A FORMULA

The 2015 report of the fourth UN-GGE elaborated on these concepts and laid down a comprehensive framework for further discussion on cyber norm evolution. Section III of the report lays down several norms, rules and principles for responsible state behaviour in cyberspace.[202] The 2013 and 2015 reports of the GGE have the makings of a broad formula for devising a regime on cyberspace. However, it has not fostered agreement on many crucial normative questions, including on the definition and nature of cyberspace itself. Therefore, instead of continuing to focus on extrapolating academic theory in International Law to promulgate new norms, focus must be shifted on the process behind obtaining universal consensus on a formula that works for all stakeholders-so that work may proceed on the details phase.

[198] James Andrew Lewis, " Revitalizing Progress on International Negotiations in Cybersecurity" in Donahoe, Eileen, Melissa Hathaway, Paul Twomey, James A. Lewis, Joseph Nye Jr, and Eneken Tikk. "Getting beyond Norms: New Approaches to International Cyber Security Challenges." (2017): 13.

[199] Lewis 13.

[200] Lewis 13

[201] "The UN GGE on Cybersecurity: How International Law Applies to Cyberspace," Council on Foreign Relations, accessed April 30, 2018, https://www.cfr.org/blog/un-gge-cybersecurity-how-international-law-applies-cyberspace.

[202] United Nations, *2015 GGE Report*: 12.

HURDLES

Drawing from what appeared to be consensus within the group on the norms process a fifth GGE was instituted by the United Nations "to study, with a view to promoting common understandings, … how international law applies to the use of information and communications technologies by States, as well as norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building…."[203] However, due to what cyber security and International Law expert and chair of the Tallinn Manual Process, Prof.Michael Schmitt terms the 'politicization of cyber norms,' the UN-GGE was not able to arrive at consensus due to stonewalling by Cuba and reportedly China and Russia. Gauging from Cuba's publicly available statement[204], the UN-GGE disagreed on three fundamental questions. It appears from their statement that applying the contested norms of international law to the cybersphere would convert cyberspace into a 'theatre of military action' and legitimize unilateral punitive sanction. Mike Schmitt is critical of this position -arguing that it has no validity in international law and has been adopted by states to gain an asymmetric strategic advantage as the states engaged in the stonewalling were rarely the victims of unlawful cyber attacks.[205] Further, as pointed out by Arun Mohan Sukumar, the dissenting states did not want the rules of the game to be dictated by militarily advanced states - a problem that can only be solved through multilateral parliamentary diplomacy that takes all stakeholders on board in the norms formation process. [206]

CONTESTATION

A core divide in the cyber norms formation process revolves around the question of sovereignty.[207] The Sino-Russian view suggests that sovereignty in international law is absolute and no entity other than the sovereign state itself can limit the exercise of this power.[208] Consequently, both Russia and China believe that each country has the right to manage the use

[203] Michael Schmitt and Liis Vihul, "International Law Politicized: The UN GGE's failiure to advance cyber norms," *Just Security*, Jun 30 2017, accessed 6th May 2018, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

[204] Declaration By Miguel Rodríguez, Representative Of 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, New York, June 23, 2017.

[205] These include not knowingly allowing their territory to be used for the commission of internationally wrongful acts using Information Communication Technologies (ICTs); to cooperate for the exchange of information using ICTs; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations and to not knowingly supporting ICT activity contrary to the principles of international law.

[206] "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?," Lawfare, July 4, 2017, accessed 6th May 2018, https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

[207] Eneken Tikk and Mika Kenttunen. "The Alleged Demise of the UN GGE: An Autopsy and Eulogy." 2017. Accessed May 1, 2018. http://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf

[208] Assembly, UN General. "Developments in the field of information and telecommunications in the context of international security." *UN document A/C* 1 (2015): 66.; Zeng, Jinghan, Tim Stevens, and Yaru Chen. "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty"." *Politics & Policy* 45, no. 3 (2017): 432-464.

of its own cyberspace and define its ‘network frontiers’[209]through the implementation of domestic legislation or the framing of state policy. According to this group of states, each country has the right to patrol information at its cyber borders - a view which has been a principled stand in accordance with their long-time reading of International Law.[210] According to these countries, ICTs come laden with foreign influence and can disrupt the sovereign authority of the concerned state[211], which is directly at odds with the desire of the US and like-minded states in the G-7 to preserve the free-flow of information.

The Russian chair of the 2004/2005 GGE stated that issues of 'international informations security' must be discussed in light of the global information revolution.[212] The UK and US have repeatedly stated that the use of the term in this fashion indicates that information itself is a security threat which must be guarded against.[213] As per their position, excessive focus on ‘information security’ could potentially spiral a shift towards a position where the internet no longer serves as a platform for the rapid exchange of discourse and ideas but as domains of excessive sovereign regulation.[214] The alleged Russian interference in the U.S. elections through the spread of fake misinformation and ‘fake news’ via social media platforms has resulted in calls for the re-evaluation of this stance and assess these actions against existing international law and national security strategy and thus amend domestic policy accordingly .[215]

The ideological split on the nature of cyberspace has also resulted in two radically different approaches on how to regulate it. The United States has pushed for a soft ‘norms’ based approach where they seek to apply existing tenets of International law to cyberspace without creating a new treaty and promoting them aggressively.[216] The use of this terminology might be confusing as the application of International Law to any domain would result in the creation of autonomous binding obligations on all states even in the absence of a treaty. So, it remains

[209] Yuan Yi,. “网络空间的国界在哪 ” [Where Are the National Borders of cyberspace]? 学习时报. May 19 2016. Accessed on Jan 06, 2018, http://www.studytimes.cn/zydx/KJJS/JUNSZL/2016-05-19/5690.html.

[210] *Yuan Yi; Tikk and Kerttunen,* at 17; Grigsby, Alex. "The End of Cyber Norms." *Survival* 59, no. 6 (2017): 109-122: 111.

[211] Yu Li . “如何认识与维护互联网主权” [How to Understand and Protect Internet Sovereignty]. Peoples Daily. February 2, Accessed on Jan 06, 2018, http://media.people.com.cn/GB/16996575.html.

[212] 13th Plenary Meeting of the First Committee A/C.1/60/PV.13: 5.; See also 2000 Information Security Doctrine of the Russian Federation that was re-adopted in 2008 and remained in force until December 2016 when a new Doctrine on Information Security of the Russian Federation was adopted. See further the Chinese contribution in 2006, whereby the free flow of information should be guaranteed under the premises that national sovereignty and security must be safeguarded and that the historical, cultural and political differences among countries be respected (Developments in the Field of Information and Telecommunications in the Context of International Security (A/61/161)) in *Tikk and Kerttunen,* at 18.

[213] Assembly, UN General. "Developments in the field of information and telecommunications in the context of international security." *UN document A/C* 1 (2015): 66.

[214] Assembly, UN General. "Developments in the field of information and telecommunications in the context of international security." *UN document A/C* 1 (2015): 66.

[215] "Election Hacking, As We Understand It Today, Is Not A Cybersecurity Issue." Lawfare. January 05, 2018. Accessed Jan 06, 2018, https://www.lawfareblog.com/election-hacking-we-understand-it-today-not-cybersecurity-issue; "International Law and the US Response to Russian Election Interference." Just Security. January 05, 2017. Accessed Jan 06, 2018, https://www.justsecurity.org/35999/international-law-response-russian-election-interference/.

[216] Finnemore, Martha. "Cultivating international cyber norms." *America's cyber future: Security and prosperity in the information age* 2 (2011): 89-100.

unclear why the US approach is considered a 'soft approach' to cyber governance. On the other hand Russia and China have stated that existing tenets of customary International Law were never intended apply to cyberspace and the creation of a new *lex specialis* (specific law) through the drafting of a treaty that regulates cyberspace is required.[217]

THE BIRTH OF COALITIONS

Much like in the case of the other regimes, a variety of regional and strategic groupings have put forward representations of their orientation on cyber-governance.[218] The Joint Statement made by the BRICS leaders at Xiamen in September, 2017 and prioritised the equal participation of all states in cyber governance and the need to make structures that regulate cyberspace more representative and inclusive.[219] This critique applies to the GGE process where the P5 have participated in all five GGE processes. Estonia, Belarus, Brazil and India have participated in four while Canada, Egypt, Japan and Mexico have been a part of three GGE processes. Other states have been involved in two or less.[220]

The G7 have also used their strategic grouping to endorse the applicability of the framework of International Law and the UN Charter-including self-defense, human rights law and humanitarian law through the G7 Declaration on Responsible State Behaviour in Cyber Space in April, 2017.[221] The joint endorsement of this doctrine by G7 states makes their position on the applicability of International law clear although clearer articulation providing legal reasoning and pragmatic enforcement mechanisms is needed. On the other hand, India also endorsed the communique of the meeting of G20 Finance Ministers and Central Bank Governors in Baden-Baden, Germany in March 2017, which focused on the need for digital financial inclusion[222] and addresses the role of cybersecurity in the protection of financial services.[223] The European Union High Representative of the Union for Foreign Affairs and Security Policy submitted a report that explicitly recognised the importance of developing a political response to cybersecurity threats as many of the threats themselves are geopolitical in nature. [224]Further, the report acknowledged that cyberspace is a domain of operations like land, air sea and space and therefore deserves priority in EU's defense

[217] "Political and Military Aspects of the Russian Federation's State Policy on International Information Security" *Military Thought*, 2015.

[218] "Comparing Cybersecurity Norms," Carnegie Endowment for International Peace, accessed April 30, 2018, https://carnegieendowment.org/publications/interactive/cybernorms.

[219] BRICS. "BRICS Leaders Xiamen Declaration." (2017).

[220] Australia, Ghana, Indonesia, Israel, Kenya,Malaysia and South Africa have been a part of two GGEs. Argentina, Colombia, Botswana, Cuba,Finland, Italy, Jordan, Kazakhstan,Mali, Netherlands,Pakistan, Qatar, Senegal,Serbia, Spain, South Korea, Switzerland have been involved in just 1 GGE process.

[221] "G7 Declaration On Responsible States Behavior In Cyberspace" www.mofa.go.jp/files/000246367.pdf

[222] Ministers, Finance. "Communiqué Meeting of Finance Ministers and Central Bank Governors." *March 2017*, at para 7, accessed April 30, 2018, http://www.g20.utoronto.ca/2017/170318-finance-en.pdf.

[223] Ministers, Finance. "Communiqué Meeting of Finance Ministers and Central Bank Governors." *March 2017,* at para 7, accessed April 30, 2018, http://www.g20.utoronto.ca/2017/170318-finance-en.pdf.

[224] "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" accessed April 30, 2018, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN, at 17.

strategy.[225] Russia has extended its multilateral efforts regionally at the Shanghai Cooperation Organization (SCO). In 2009, the SCO arrived at an agreement that aimed to guarantee 'international information security'.[226] In 2011, Russia and China were supported by other SCO countries in their submission of a draft, which was updated in 2015. These proposals lay out the rules of the road in cyberspace governance that focuses on 'international information security' and sovereignty[227] China took over the rotating Chairmanship of the Organisation this year and the next meeting will be held in Qingdao in July 2018. It is possible that Russia and China may continue to use the organisation to continue to pivot towards the signing of a cyber treaty and India's participation in this Organisation sets it up nicely to get involved in this process if it strategically suits its needs.In addition to the independent multilateral initiatives, there have also been several bilateral and tri-lateral initiatives seeking to articulate common understandings on cyber norms[228] These understandings could be useful for the purpose of building economic or diplomatic relationships with states although to be of any normative or legal significance, clearer legal reasoning would be needed.

CHAPTER 6: RECOMMENDATIONS

There were a number of factors that came together to ferment the success of the different agreements outlined above and can serve as lessons that can be carried over to the cyber negotiations process. The unique nature of cyberspace means that the recommendations need to be tailored to account for the unique nature of pay-offs and costs that the transitory nature of offensive cyber weapons or the problems of attribution in cyberspace hold for states and non-state actors. With this framework in mind, we articulate eleven recommendations under the following sub-headings : Size of negotiations, The Bargaining Process, Negotiation Strategies, Role of International law, Role of non-state actors and Dispute Resolution and coordination mechanisms.

SIZE OF NEGOTIATIONS

Recommendation 1: *There should be an agreement at large that involves all states and invites non-state actors to the table as interested stakeholders.*

Analysis: It is apparent that an agreement that regulates the entangled dimensions of cyberspace cannot be substituted by processes that involve a sample representation of states. While the GGE process marked an important point of commencement for future cyber negotiations, it cannot

[225] "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" accessed April 30, 2018, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN, at 81.

[226] Concluded between People's Republic of China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan on July 16, 2009.

[227]Assembly, UN General. *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, UN Doc.* A/69/723, annex I (Jan. 9, 2015), accessed April 30, 2018, http://www. un. org/ga/search/view_doc. asp, 2015.

[228] "Comparing Cybersecurity Norms," Carnegie Endowment for International Peace, accessed April 30, 2018, https://carnegieendowment.org/publications/interactive/cybernorms.

mark the end of the process and needs to be built on by involving all states. In order to foster legitimacy, strength, and sustainability of the emerging norms, there must be an agreement at large, which considers the voices of all states in a manner that encompasses widespread consent to the broad contours of the regime, even if consensus cannot be arrived at on every sub-point. This agreement at large needs to ensure that the voices of industry, civil society, and academia are also taken into account because these non-state stakeholders are becoming increasingly important for cyber governance and stability. The Environmental, UNCLOS and Use of Force regimes offer key learnings in this regard. Given the entangled dimensions of the phenomenon being negotiated, bilateral agreements that foster fragmented understandings of the concept at hand are not effective. The universal nature of these agreements not only enabled internalization of the norms and evolution of some of the legal provisions to the status of custom but also protected the regime when powerful players such as the US threatened exit from the regime. We believe the character of the cyber norms process should be 'multilateral with multi-stakeholder engagement.' Unlike other regimes, offensive operations in cyberspace impacts a wide range of actors-both in conjunction with and severed from state interests. Further, it has a range of implications for human rights and civil liberties. Therefore, it is crucial to have representatives from private sector and civil society present at the negotiations and representing their views and experiences in dealing with cyber security issues. While facilitating consensus among a diverse range of non-state entities may be difficult, it is important that their views are reflected at the table and taken into account by the decision-makers.

Feasibility: Present discourse on cyber security is fragmented into various regional or strategic groupings who harbour different understandings of cyber security and the role of an international regime that might regulate its contours. In order to build on the fragments of an existing formula, all parties must be brought to the negotiating table. The use of strategic negotiation tactics deployed by a robust and neutral coordination mechanism, which could be inter-governmental bodies such as the UN First Committee or non-governmental bodies such as the GCSC could work towards facilitating a positive outcome that can be considered by decision-makers.

THE BARGAINING PROCESS

Recommendation 2: *Ideas, research, and a pre-existing material (drafts and agreements) are critical foundations and should be leveraged.*

Analysis: As evident from our case studies, often the dawn of an all-encompassing regime are from ideas that emerge through conversations, correspondences and paper presentations by individuals, organizations or coalitions. The outlawing of war or the emergence of the Exclusive Economic Zone both originated as academic ideas that were then taken forward at the institutional level. Therefore, even though, the Tallinn Manuals have not found widespread consensus among states, it is crucial that the rigorous ideas incorporated in these texts are not ignored in the cyber governance project simply due to the fact that they have adopted a deracinated approach to the norms process. Instead, they can serve as the edifice on which future consensus can be forged.

Apart from academics, neutral non-governmental organisations can also play a crucial role. The ICRC's pre-draft of the Geneva Conventions and the Additional Protocols helped speed up the negotiations and served as the language of International Law that facilitated conflict initially and then finally, consensus. Microsoft's proposal for a Digital Geneva Convention could potentially play a future role as a foundational text.[229]

Feasibility: Given the wide array of academic scholarship and back-channel talks involving civil society groups, there is no dearth of ideas on the future of cyberspace. More channels of engagement, interaction and coordination between academics and policy-makers should be encouraged to ensure that these ideas play a role in the norm-creation process through bodies and forums like the IGF and the GCSC. Furthermore, there are over 70 existing multilateral and bilateral accords that should be considered and leveraged when negotiating an agreement.[230]

Recommendation 3: *There must be transparency in the bargaining process at two levels: (1) Internal Transparency: This would be internal to the Parties and not necessarily the public and (2) Transparency of process and outcomes: This would be communicated to the public at large which would foster confidence in the negotiation process and thereby enable states to represent a wide array of domestic and international stakeholders in the proceedings.*

Internal Transparency - All the regimes studied involved trade-offs and compromises and the formulation of packages and subpackages. Assuming all states are strategically incentivised to formulate an international regime for cyberspace due to the stability it fosters, they must be willing to compromise while sticking to their key policy requirements. However, they must be clear and transparent about the packages that are more important for their ideological or strategic needs so that the bargaining process can flourish. The New International Economic Order and the sovereign rights to the Exclusive Economic Zones was a bargaining chip that the G77 was not willing to compromise on during the UNCLOS negotiations both due to economic necessity and ideological dogma.

The case studies also demonstrate that undertaking a negotiation process with a clear understanding of country preferences can facilitate a bottom up cooperative process. In the Paris Agreement, this was in part achieved by having Parties present their 'intended nationally determined contributions' prior to COP21.[231]

Transparency of process and outcomes - The GGE process thus far has been marred by opacity. The draft of the failed 2017 GGE has not yet been released, which has prevented widespread public debate on the stumbling blocks rather than using it as a tool for progressive conflict.

Feasibility: While transparency is an ideal notion, decision-makers must strive for the non-attributability of offensive cyber action means that states and non-state may gain greater payoffs from not disclosing their capabilities and preferences. There needs to be robust diplomatic

[229] Brad Smith, "The need for a Digital Geneva Convention," Microsoft, Feb 14,2017, accessed Apr 28th 2018, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

[230] "Comparing Cybersecurity Norms," Carnegie Endowment for International Peace, accessed April 30, 2018, https://carnegieendowment.org/publications/interactive/cybernorms.

[231] Nationally Determined Contributions (NDCs) | UNFCCC," accessed April 30, 2018, https://unfccc.int/process-and-meetings/the-paris-agreement/nationally-determined-contributions-ndcs#eq-5.

posturing to persuade states to adopt transparency mechanisms both during and after the negotiation process. There needs to be conviction that both the reputational gains and global stability gained through transparent strategies, commitments, and progress thus enabling responsive and collective action and response.

NEGOTIATION STRATEGIES

Recommendation 4: *Coalitions of like-minded states grouped by common ideology, interests, focus areas or identities may aid in fostering positive conflict , identifying key areas for consensus and in the development of a formula in the long run*

Analysis: A fragmented approach to cyber governance may not fulfill the goal of regulating cyberspace, but it could be a potential catalyst for a stable international system as it would allow for some certainty in the formation of strategic alliances and in national approaches to cyberspace. Coalition-building was successfully used to articulate varied state interests and anchor the negotiations throughout the UNCLOS process through groups such as the G77. Further, given the nature of contestation in cyberspace and the present lack of consensus on applicable International Law, fragmentation, through regional or strategic groupings may be the way forward in the short-run until universal minimum core markers of consensus may be found. This process lead to the success of norm entrepreneurs such as AALCC during the UNCLOS negotiation process. Their recommendations and declarations aided the genesis of a formula that guided the negotiations. As outlined in the Report, existing governmental groups and forums could be potentially leveraged such as the Freedom Online Coalition, the G7, or the G20 as spaces for consensus building on specific topic areas.

Feasibility: Overlapping consensus among multiple fragmented groupings is possible if the various coalitions approach the negotiations willing to make compromises while not letting go of the core ideological basis of their groupings. For example, the G77 entered into trade-offs with the western states on various issues but none that threatened the establishment of an Exclusive Economic Zone under the agenda of the New International Economic Order.

Recommendation 5: *In order to work out the various formulae, informal negotiation must be encouraged.*

Analysis: Informal negotiation among a variety of smaller groups will allow delegates to engage with each other as individuals that represent the social, cultural and economic needs of the citizens of that state or region rather than engaging in a deracinated format as macro-state units. This mode of engagement was particularly fruitful in the Law of the Seas and the Paris Agreement negotiations as it converted a 'one-size-fits-all' approach into a more inclusive ones that sought to recognize the diverse concerns of participating states. Progress can be made one issue at a time rather than trying to work out the details of all issues simultaneously once a broad formula has been agreed upon.

Feasibility: This recommendation is feasible once all delegates have been brought together for the negotiation process. It will also facilitate engagement and informal dialogue with non-state actors.

Recommendation 6: *Voting must seek to facilitate consensus by using tactics such as the Indaba strategy*

Analysis: The mode of voting on issues must seek to facilitate consensus. A process that builds on voting by the majority would amplify the voices of coalitions but could therefore reduce the incentives for major powers to stay on in the agreement. This was seen in the UNCLOS, IHL and the Paris Agreement. The harms of exit by a major power for the future of the regime must thus be considered. In the case of UNCLOS, the development of IHL or the Paris Agreement, the US exit did not threaten the existence of the regime. However, if the US were to exit the WTO and set up parallel regimes, then the future of the trading system would need re-evaluation. In the case of cyberspace, it is too early to risk exit by any country from the negotiations altogether due to the entangled nature of cyberspace and the lack of an already established broad formula. Instead, modes of negotiation that allow consensus to emerge without jeopardizing the process must be adopted. The Indaba negotiation strategy that obliges dissenters to propose alternate paths may be useful to ensure that any stonewalling is done after considering the path ahead.

Feasibility: While apparent divisions discussed in cyberspace negotiations as discussed Chapter 5 make the emergence of consensus on certain issues difficult, consensus on the least common denominator must be the goal of any negotiation.

Recommendation 7: *Large regimes are decades in fruition. A small start does not dictate the eventual result.*

Analysis: Most multilateral regimes evolve over a long period of time in order to enable the accommodation of multiple views and interests. It is important to not set a fixed deadline and enable the negotiations to evolve organically. However, while a diplomatic agreement is in the making, more urgent progress is needed on developing technical solutions that can prevent internet infrastructure from being attacked or utilised as third-party systems when an attack is being carried out. Cooperation with non-state actors can facilitate the needed research and development of these solutions.

Feasibility: As long as a coordination mechanism that enables various stakeholders to interact regularly is set up, allowing time to accommodate diverse viewpoints should be beneficial for the cyber norms process.

ROLE OF INTERNATIONAL LAW

Recommendation 8: *International Law must be used as a tool for the facilitation of positive conflict but the cyber norms process must be careful to not delve into the details of its application until a broad formula has been worked out.*

Analysis: As seen in the UNCLOS negotiations, reference to existing principles of International law or regional understandings such as the notion of the patrimonial sea are key for laying out a framework for further discussion. These principles serve as a common baseline on which first, positive conflict and then, consensus can emerge. Before jumping on to the applicability of specific norms of International Law in cyberspace, there must be consensus on what the broad contours of the agreement would be. For that to happen, there needs to be a common understanding on the essence of cyberspace, the extent to which it can be weaponized and the rights and obligations of sovereign nations in this sphere. Before arriving at answers on specific questions such as the applicability of standards of self-defense or standards of attribution, broader questions on the nature of cyberspace and the extent of sovereignty that may be exercised therein need to be answered first.

Recommendation 9: *The cyber norms process is not ready for the imposition of rigid, legally binding obligations as a desired outcome yet.*

Analysis: The legally binding outcomes of the process should not be envisaged until a formula has been agreed upon. However, at this stage, the focus should be on national capacity building and voluntary compliance with cyber security requirements much like the INDCs at the Paris Agreement. A rigid legally binding agreement risks amplifying contestation or increasing Exit by many key players, something the process can ill-afford at this state due to the nascency of the negotiations and the real need to cull out a workable agreement. Once a shared formula is arrived at, the objective-either in the form of a global treaty or 'soft norms' can be agreed upon driven by increasing political participation by stakeholders who feel incentivised to improve the outcome of the process.

Feasibility: Texts such as the Tallinn Manual set out a useful trajectory for the application of international law. However, the cyber norms process is not ready to apply these norms in detail and must therefore use existing principles of international law to arrive at a clear picture on the formula first.

ROLE OF NON-STATE ACTORS

Recommendation 10: *Wide participation by non-state actors can be key in negotiation processes.* I*dentification of norm-entrepreneurs and supporting them may be important for a successful outcome.*

Analysis: Involvement of non-state actors can create external pressure for outcomes to be reached that are acceptable to the public, can contribute to the objectives of the agreement, and can play an important role in accountability at the national level of state commitments. At the sametime, states are often reluctant to take initiatives on matters which would require an agreement at large as the transaction costs of facilitating consensus would be greater than the individual benefits of a stable regime. Therefore, multi-stakeholder non-state bodies and forums pursuing multi-stakeholder models of Internet Governance such as the, GCSC, IGF, ICANN, ISO, ITU, and ISOC should continue to play a role-both in finding areas for collaboration, generating ideas, normative content, and developing standards that could inform a future agreement. These forums and bodies can also serve as spaces for bringing multiple actors to the table to discuss key issues and in doing so establish a foundation for future discussion. Such interactions are already taking place. For example, ICANN and OAS have signed an MOU to cooperate on common areas of interest relevant to cyber security.[232] Such bodies can and do play an important role in

[232] "ICANN and OAS to work together to increase regional cyber security', 30 Oct 2015, ICANN blog, accessed Apr 28th 2018, https://www.icann.org/news/announcement-2015-10-30-en.

areas such as capacity building - for example the ITU undertakes capacity building efforts towards harmonizing regulatory frameworks and the Global Forum on Cyber Expertise undertakes capacity building efforts inline with international legal frameworks.[233]   Apart from non-governmental organizations, large private sector organizations most significantly affected by the weaponization of cyberspace should also be consulted so that the formula agreed upon takes into account their experience, understanding, and requirements. It is crucial that governments also continue to engage with these non-state actors throughout the negotiation process.

Feasibility: There are multiple non-state actors that have been involved in the present multi-stakeholder cybersecurity process. The key lies in enabling them to play a role in either co-ordinating the arrangement or providing valuable expertise, depending on the nature of the organisation.

DISPUTE RESOLUTION AND COORDINATION BODY

Recommendation 11: *A dispute resolution or co-ordination body is needed but the present legal regime is not robust enough to create a mechanism that adjudges cyber disputes yet.*

Analysis: The dispute resolution mechanism in the cyber norms process can emerge at two stages. Right now, even before the conclusion of the formula phase of the negotiations, a global consortium that establishes best practices and conducts cyber security inspections may be crucial. This is because until a more cohesive formula is drawn up, a judicial tribunal will not be able to rule on International cyber disputes.

Once a formula has been arrived at and political consensus has enabled the framing of parameters for attribution of cyber offensive attacks, a judicial body with teeth such as the WTO Appellate Body may be considered.

Feasibility: Feasibility of setting up these coordination mechanisms depends on the willingness of various stakeholders to fund, arrange and support the functioning of these mechanisms.

[233] Sash Jayawardene, Joris Lakis and Erin Jackson," Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance". November 2015, The Hague Institute for Global Justice.

ANNEX
SUMMARY OF FINDINGS

Aspect of Negotiation	UNCLOS	Use of Force/ Development of IHL	Trade	Environment	Implications for Cyber
Size	Multilateral- more than 150 + negotiating states, 150 + negotiating issues	**Use of Force**: Kellogg-Briand Pact had 31 signatories by effective date; 14 states party to the negotiations. Initially, 50 parties signed the UN Charter **IHL**: Geneva Conventions ratified by 196 states; Additional Protocol ratified by 174,168 and 73 states respectively and had around 120 members participating in negotiations	Started off small - 23 countries at GATT 1947 but WTO has 164 members	174 states And the EU were parties; 196 signatories	Should be an all-encompassing agreement at large
Formal/ Informal Bargaining Process	Number of informal bargaining groups and sub-committees on various issues	Formal bargaining process driven by heads of states and leading diplomats	Business style tariff reductions at GATT, more holistic law-driven consensus building at WTO	Multilateral process with 'formal informals'	Informal bargaining processes to diagnose an appropriate formula
Rigidity of International Law	Output was a single negotiated treaty text	Engraved into Article 2(4) has been recognized as customary international law **IHL**: Codified body of law in the Four Geneva Conventions and two Additional Protocols	GATT: Low levels of legal discipline, WTO: Rigid structure of International Law	Internally Determined Contributions (INDCs)- voluntary compliance	Until formula diagnosis, a 'light touch' approach should be adopted that ensures 'cyber hygiene' without forcing states to make commitments

Aspect of Negotiation	UNCLOS	Use of Force/ Development of IHL	Trade	Environment	Implications for Cyber
Time	Took 15 years as there was no time pressure. Diagnostic Phase: 6 years; Formula Phase: 2 years; Details Phase: 7 years	Pact of Paris was negotiated between 1925-1929 although the informal origins of the idea came as early as 1919; UN Charter was negotiated within a year of the Dumbarton Oaks Conference in 1944 **IHL**: Geneva Conventions negotiated quickly in the aftermath of World War II. Additional Protocols took longer between 1974-77	GATT was negotiated quickly after World War II. Came into effect by 1947. Uruguay Round setting up the WTO took 8 years.	Negotiations officially took between 30 Nov-12 Dec, 2015 but built on 4 decades of environmental jurisprudence	Should not set a fixed deadline until a formula emerges
Negotiation Strategies	Use of trade-offs and packages/sub-packages	Use of trade-offs to determine what the functioning of UNSC would be like and the core norms of IHL	Tariff reductions were the initial trade-off but as the WTO mandate grew to fields such as Intellectual Property, informal mechanisms had to be deployed to facilitate consensus	Use of trade-offs and sub-packages	Clear use of trade-offs and sub-packages in a transparent manner so that all parties are aware of the bargaining chips
Decision Rule	Consensus or near consensus in decision-making	**Use of Force**: Consensus among the major powers **Geneva Conventions**: Majority Vote with negotiation on key substantive issues	Simple majority at GATT; Consensus with every party having a veto at WTO	Indaba negotiation strategy	Facilitative consensus along the lines of the Indaba orientation

Aspect of Negotiation	UNCLOS	Use of Force/ Development of IHL	Trade	Environment	Implications for Cyber
Evidence of Exit and Voice	Multiple coalitions such as the Group of 77 formed to give 'voice' to the needs of developing countries. USA did not sign the treaty in 1982	Entire process was driven by the major military powers at the time. Article 2(4) was driven by the victors of World War II, so there was not much scope for the exercise of 'voice' although there was contestation among the major powers	GATT-Low Legal discipline-High Exit-Low Voice; WTO-	USA has indicated that they will exit the Agreement	Should try to ensure maximum voice for all participants while ensuring that the tipping point for exit is not met
Use of Non-State Groups	Largely state-centric process	Academics that originally conceptualised the idea leading up to KB Pact; IICRC emerged as a major norm enterpreneur in the field of IHL	While NGOs are now increasingly coming into the fray, the original negotiations were largely state-centric initiatives	NGOs and specialist groups were invited to the negotiation process and helped drive consensus	Groups like the GCSC should endeavour to facilitate consensus, prepare research and take initiatives at conferences. There must also be constant state engagement with the private sector
Set up of Dispute Resolution/ Co-ordination Body	ITLOS; International Sea-Bed Authority	ICJ//UNSC	WTO Dispute Settlement Body	Climate Change Displacement Co-ordination Agreement to tackle forced migration due to environmental reasons	Cyber consortium that ensures cyber hygiene compliance and fosters co-ordination in international cyber dispute resolution and investigations

MEMO 3
DEFINING OFFENSIVE CYBER CAPABILITIES

Mr. Thomas Uren, Visiting Fellow Cybersecurity, International Cyber Policy Centre, ASPI

Mr. Bart Hogeveen, Analyst, the International Cyber Policy Centre, ASPI

Mr. Fergus Hanson, Head, International Cyber Policy Centre, ASPI

MEMO №3

INTRODUCTION

States are developing and exercising offensive cyber capabilities. The United States, the United Kingdom and Australia have declared that they have used offensive cyber operations against Islamic State,[234] but some smaller nations, such as the Netherlands, Denmark, Sweden and Greece, are also relatively transparent about the fact that they have offensive cyber capabilities.[235] North Korea, Russia and Iran have also launched destructive offensive cyber operations, some of which have caused widespread damage.[236] The US intelligence community reported that as of late 2016 more than 30 states were developing offensive cyber capabilities.[237]

There is considerable concern about state-sponsored offensive cyber operations, which this paper defines as **operations to manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems or networks**.

It is assumed that common definitions of offensive cyber capabilities and cyber weapons would be helpful in norm formation and discussions on responsible use.

This paper proposes a definition of offensive cyber operations that is grounded in research into published state doctrine, is compatible with definitions of non-kinetic dual-use weapons from various weapons conventions and matches observed state behaviour.

In this memo, we clearly differentiate offensive cyber operations from cyber espionage. We address espionage only in so far as it relates to and illuminates offensive operations. Only offensive cyber operations below the threshold of armed attack are considered, as no cyber operation thus far has been classified as an armed attack, and it appears that states are deliberately operating below the threshold of armed conflict to gain advantage.[238]

This paper examines the usefulness of defining cyber weapons for discussions of responsible use of offensive cyber capabilities. Two potential definitions of cyber weapons are explored—one very narrow and one relatively broad—before we conclude that both definitions are problematic and that a focus on effects is more fruitful.

Finally, the paper proposes normative courses of action that will promote greater strategic stability and reduce the risk of offensive cyber operations causing extensive collateral damage.

[234] Michael S Rogers, Commander US Cyber Command, statement to the Senate Committee on Armed Services, 27 February 2018, online; Prime Minister Malcolm Turnbull, 'Offensive cyber capability to fight cyber criminals', media release, 30 June 2017, online; Director GCHQ, speech at CyberUK18, 12 April 2018, online.

[235] Council on Foreign Relations, *Europe is developing offensive cyber capabilities: the United States should pay attention*, 26 April 2017, online.

[236] Council on Foreign Relations Cyber Operations Tracker, online.

[237] James Clapper, Marcel Lettre, Michael S Rogers, *Foreign cyber threats to the United States*, joint statement for the record to the Senate Armed Services Committee, 5 January 2017.

[238] Although offensive cyber operations have been used by combatants in the context of armed conflicts.

DEFINITIONS OF OFFENSIVE CYBER CAPABILITIES

This section examines definitions of offensive cyber capabilities and operations in published military doctrine and proposes a definition consistent with state practice and behaviour. We first define operations and capabilities to clarify the language used in this report.

What are capabilities? In the context of cyber operations, having a capability means possessing the resources, skills, knowledge, operational concepts and procedures to be able to have an effect in cyberspace. In general, capabilities are the building blocks that can be employed in operations to achieve some desired objective. Offensive cyber operations use offensive cyber capabilities to achieve objectives in or through cyberspace.

US military joint doctrine defines offensive cyber operations as 'operations intended to project power by the application of force in and through cyberspace'. One category of offensive cyber operations that US doctrine defines is 'cyberspace attack'—actions that manipulate, degrade, disrupt or destroy targets.[239]

UK military doctrine defines offensive cyber operations as 'activities that project power to achieve military objectives in, or through, cyberspace. They can be used to inflict temporary or permanent effects, thus reducing an adversary's confidence in networks or capabilities. Such action can support deterrence by communicating intent or threats.'[240] UK doctrine further notes that 'cyber effects will primarily be in the virtual or physical domain, although some may also be in the cognitive domain, as we seek to deny, disrupt, degrade or destroy.'

In both UK and US military doctrine, offensive operations are a distinct subset of cyberspace operations that include defensive actions; intelligence surveillance and reconnaissance and operational preparation of the environment—non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations.

This is consistent with the Australian definition, which is that offensive cyber operations 'manipulate, deny, disrupt, degrade or destroy targeted computers, information systems or networks'.[241]

The Netherlands' defence organisation sees offensive cyber operations as 'digital resources whose purpose it is to influence or pre-empt the actions of an opponent by infiltrating computers, computer networks and weapons and sensor systems so as to influence information and systems'.[242]

Two common threads in state definitions are identified. Offensive cyber operations:

- are intended to deny, disrupt, degrade, destroy or manipulate targets to achieve broader objectives (henceforth called denial and manipulation effects)

[239] Joint Chiefs of Staff, JP 3-12, *Cyberspace operations*, Joint Publication 3-12 (R), 5 February 2013, unclassified version, online.

[240] UK Ministry of Defence, *Cyber primer*, 2nd edition, July 2016, online.

[241] From the Department of the Prime Minister and Cabinet, *Cyber lexicon* (in draft). This is consistent with public statements by the Minister Assisting the Prime Minister for Cyber Security, who has described using 'offensive cyber capabilities to disrupt, degrade, deny and deter' adversaries.

[242] 'Defence cyber strategy', letter from the Minister for Defence, 23 February 2015, online.

- have a 'direct real-world impact'.[243]

Another observation is that these definitions stress that 'while cyber operations can produce stand-alone tactical, operational, and strategic effects and achieve objectives, they must be integrated' in a military commander's overall plan.[239] This doctrine, however, originates from military establishments within a relatively narrow range of countries. In other states, offensive cyber operations may well be less integrated into military planning and will occur to achieve the political and/or strategic goals of the state leadership.[244]

This paper proposes that **offensive cyber operations manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems or networks**.

There are relatively few publicly available offensive cyber doctrine documents, but observed behaviour indicates that states such as Iran, North Korea and Russia are using operations that cause denial and manipulation effects to support broader strategic or military objectives.

By definition, offensive cyber operations are distinct from cyber-enabled espionage, in which the goal is to gather information *without* having an effect. When information gathering is a primary objective, stealth is needed to avoid detection in order to maintain persistent access that allows longer term intelligence gathering.

This definition does classify relatively common events, such as ransomware attacks, website defacements and distributed denial of service (DDoS) attacks, as offensive cyber operations.

Although the 'manipulate, deny, disrupt, degrade or destroy' element of the definition lends itself to segmentation into different levels, further examination shows that segmentation based on the *type* of attack is not particularly useful. Information and communication technology (ICT) infrastructure is inherently interconnected, and even modest disruption can cause relatively drastic second-order effects. Modifying the state of a control system, for example, could lock a person's garage or launch a nuclear missile.

Conversely, seriously destructive attacks, such as data wipers, can have damaging effects on different scales. Compare the damage caused when North Korea infiltrated the Sony Pictures Entertainment network[245] with the damage caused during the Russian-launched NotPetya attack'[246] At Sony Pictures, more than 4,000 computers were wiped and, although that cost US$35 million to investigate and repair, it did not significantly affect the broader Sony corporation[247] and did not directly affect other entities. The NotPetya event also involved data destruction, but it was probably the most damaging cyberattack thus far: US$300 million in damages for FedEx; US$250–300 million for Danish shipper Maersk[248]; more than US$310 million for American pharmaceutical

[243] Director GCHQ, speech at CyberUK18, 12 April 2018, online.

[244] Although individuals and groups can conduct offensive cyber operations, states can harness considerably greater expertise and resources than can small groups, so state behaviour is ultimately more concerning. See JM Porup, 'How hacking team got hacked', *Ars Technica*, 19 April 2017, online; Peter Bright, 'With arrests, HBGary hack saga finally ends', *Ars Technica*, 11 March 2012, online.

[245] Federal Bureau of Investigation, 'Update on Sony investigation', media release, 19 December 2014, online.

[246] 'Statement from the Press Secretary', The White House, 15 February 2018, online.

[247] Tim Hornyak, 'Hack to cost Sony $35 million in IT repairs, *CSO*, 4 February 2014, online.

[248] AP Møller – Maersk A/S, *2017 annual report*, online.

giant Merck; US$387 million for French construction giant Saint-Gobain; and US$150 million for UK chocolate maker Mondelez International. It is possible that flow-on effects from the disruption to the logistics and pharmaceutical industries may have affected the broader global economy.

Table 1 is a selected list of state activities that this paper defines as offensive cyber operations. Those operations are assessed for the scale, seriousness, duration and specificity of their effect.

Ultimately, the seriousness of a cyberattack is based on its ultimate effects or on the effects that it enables. The scale and seriousness of incidents should be based upon measuring the ultimate consequences of an incident and the economic and flow-on effects.

Table 1: State offensive cyber

OPERATION	MANIPULATION, DENIAL, DISRUPTION, DEGRADATION EFFECT			
	Seriousness	**Scale**	**Duration**	**Specific**
NotPetya	High—data destruction	Global. Affected organisations in Europe, US and Asia (Maersk, Merck, Rosneft, Beiersdorf, DHL and others) but also a concentration in Ukraine (banking, nuclear power plant, airports, metro services).	Short-term, with recovery over months to a year.	No
WannaCry	High—data destruction	Global, but primarily in Russia, Ukraine, India and Taiwan, affecting multinationals, critical infrastructure and government.	Short-term, with recovery over months to a year.	No
Sony Pictures Entertainment	High—data destruction	Focused on Sony Pictures Entertainment (<7,600 employees), a subsidiary of Sony Corporation (131,700 employees in 2015)[a]	Short-term, with recovery in months.	Yes
Stuxnet	High—destruction of centrifuges	Focused on Iran's nuclear weapon development programme	<1 year	Yes
Various offensive cyber operations against ISIS by US, Australia,	Varied—some data destruction but also denial and manipulation effects	Focused on Islamic State	Unknown	Yes

UK				
Estonia 2007	Medium—temporary denial of service	Principally Estonian electronic services, affecting many European telcos and US universities	3 weeks	Yes

a Sony Corporation, US Securities and Exchange Commission Form 20-F, FY 2016, online.

CYBER WEAPONS AND ARMS CONTROL

Cyber weapons are often conceived of as 'powerful strategic capabilities with the potential to cause significant death and destruction',[249] and in an increasingly interconnected world it is easy to speculate about catastrophic effects. It is also difficult to categorically rule out even seemingly outlandish offensive cyber scenarios; for example, it seems unlikely that a fleet of self-driving cars could be hacked to cause mass destruction, but it is hard to say with certainty that it is impossible.[250] Although the reality is that offensive cyber operations have never caused a confirmed death, this 'uncertainty of effect' is potentially destabilising, as states may develop responses based on practically impossible worst-case scenarios.

In a Global Commission on the Stability of Cyberspace issue brief, Morgus et al. look at countering the proliferation of offensive cyber capabilities and conclude that limiting the development of cyber weapons through traditional arms control or export control is unlikely to be effective.[251] This paper agrees, and contends that previous arms or export control agreements may succeed where the following three conditions are present:

1. Capability development is limited to states, usually because weapons development is complex and highly industrialised.
2. There is a common interest in limiting proliferation.
3. Verification of compliance is possible.

Perhaps only one of these three conditions—a common interest in limiting proliferation—exists in the world of cyber weapons, although even this is not immediately self-evident.

In the context of international arms control, a limited number of capability developers usually means that only states (and ideally only a small number of states) have the ability to develop weapons of concern, that states have effective means to control proliferation, or both. In cyberspace, however, there are many non-state actors—in the cybersecurity industry and in the

[249] Robert E Schmidle Jr, Michael Sulmeyer, Ben Buchanan, 'Nonlethal weapons and cyber capabilities', in George Perkovich, Ariel E Livite (eds), *Understanding cyber conflict: 14 analogies*, Carnegie Endowment for International Peace, 16 October 2017, online.
[250] Jason Kornwitz, 'The cybersecurity risk of self-driving cars', *Phys.org*, 16 February 2017, online.
[251] Robert Morgus, Max Smeets, Trey Herr, *Countering the proliferation of offensive cyber capabilities*, issue brief 1, Global Commission on the Stability of Cyberspace, 22 December 2017, online.

criminal underworld[252]—developing significant cyber capability. Additionally, the exchange of purely digital goods is relatively difficult for states to control compared to exchanges of physical goods. States do not have a monopoly on capability development and find it difficult to effectively control the spread of digital goods, and so therefore cannot credibly limit broader capability development.

For chemical, biological and nuclear weapons, the human suffering caused by their use is generally abhorred and there is a very broad interest in restraining the use of those weapons. Offensive cyber operations, by contrast, could achieve military objectives without causing human suffering; for example, the warfighting capability of an adversary could be degraded by disrupting their logistics such that military objectives could be achieved without fighting. It has been suggested that states have a 'duty to hack' when the application of offensive cyber operations will result in less harm than all other applications of force,[253] and the UK's Minister of State for the Armed Forces, Nick Harvey, noted in 2012 that offensive cyber operations could be 'quite a civilised option' for that reason.[254]

Additionally, cyber weapons can be developed entirely in environments where visibility for verification is impossible, such as in air-gapped networks in nondescript office buildings. Unlike for weapons of mass destruction, there are no factories or supply chains that can be examined to determine whether capabilities exist and stockpiles are being generated.[255]

Unlike many military capabilities—say, nuclear-armed submarines or ballistic missiles—offensive cyber capabilities are unique in that once defenders have technical knowledge of the potential attack, effective countermeasures can be developed and deployed relatively easily.[256]

For this reason, states already have considerable interest in limiting the proliferation of offensive cyber capabilities—they want to keep those capabilities secret so they can exploit them. The US Vulnerabilities Equities Process (VEP) policy document[257] states that when the US Government discovers vulnerabilities[258] most are disclosed, but some will be kept secret to satisfy law enforcement or national intelligence purposes where the risk of the vulnerability is judged to be outweighed by possible intelligence or other benefits. Undoubtedly, all states that engage in

[252] Lillian Ablon, Martin C Libicki, Andrea A Golay, *Markets for cybercrime tools and stolen data: hackers' bazaar*, RAND Corporation, Santa Monica, California, 2014, online.

[253] Duncan B Hollis, 'Re-thinking the boundaries of law in cyberspace: a duty to hack?', Temple University Legal Studies research paper no. 2014-16, in J Ohlin et al. (eds), *Cyberwar: law and ethics for virtual conflicts*, Oxford University Press, 2014, online.

[254] 'New forms of warfare: cyber, UAVs and emerging threats: Q&A', Fourth Plenary Session, IISS Shangri-La Dialogue 2012, online.

[255] Aggressive counter-intelligence operations might illuminate the development of cyber weapons, but those operations are likely to be so valuable to intelligence agencies that they would not be compromised for the sake of arms control.

[256] Cyber defence via patching can be quick and decisive, and a key strategy for defending against malware is patching software vulnerabilities.

[257] Vulnerabilities equities policy and process for the United States Government, charter, The White House, November 2017, online.

[258] Software vulnerabilities are often 'exploited' to achieve unauthorised access and control of computer systems. Vulnerabilities and associated exploits are often a key enabler of offensive cyber capabilities.

vulnerability discovery will have a common interest in keeping at least some secret so that they can be exploited for national security purposes.

DEFINING CYBER WEAPONS

Despite scepticism about the effectiveness of traditional arms control, this paper develops both a narrow and a broad definition of cyber weapons to test whether those definitions could be useful in arms control discussions. The definitions have been developed by examining selected international weapons conventions and previously published definitions.

One problem with defining cyber weapons is that cyber technologies are primarily dual-use: they can be used for both attack and defence, for peaceful and aggressive purposes, for legal and illegal activities. Software can also be quite modular, such that many cybersecurity or administrative tools can be brought together to form malware.

Weapons in the physical domain have been categorised into three groups: small arms and light weapons; conventional arms; and weapons of mass destruction (WMD).[259] Given that cyber weapons are often conceived of as potentially causing mass destruction and because WMDs are subject to the most rigorous international counter-proliferation regimes, this paper examines definitions through the perspective of the dual-use WMD counter-proliferation Chemical Weapons Convention and Biological Weapons Convention.[260]

Biological weapons, a class of WMD, are described as (our emphasis):[261]

1. microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have *no justification for prophylactic, protective or other peaceful purposes*;
2. weapons, equipment or means of delivery designed *to use* such agents or toxins *for hostile purposes or in armed conflict.*

The Chemical Weapons Convention defines chemical weapons as (our emphasis):[262]

(a) toxic chemicals and their precursors, *except where intended for purposes not prohibited* under the Convention and as long as the types and quantities are consistent with such purposes; and

(b) munitions and devices, specifically designed to *cause death or other harm* through the toxic properties of those chemicals …

[259] UN Office for Disarmament Affairs, *Nuclear weapons*, online.

[260] We exclude nuclear weapons here, since neither the Non-Proliferation Treaty nor the IAEA properly define 'nuclear weapon' and because nuclear technology was first and foremost developed for weapons purposes. Civilian applications came later. See Steven E Miller, 'Cyber threats, nuclear analogies? Divergent trajectories in adapting to new dual-use technologies', in George Perkovich, Ariel E Levite (eds), *Understanding cyber conflict: 14 analogies*, Carnegie Endowment for International Peace, November 2017 online.

[261] Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, Article 1, online.

[262] Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, article ii, online.

These conventions, both of which deal with dual-use goods, define by exclusion: only substances that do not or cannot have peaceful purposes are defined as weapons. The material of concern is not inherently a problem—it is how it is used.

In the context of armed conflict, the *Tallinn Manual* characterises cyber weapons by the effects they have, not by how they are constructed or their means of operation:

> cyber weapons are cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack.[263]

Herr and Rosenzweig define cyber weapons as malware that has a destructive digital or physical effect, and exclude malware used for espionage.[264] Herr also considers that malware is modular and consists of a propagation element that the malware uses to move from origin to target; an exploit that will allow the malware to execute arbitrary commands on the target system; and a payload that will execute some malicious instructions.

Rid and McBurney define cyberweapons as 'computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings'.[265]

A NARROW DEFINITION

Following the logic of dual-use weapons conventions, a narrow definition of cyber weapons is *software and information technology (IT) systems that, through ICT networks, cause destructive effects and have no other possible uses*. The IT system aspect of this definition requires some level of integration and automation in a weapon: code that wipes a computer hard disk is not a weapon by itself—by itself it cannot achieve destructive effects through cyberspace—but could form part of a weapon that wipes hard drives across an entire organisation.

Based on this narrow definition, Table 2 shows our assessment of whether reported malware examples would be defined as cyber weapons.

Table 2: Cyber weapon assessment

MALWARE OR SYSTEM	DESCRIPTION	WEAPON
Distributed denial of service (DDoS) systems	Aggregation of components, including bots and control software, such that they have no	Yes, although this is arguable because effects tend to be temporary (disruptive and not

[263] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, supra note 2, at Rule 103, Commentary, p. 452.
[264] Trey Herr, Paul Rosenzweig, 'Cyber weapons and export control: incorporating dual use with the PrEP model', *Journal of National Security Law and Policy*, 25 September 2014, 8(2), online.
[265] Thomas Rid, Peter McBurney, 'Cyber-weapons', *The RUSI Journal*, 157(1):6–13, online.

	other purpose than to disrupt internet services.	destructive). Each individual component is likely to have non-destructive uses.
Dragonfly a.k.a. Energetic Bear campaign[a]	Espionage campaign against energy critical infrastructure operators that developed industrial control system sabotage capabilities.	No. This was both manual and for espionage only; it never disrupted critical operations. However, the intent demonstrated is to develop capabilities to disrupt critical infrastructure.
Blackenergy 2015 Ukrainian energy grid attack[b]	Access to Ukrainian energy company was used to disrupt electricity supply.	No. Blackenergy malware was very modular and this attack was quite manual. This malware does contain destructive capability.
Industroyer a.k.a. Crashoverride malware[c]	Malware in a Ukrainian energy supply company was used to disrupt electricity supply.	Yes. Integrated malware disrupted electricity supply automatically.
TRISIS malware[d]	Malware intended to sabotage a Saudi Arabian petrochemical plant.	Yes. Malware with no espionage capability was specifically designed to destroy a petrochemical plant.
WannaCry	A self-propagating data wiper.	Yes. Malware with no espionage capability was designed to irreversibly encrypt computer hard drives.
Metasploit	An integrated collection of hacking tools that can be used for defence, for espionage, or for destruction and manipulation.	No. Metasploit has many non-destructive uses and is not integrated into a system that causes destruction.
NotPetya	A self-propagating data wiper.	Yes. Automatically destroyed data.
Flame, Snake, Regin	Very advanced modular malware.	No. These could cause denial and manipulation effects and could be automated but have other uses. They seem to be designed primarily for espionage.
Stuxnet	Self-propagating malware that subverted industrial control systems to destroy Iranian nuclear	Yes. Highly tailored to automatically destroy targeted

	fuel enrichment centrifuges.	centrifuges.
Large-scale man-in-the-middle attack system (e.g. mass compromise of routers)[e]	Compromise of many mid-points could enable large-scale access that could be used to enable intelligence, destruction or manipulation, or even to patch systems.	No. Intent is everything here.
Powershell	A powerful scripting and computer administration language installed by default with the Windows operating system.	No. Many non-destructive uses.
A Powershell script designed to automatically move through a network and wipe computers.	Destructive intent is codified within the script commands.	Yes.

a Symantec, *Dragonfly: Western energy companies under sabotage threat*, 2014, online.

b Kim Zetter, 'Inside the cunning, unprecedented hack of Ukraine's power grid', *Wired*, 3 March 2016, online.

c Andy Greenburg, '"Crash override": the malware that took down a power grid', *Wired*, 12 June 2017, online; Robert M Lee, 'Crashoverride', *Dragos*, 12 June 2017, online; Anton Cherepanov, Robert Lipovsky, 'Industroyer: biggest threat to industrial control systems since Stuxnet', *welivesecurity*, 12 June 2017, online.

d Nicole Perlroth, Clifford Krauss, 'A cyberattack in Saudi Arabia had a deadly goal: experts fear another try', *New York Times*, 15 March 2018, online; *TRISIS malware: analysis of safety system targeted malware*, Dragos, online.

e US CERT, *Russian state-sponsored cyber actors targeting network infrastructure devices*, Alert TA18-106A, 16 April 2018, online.

This narrow definition is consistent with the narrowness of definitions from both the Biological Weapons Convention and the Chemical Weapons Convention, both of which deal with dual-use goods.

The definition captures intent by excluding all other tools where intent is ambiguous; only tools that can only be used for destruction are included.

This narrow definition is problematic for at three reasons.

First, it does not map directly onto state definitions of offensive cyber activities—actions that manipulate, disrupt, deny and degrade would likely not be captured and so much offensive cyber activity will not involve cyber weapons. The offensive cyber operation, for example, that US Cyber Command conducted against Islamic State's propaganda operations did not require cyber weapons. Cyber Command obtained Islamic State administrator passwords and deleted content and changed passwords to lock out the original owners.[266] This offensive cyber operation could have been entirely conducted using standard computer administration tools. No malware, no exploit, no software vulnerability and certainly no cyber weapon was needed.

Second, even the most destructive offensive cyber operations could be executed without ever using a cyber weapon. For example, a cyber operation that triggered the launch of conventional or nuclear weapons would not require a cyber weapon.

Third, this definition could easily be gamed by adding non-destructive functionality to otherwise malicious code.

A BROADER DEFINITION

A broader definition of cyber weapons could be *software and IT systems that, through ICT networks, manipulate, deny, disrupt, degrade or destroy targeted information systems or networks.*

This definition has the advantage that it would capture the entirety of tools that could be used for offensive cyber operations.

Many cyber operations techniques, however, take advantage of computer administration tools, and the difference between espionage and offensive action is essentially a difference in intent; for example, the difference between issuing a command to copy files and issuing one to delete files. Indeed, it is possible to conduct cyber operations—both intelligence and offensive operations—using only legitimate tools such as the scripting language Windows Powershell.[267] Yet it makes no sense to define what *could* be used for destructive effects as a cyber weapon; it is nonsensical to label Powershell as a cyber weapon.

This definition would also include perfectly legitimate tools that state authorities and the cybersecurity community use for law enforcement, cyber defence, or both.

These two definitions highlight the dilemma involved in defining cyber weapons. A narrow definition can perhaps be more readily agreed to by states, but excludes so much potential offensive cyber activity that efforts to limit cyber weapons based on that definition seem pointless. The broader definition would capture tools used for so many legitimate purposes that agreement on their status as weapons is unlikely, and limitations could well harm network defenders more than attackers.

[266] Ellen Nakashima, 'US military cyber operation to attack ISIS last year sparked heated debate over alerting allies', *The Washington Post*, 9 May 2017.

[267] Powershell is a powerful scripting language used for many standard computer administration tasks that is installed by default on Windows computers. See Symantec, *Increased use of Powershell in attacks*, online.

OPTIONS FOR CONTROL

This paper therefore agrees with Morgus et al.[268] that limiting the development of cyber weapons by controlling the development of defined classes of weapons is unlikely to be effective. There are, however, options for more effective responses that focus on affecting the economics of offensive cyber operations and the norms surrounding their application.

Affecting the markets involved in offensive cyber capability development would raise the cost of capability development and encourage states to conduct operations sparingly.

One market associated with cyber capabilities is that for software vulnerabilities and their associated exploits (code that takes advantage of a vulnerability). Software vulnerabilities are often exploited by malware to gain unauthorised access to computer systems and are often—although not always—required for offensive cyber capabilities. Ablon and Bogart have found that the market price for software exploits is sensitive to supply and that prices can rise dramatically for in-demand, low-supply products.[269] A multifaceted approach to restricting supply could raise the cost of acquiring exploits and therefore the cost of building offensive cyber capabilities.

Shifting the balance of vulnerability discovery towards patching (rather than exploitation for malicious purposes) would raise the value of all vulnerabilities. As suggested by Morgus et al., one possibility is that software vulnerabilities are bought for the express purpose of developing fixes and patches, as suggested by Dan Geer in a 2014 BlackHat conference keynote.[270]

A secondary response would be to enable more effective repair of vulnerabilities that would close the loopholes that enable computer exploitation. NotPetya, assessed by the US Government to be the most destructive cyberattack thus far,[271] used publicly known vulnerabilities for which patches had been available for months. Effective cyber hygiene would have prevented much of the damage that NotPetya caused.

From a policy point of view, this could be attacked at several levels by encouraging research into vulnerability mitigation and more effective patching processes; educating decision-makers to prioritise and resource vulnerability discovery and patching; government policy to encourage more effective patching regimes; and promoting VEP policies in other states (discussed below).

Whenever a vulnerability is exploited for any purpose—including cyber espionage, offensive operations and cybercrime—there is a risk of discovery, which could ultimately result in patching and loss of the ability to exploit the vulnerability. Raising the value of all vulnerabilities will encourage states to use offensive cyber capabilities sparingly to avoid discovery and hence loss of capability via patching.

A complementary approach would be to change incentives within software development to encourage secure application development. Again, this could be approached at many levels:

[268] Robert Morgus, Max Smeets, Trey Herr, *Countering the proliferation of offensive cyber capabilities*, issue brief 1, Global Commission on the Stability of Cyberspace, 22 December 2017, online.

[269] Lillian Ablon, Andy Bogart, *Zero days, thousands of nights*, RAND Corporation, Santa Monica, California, 2017, online.

[270] Dan Geer, BlackHat conference keynote, 2014, online.

[271] 'Statement from the Press Secretary', The White House, 15 February 2018, online.

altering computer science curriculums; promulgating secure coding standards;[272] and altering the balance of liability in commercial code, for example.

Reducing the supply of exploits and raising their cost encourages states to conduct cyber operations in a way that avoids attracting attention to mitigate the risk of discovery and loss of capability. This effort to operate quietly would vastly reduce the risk of inadvertent large-scale damaging events.[273]

RECOMMENDATION: ENCOURAGE THE ESTABLISHMENT OF NATIONAL VULNERABILITIES EQUITIES PROCESSES

There is a common interest among all states that are conducting cyber operations—defensive or offensive—in actively assessing the risk and benefits of keeping vulnerabilities secret for exploitation. The US VEP document states that in 'the vast majority of cases, responsibly disclosing a newly discovered vulnerability is clearly in the national interest'. Assuming this is true, the presence of VEP policies in many states would tend to result in more responsible disclosure and patching and therefore result in a reduced supply of vulnerabilities and exploits.

This reduced supply of vulnerabilities would raise the cost of offensive capability development and therefore restrict proliferation and reduce the use of offensive operations.

RECOMMENDATION: PROMOTE FOCUSED OPERATIONS

Unlike a kinetic weapon, for which direct consequences such as blast radius may be well understood, offensive cyber operations can easily have unintended consequences. Since states are conducting offensive cyber operations below the threshold of armed conflict, another option to limit offensive operations is to promote operations that are tightly focused so that operations do not affect innocent bystanders.

We have assessed that both the Sony Pictures and Stuxnet attacks were specific, as both affected specific targets and did not cause direct effects elsewhere (Table 1). The NotPetya and WannaCry incidents were not specific: they affected many organisations world-wide.

It is possible, therefore, to conduct focused offensive cyber operations that are specific and limit collateral damage; it is not an inherent fact of cyberspace that operations cannot be targeted and specific. To reduce the risks of collateral damage, there would be merit in promoting a norm of 'due diligence' for offensive cyber operations, requiring that states invest in rigorous testing to ensure that effects are contained before engaging in offensive cyber operations.

[272] See Microsoft's Security Development Lifecycle as an example, online.

[273] Although rising prices for exploits encourage researchers to search for them, the history of rising prices in the market for IOS (Apple's iPhone operating system) exploits indicates that robustly patching vulnerabilities can affect the value of exploits.

MEASURING DAMAGE FOR MORE EFFECTIVE RESPONSES

In addition to altering the computer vulnerability lifecycle, governments should also respond directly to cyber operations. Effective responses should be both directed against perpetrators and proportionate. Currently, both the identification of perpetrators (attribution) and the assessment of damage (to determine a proportionate response) are suboptimal. Much has been said about attribution, and this paper will not cover it further.

When state-sponsored operations such as NotPetya and WannaCry occur, there is no independent assessment of damage. An accurate accounting of harm could be used to justify an appropriately proportionate response.

NotPetya has been called 'the most destructive and costly cyber-attack in history'.[274] It seems that total cost estimates of over US$1 billion are based on collating the financial reports of public companies such as Merck,[275] Maersk,[276] Mondelez International[277] and FedEx,[278] and then adding a 'fudge factor' to account for all other affected entities. Publicly listed companies have formal reporting obligations, but the vast majority of entities affected by NotPetya do not, and it seems likely that the cost of NotPetya has been significantly understated.

An independent body that identifies common standards, rules and procedures for assessing the cost of cyberattacks could enable a more accurate measure of damage. The International Civil Aviation Organization's system for air crash investigations may provide a framework.[279] It assigns a role for various stakeholders, including the airline, the manufacturer, the registrar and so on. The investigation is assigned to an autonomous safety board with the task of assessing what happened, not who was at fault.[280] For a cyber incident, an investigation board could include a national cybersecurity centre, the affected entity, the manufacturer of the affected IT system, relevant software developers and other stakeholders.

Using assessments of scope and seriousness to develop proportionate responses would encourage attackers to construct focused and proportionate offensive cyber operations.

[274] 'Statement from the Press Secretary', The White House, 15 February 2018.

[275] Merck, 8-K filing, October 2017, online.

[276] Maersk, *2017 annual report*, online.

[277] Mondelez International, 'Mondelez International reports 2017 results', media release, 31 January 2018, online.

[278] FedEx, 'FedEx Corp reports first quarter earnings: cyberattack lowers results', media release, 19 September 2017, online.

[279] International Civil Aviation Organization, *Annex 13—Aircraft accident and incident investigation.*

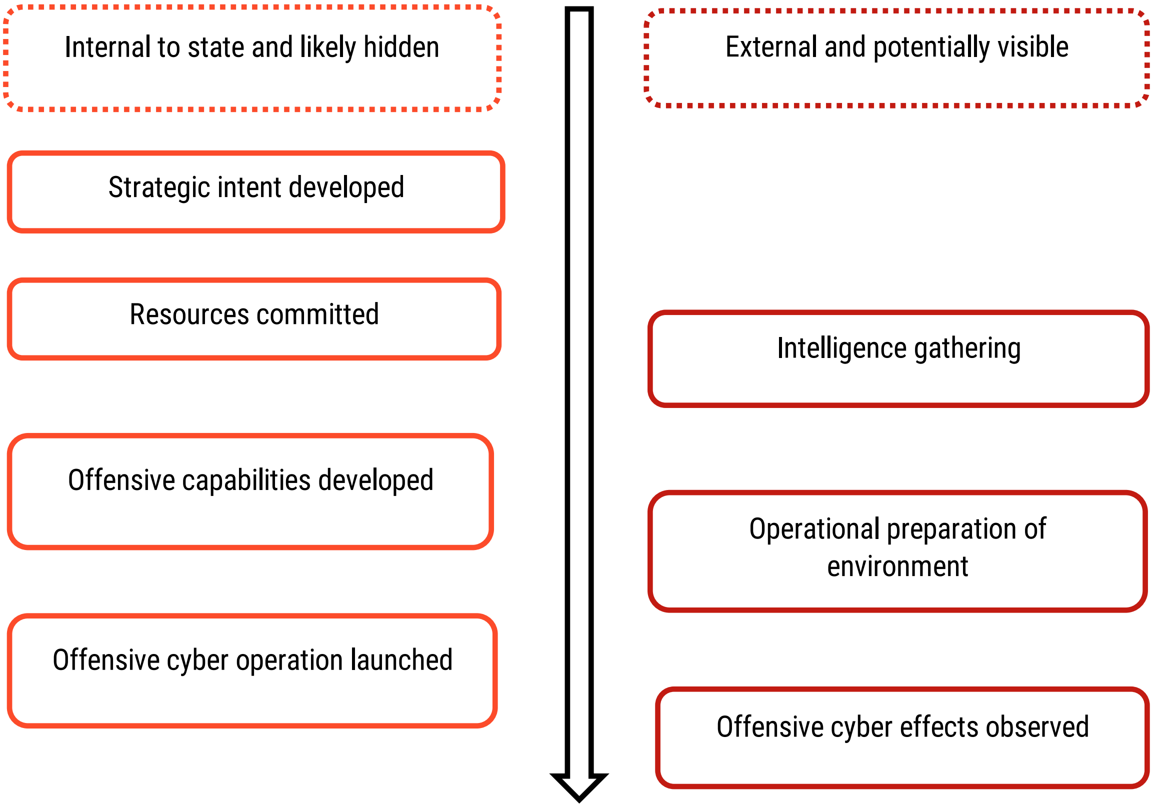
[280] A body analogous to the International Civil Aviation Organization could adopt standards and recommend practices concerning the assessment of damage after cyber incidents. Those assessments could occur in phases: a two-week quick assessment of scale and seriousness; a more in-depth one-month assessment that places firmer ranges on the scope of damage; and a three- or six-month assessment that uses agreed upon accounting methods to more rigorously quantify both scope and cost. An initial assessment of scope might range from local (affecting a single company or a single geographical region), sectoral (affecting a sector of a single national economy), national (affecting an entire country) to global (affecting the world).

RECOMMENDATION: INVEST IN TRANSPARENCY AND CONFIDENCE BUILDING

We have noted above that uncertainty about the effects caused by offensive cyber operations has the potential to be destabilising. State transparency in the use of offensive cyber operations could address this concern and help promote norms of responsible state behaviour.

Figure 1 shows the lifecycle of an offensive cyber capability, starting at the point that a state forms an intent to develop capability. Resources are committed; intelligence is gathered to support capability development; capability is developed; the environment is prepared (by deploying malware, for example); and finally the operation is launched and effects are observed. Crucially, there are distinct elements during this lifecycle that require operation on the public internet and are therefore potentially observable: intelligence gathering, operational preparation of the environment, and offensive cyber effects (in orange).[281]

Figure 1: Offensive cyber capability lifecycle


Internal to state and likely hidden
External and potentially visible
Strategic intent developed
Resources committed
Intelligence gathering
Offensive capabilities developed
Operational preparation of environment
Offensive cyber operation launched
Offensive cyber effects observed

Although it is not possible to see or measure cyber weapons, to quantify them or inspect 'cyber weapon factories', a level of confidence-building transparency can still be achieved. Public doctrine that defines a nation's strategic intent and its assessment of acceptable and responsible uses of offensive cyber operations would be extremely helpful.

[281] Other intelligence efforts could shed light on the hidden elements in this lifecycle but are beyond the scope of this paper. Also, strategic intent may also be visible.

This visibility may be sufficient to enhance confidence building as predictability is increased. Many responsible states will be reluctant to deviate from public statements regarding offensive cyber capability development because effects will possibly become visible at a later stage that will prompt incident response, forensic analysis and maybe political attribution and embarrassment.

There is already some public documentation of offensive cyber capabilities. There are unclassified doctrines, official statements and unofficial reporting on the states that have—or are developing—offensive capability. There are also voluntary national reports in the context of the UNGGE. Additionally, open source verification by research institutes such as the SIPRI Yearbook, IISS Military Balance and reports similar to the Small Arms Survey are authoritative and credible sources that inform policy actions by states. Finally, independent analysis and reporting from cybersecurity companies such as Symantec, Crowdstrike, BAE Systems, FireEye and Kaspersky Lab provides invaluable technical information. These firms also play a key role in early detection and response.

SUMMARY AND CONCLUSION

Offensive cyber capabilities are defined as **operations in cyberspace to manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems or networks**.

This paper has examined narrow and broad definitions of cyber weapons and found them problematic for use in control discussions.

However, a range of other measures would help limit the use of offensive cyber capabilities and reduce the risk of collateral damage when they are used:

- Markets for the vulnerabilities that are used to create offensive cyber capabilities can be affected to make capability development more expensive. VEP processes would form one element of a broader effort to patch vulnerabilities and restrict supply.
- Promoting the principle that offensive cyber operations should be focused and taking active steps to limit unintended consequences could limit the effects of operations on innocent bystanders, including through the promotion of the concept of 'due diligence'.
- Responses to cyber incidents could also be improved by better accounting of the damage incurred. A robust assessment of damage using agreed standards would enable a more directly proportionate response and would help reinforce the expectation of specific and proportionate offensive cyber operations.
- Finally, increased state transparency would promote acceptable norms of behaviour. Although monitoring and verification are difficult, this paper presents an offensive cyber operation lifecycle that indicates that various stages provide some visibility, which could build confidence.

ACRONYMS AND ABBREVIATIONS

DDoS	distributed denial of service
ICT	information and communication technology
IT	information technology
UNGGE	United Nations Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security
VEP	vulnerabilities equities process
WMD	weapon of mass destruction

MEMO 4
DEFINING OFFENSIVE CYBER CAPABILITIES

Dragan Mladenović, DiploFoundation

Vladimir Radunović, Director, E-diplomacy and Cybersecurity, DiploFoundation

MEMO №4

1 INTRODUCTION, PROBLEMS AND METHODOLOGY

The purpose of international conflicts is always a violent realization of interests of nations. The nature, means, methods, and technology of conflicts have evolved during history becoming more efficient by nature and at the same time more complicated for regulation. Isaac Asimov, nearly thirty years ago, almost prophesied: „The saddest aspect of life right now is that science gathers knowledge faster than society gathers wisdom“[282]. The use of ICTs and offensive cyber capabilities (OCC) as means and method for projection of national power in international relations today has got the potential to seriously threaten international peace and stability.

Since 1998, when the Russian Federation proposed putting regulation of information and ICT use in the context of international security in the official agenda until today, the leading military forces of the world have been fast at developing their capabilities for cyber conflict, while international community failed to regulate this field in accordance with the declared goals of the UN Charter.[283] The development of OCC is becoming faster and uneven, and its effects increasingly serious.

Expressions like "offensive cyber abilities", "cyber weapons" and "cyber attack" are often used in the contemporary international practice in the context of serious disagreements and political conflict. Their meaning, content and consequences are rapidly evolving with advances in technology. The absence of a unified position on the nature, character and content of these phenomena complicates international communication, regulation and resolution of crisis situations.

The basic step in legal implementation and international regulation of the OCC is to establish a common understanding of what they are. It should be kept in mind that the absence of consent does not only influence international peace and stability, but also the application of general human rights standards.

This paper seeks to provide a contribution to a clear understanding of nature and character of OCC. The basic motto in achieving this goal, in order to avoid the danger of media and political bias, will be in line with the idea that “books must follow sciences, and not sciences books”[284].

2 WHAT ARE OCCS, WHO USES THEM AND HOW?

The following lines will discuss what constitutes the nature of OCC in social, political, military, security, technology, and international law context. The appropriate definitions from official government documents, as well as the existing academic and professional knowledge base, will serve as the foundation of the discussion.

2.1 THE ENVIRONMENT IN WHICH THE OCCS ARE USED

States have different views on what is the environment for the OCC. According to one model, represented by Russia, the domain refers to a unified set of all information related to national

[282] Asimov, Isaac, and Jason A. Shulman, eds. *Isaac Asimov's book of science and nature quotations*. Weidenfeld & Nicolson, 1988., p. 281.

[283] UN Charter, Preamble.

[284] Francis Bacon, "Proposition Touching Amendment of Laws." in *The Works of Francis Bacon* 13: 1857-74.

security[285], an **information sphere,** which is defined as "a combination of information, informatization objects, information systems, .. , networks, .. , entities, ..., mechanisms regulating public relations in the sphere."[286]

The focus of the other approach, led by the U.S., is directed towards a specific environment created by the operation and interaction of (digital) technical systems and infrastructures - cyberspace**.** According to the U.S. Department of Defense (U.S. DoD), cyberspace is "the global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[287]

The Organization of United Nations (OUN) took a functional approach to defining this environment by establishing, in 2004, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), which officially uses the expression „field of information and telecommunications", which preserves the sense and meaning of both previous approaches.[288]

Various public authorities, professional, and academic institutions use different definitions, the analysis of which can point to the following trends:

- the functional approach is becoming more represented than the formal one;
- the meaning of the area is changing along with the possibilities of ICT use;
- the application of specific technical rather than abstract concepts (such as "virtual domain") is increasing[289,290];
- cyberspace is less and less regarded as „Internet"[291,292], and increasingly as an „environment" and „operational domain" with specific purpose and application;[293,294,295,296,297]

[285] Russian: "информационная безопасность", (pronunciation 'informatsionnaya bezopasnost').

[286] Doctrine of Information Security of the Russian Federation, Approved by Decree of the President of the Russian Federation No. 646 of December 5, 2016.

[287] US DoD. *Joint Publication JP 3-12 (R), Cyberspace Operations*. (2013), http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf .

[288] UN General Assembly, Resolution 58/32 adopted by the General Assembly on 8 December 2003, Developments in the field of information and telecommunications in the context of international security, A/RES/58/32 of 18 December 2003. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/58/32.

[289] Austria, Bundeskanzleramt Osterreich, Austrian Cyber Security Strategy, (2013), 21. http://archiv.bundeskanzleramt.at/DocView.axd?CobId=50999.

[290] *Oxford English Dictionary, s.v.* „weapon". http://www.oed.com.nduezproxy.idm.oclc.org/view/Entry/240849?redirectedFrom=cyberspace#eid.

[291] FR Germany. Federal Ministry of the Interior. *Cyber Security Strategy for Germany* (February 2011), 9. http://www.oed.com.nduezproxy.idm.oclc.org/view/Entry/240849?redirectedFrom=cyberspace#eid.

[292] United Kingdom, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, (United Kingdom, UK Cabinet Office, 2011), p. 11. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

[293] Michael N. Schmitt, ed. *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press, (2017), 258. https://www.ccdcoe.org/strategies-policies.html.

- data and information[298] in cyberspace are of ICT, digital, and electromagnetic nature;[299, 300, 301, 302, 303, 304]
- cyberspace is considered a subset of a wider information domain;
- cyberspace is a set of information, systems, infrastructures and entities which make up information-related assets;
- the existence of cyberspace is functionally based on interaction of entities and assets through processes and services, by networking[305, 306, 307]with data;[308, 309, 310, 311, 312]
- data-related processes (creation, storage, processing, transmission, destruction) in cyberspace are highly automated by ICT systems.

[294] Presidency of the Council of Ministers, Government of Italy, *National Strategic Framework for Cyberspace Security* (2013), 9. https://www.ccdcoe.org/strategies-policies.html.
[295] Japan, Government of Japan, *National Security Strategy* (2013), 9. http://www.cas.go.jp/jp/siryou/.
[296] Austria, Austrian Cyber Security Strategy.
[297] Switzerland, Federal Department of Defence, Civil Protection and Sport DDPS, *National strategy for the protection of Switzerland against cyber risks* (2012), 5. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf.
[298] Data is a set of values of qualitative or quantitative variables. Information is data in context; data which are processed, organized, interpreted, structured or presented in a given context, which make it useful, and with an information value; a sequence of symbols that can be interpreted as a message, and which provides knowledge or insight about a certain matter.
[299] Schmitt, *Tallinn Manual 2.0,* p. 258.
[300] James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko, eds., *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2* (New York, NY: The EastWest Institute, 2014), p. 22.
[301] JP 3-12 (R), p. V.
[302] Совет Федерации, Федералыного Собрания Российской Федерации, *Концепция стратегии кибербезопасности Российской Федерации - Проект*, (10 января 2014), 2, http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf.
[303] France, Agence Nationale de la Securite des Systemes d'Information, *Information Systems Defence and Security: France's Strategy* (2011). https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf. Note: the 2015 strategy does not contain the definition of cyberspace.
[304] Finland, Ministry of Defence, Secretariat of the Security and Defence Committee, *Finland's Cyber Security Strategy* (2013), 12. http://www.enisa.europa.eu/media/news-items/new-cyber-security-strategies-of-austria-finland-worldwide.
[305] Netherlands, Ministry of Defence, *The Defence Cyber Strategy* (2012), p. 4. http://www.ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf.
[306] Canada, Government of Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (2010), 2. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx.
[307] FR Germany. Federal Ministry of the Interior. *Cyber Security Strategy for Germany* (February 2011), 12. http://www.oed.com.nduezproxy.idm.oclc.org/view/Entry/240849?redirectedFrom=cyberspace#eid.
[308] International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 27032:2012, Information technology — Security techniques — Guidelines for cybersecurity* (Geneva, Switzerland: ISO/IEC, 2012).
[309] ITU, *ITU Terms and Definitions*.
[310] Совет Федерации, Федералыного Собрания Российской Федерации, p. 2.
[311] France, Agence Nationale de la Securite des Systemes d'Information.
[312] India, *National Cyber Security Policy* (2013), p. 1. http://deity.gov.in/content/national-cyber-security-policy-2013-1.

The practical impact of how cyberspace is defined on the OCC phenomenon is visible from the structure of cyberspace as defined by the U.S. DoD[313], according to which cyberspace consists of three layers: physical network layer, logical network layer, and cyber-persona layer.[314]

A similar approach is taken by the United Kingdom Ministry of Defence (UK MoD) which defines cyberspace as: "An operating environment consisting of the interdependent network of digital technology infrastructures (including platforms, the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein spanning the **physical**, **virtual** and **cognitive** domains."[315]

The said layers should not be viewed as separate domains, but conceptually linked together[316]. For easier understanding in further analysis, these conceptual layers will be called: physical, logical, and cognitive.

2.2 THE ORIGIN, DEFINITIONS AND APPLICATION OF OFFENSIVE CYBER CAPABILITIES

Understanding of OCC, cyber weapons and attacks lays in their interdisciplinary nature, contents and characteristics. The official attitudes of states, the linguistic-semantic meaning of terms, the level of knowledge of academic and professional community and the provisions of international law are of importance.

2.2.1 MILITARY LINGUISTIC PERCEPTION

The term "offensive cyber capabilities" primarily belongs to the military-security field of activity. It is necessary to keep in mind that the internal process of defining military terms is based on different principles[317], standards, rules, practices, capacities and needs of specific armies.

General military dictionaries define the term (noun) "offense/offence"[318] as "an aggressive military action",[319] a process of moving forward (towards the enemy), with an excellent counterpart in

[313] JP 3-12 (R), p. 4..

[314] JP 3-12 (R), p. I-3.

[315] United Kingdom Ministry of Defence, Development, Concepts and Doctrine Centre. Cyber Primer, Second Edition, 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf.

[316] For example, a data or data set that is automatically manipulated using computer-information systems simultaneously exists in the form of signal or record in the physical environment (such as a magnetic or mechanical record, an electron or photon flow, an electromagnetic or sound wave), at the same time having a logical value as part of an algorithm, and information-cognitive value for the entity to which it is represented in the appropriate context.

[317] The three fundamental principles used in the U.S. Department of Defense (DoD) Terminology Program for making US DoD dictionaries are: clarity, conciseness, and completeness. Katsos, G. (January 10, 2018). *Department of Defense Terminology Program*. Joint Force Quarterly, No.88. http://ndupress.ndu.edu/Media/News/News-Article-View/Article/1413093/department-of-defense-terminology-program/.

[318] US spelling of offence (British English word).

[319] *Offence*. Bowyer, R. (2015). *Dictionary of Military Terms: Over 6,000 words clearly defined*. Bloomsbury Publishing. p. 171.

Russian for offensive “наступательный”,[320] while the adjective “offensive” is defined as “relating to aggressive military action”.[321]

In specialized military dictionaries, "offense" is considered a form of an active operation or action involving a contact with an adversary, which aims to impose one's advantage over the adversary intended to:

a) achieve **movement to contact,** an offensive manoeuvre designed to develop the situation and to establish contact with adversary;[322]

b) achieve **power projection** and cause effects by:

   - use of force, operation to destroy or neutralize enemy asset or system[323];
   - useing an active and offensive set of measures such as deceive, disrupt, degrade, deny, or destroy adversary capabilities[324]
   - using a **feint,** a form of military deception conducted for the purpose of deceiving the adversary as to the location and/or time of the actual main offensive action;[325]

c) use **exploitation** as „an offensive operation that usually follows a successful attack and is designed to disorganize the enemy in depth“.[326]

The general semantic meaning of “offensive” signifies a plan, intention, being in a position to undertake an attack or power projection; an activity or process of an attack or manoeuvre in relation to the operation of the object.

2.2.2 POLITICAL PERCEPTION

Offensive operations and activities in cyberspace can be performed by state and non-state entities, whereby states are the main subjects of international law[327], responsible for the use of force in international relations.

[320] U.S. War Department. (January 15, 1945). *Russian Military Dictionary*. War Department Technical Manual (TM 30-544). Washington, D.C., 296.

[321] *Ibid.*

[322] “Movement to contact*”,* US DoD Dictionary, p. 158.

[323] “Offensive counterair”*,* US DoD Dictionary, p. 169.

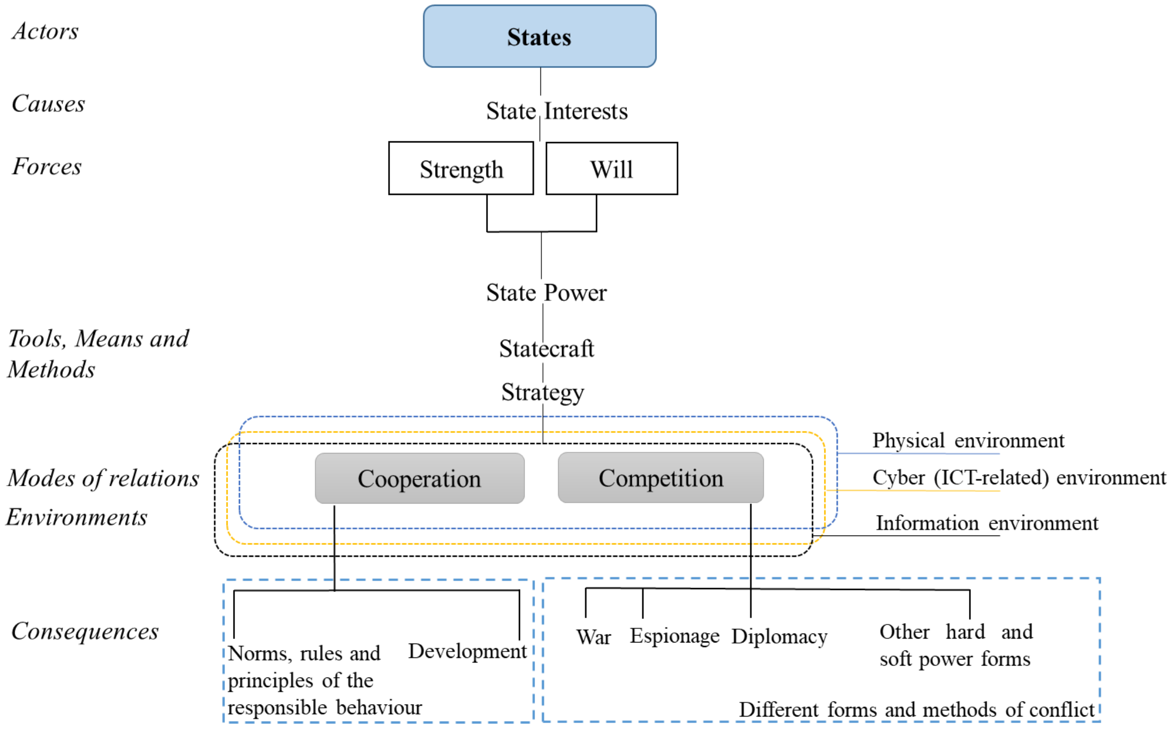
[324] “Negation”, US DoD Dictionary of Military and Associated Terms, As of March 2018. p. 165.

[325] “Feint”, US DoD Dictionary, p. 86.

[326] “Exploitation”, US DoD Dictionary, p. 84.

[327] Jack L. Goldsmith, and Eric A. Posner, *The limits of international law*, (Oxford University Press, 2005).

Figure 1: States' interests and scheme of their application.[328]



Achieving state interests is always defined in terms of power,[329] through cooperation or competition (Figure 1)[330], which means that OCCs can be applied both for competition and international cooperation. OCCs in their objective nature are neither positive nor negative, but are defined as such through their use.

State actors applying OCC are of military and non-military (intelligence, security or police) character. In both cases, the use of force can be armed (by conducting a "fight") or "unarmed" (by execution of supporting and other activities) (Table 1). In relation to state jurisdiction (for example, territorial), OCC application can have an external and internal character, so national and international law systems are applied.

Table 1. Possible modes of conducting OCCs

WAYS OF POWER PROJECTION	**BY ACTORS**	**Military**	**Non-military**
BY MEANS			
Armed		1	3

[328] Adopted from Charles W. Freeman, Jr., *Arts of Power: Statecraft and Diplomacy*, (Washington, DC: United States Institute of Peace, 1997).
[329] Morgenthau, Hans, and Politics Among Nations. "The struggle for power and peace." *Nova York, Alfred Kopf* (1948).
[330] Charles W. Freeman, Jr., *Arts of Power: Statecraft and Diplomacy*.

Non-armed	2	4

In situations of international armed and non-armed conflicts, the institutionalized power and force are always applied, and are often put before the law by states, but this is not and should not be unlimited. Norms, principles, standards and rules of legality, humanity, peaceful coexistence, ways of applying force[331] and preservation of human rights must be respected as civilisation heritage.

2.2.3 MILITARY AND SECURITY PERCEPTION

Analysis of the scope and content, definition of the OCC from doctrinal and tactical documents, and information on the status, organization and tools of military and intelligence agencies and units is not easily conducted. Details about them are classified and largely inaccessible, even when states publicly announce they own OCC. In addition, agencies from different states have different traditions, experiences, missions, resources, internal and external environments, and hence different tasks, doctrines, capabilities, and procedures.

Available military, political and strategic documents allow for some insight into how countries define OCC. A blended definition of OCC, taking into account major (mainly complementary) elements of various available state definitions, may be useful for broadly scoping the variety of views:

Digital means[332], material or immaterial resources[333], such as a device, computer program, or technique (including any combination of software, firmware, or hardware)[334] - as part of the full spectrum of capabilities[335] and total military power [336] -

used or designed to create effect in or through cyberspace[337], influence or deny enemy action[338] in both cyberspace and the physical sphere[339], and/or initiate cyber attack[340] - (only)[341] against military targets[342] -

[331] *Ius ad bellum* and *ius in bello* systems of rules of the LOAC.

[332] Netherlands. Ministry of Defence. *The Defense Cyber Strategy.* (2015). https://zoek.officielebekendmakingen.nl/kst-33321-5.pdf.

[333] Belgium. Defence Strategy Department. *Cyber Security Strategy for Defence.* (2014). https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf.

[334] JP 3-12 (R).

[335] UK Government. National Cyber Security Strategy 2016-2021. (2016.) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

[336] Netherlands. *The Defense Cyber Strategy.*

[337] JP 3-12 (R).

[338] Netherlands. *The Defense Cyber Strategy.*

[339] UK Government. National Cyber Security Strategy 2016-2021.

[340] *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2.*

[341] The Netherlands explicitely states that OCC, within the scope of their Ministry of Defence, can be used only against military targets.

[342] Netherlands. *The Defense Cyber Strategy.*

with the intention to protect network capacity and guarantee confidentiality, integrity and availability, limit or eliminate adversary's capability[343]*, influence information and systems*[344]*, cause damage, disruption or destruction*[345]*, or as cyber deterrence*[346]*,*

by deliberately intruding[347]*, infiltrating, manipulating or disrupting computers, networks, systems* [348]*,*[349] *and weapons and sensory systems*[350]*.*

While this blended definition can possibly serve as basis for further dialogue on a common definition, it can primarily help better mutual understanding of what is understood as OCC by various parties.

It is certain that the number of countries with OCC is growing, as are the related national resources.[351,352,353] A number of states publicly signal the existence of OCC within their official documents: Australia,[354] Austria,[355] Belgium,[356] Brazil,[357] Canada,[358] Denmark,[359] Finland,[360] France,[361] Germany,[362] Israel,[363] Malaysia,[364] Poland,[365] Romania,[366] Russia,[367] South Africa,[368]

[343] Belgium. *Cyber Security Strategy for Defence.*

[344] Netherlands. *The Defense Cyber Strategy.*

[345] UK Government. National Cyber Security Strategy 2016-2021.

[346] *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2.*

[347] UK Government. National Cyber Security Strategy 2016-2021.

[348] Belgium. *Cyber Security Strategy for Defence.*

[349] Netherlands. *The Defense Cyber Strategy.*

[350] *Ibid.*

[351] Karsten Geier, "Presentation of UN GGE Chair on the Inter-Regional Conference between OSCE and Asian Partners on Cyber/ICT" (presentation, Inter-Regional Conference between OSCE and Asian Partners on Cyber/ICT, Seoul, Republic of Korea, April 4, 2017).

[352] Chair: The Rt. Hon. Dominic Grieve QC MP, "Intelligence and Security Committee of Parliament Annual Report 2016–2017" (HC 655, Presented to Parliament pursuant to sections 2 and 3 of the Justice and Security Act 2013, Ordered by the House of Commons to be printed on 20 December 2017). http://mepoforum.sk/wp-content/uploads/2017/12/UK-Intelligence-Security-Committee-2016-2017.pdf.

[353] Noah Shachtman, Peter W Singer, The wrong war: the insistence on applying Cold War metaphors to cybersecurity is misplaced and counterproductive, Brookings Institution, Washington DC, 15 August 2011, https://www.brookings.edu/articles/the-wrong-war-the-insistence-on-applying-cold-war-metaphors-to-cybersecurity-is-misplaced-and-counterproductive/.

[354] Australian Government, *Australia's cyber security strategy: enabling innovation, growth & prosperity*, (21 April, 2016), https://cybersecuritystrategy.pmc.gov.au/assets/pdfs/dpmc-cyber-strategy.pdf.

[355] Austria. Austrian Cyber Security Strategy

[356] Belgium. *Cyber Security Strategy for Defence*

[357] Brazil, Ministério da Defesa, Estado-Maior Conjunto das Forças Armadas*. Doutrina Militar de Defesa Cibernética.* (18 November 2014), http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf

[358] Canada. House of Commons, *BILL C-59 An Act respecting national security matters*, (June 30, 2017), http://www.parl.ca/Content/Bills/421/Government/C-59/C-59_1/C-59_1.pdf.

[359] Danish Ministry of Defence, *Danish Defence Agreement 2010–2014*, (June 24, 2009), http://www.fmn.dk/nyheder/Documents/danish-defence-agreement-2010-2014-english.pdf.

[360] Finland. Prime Minister's Office Publications, *Government's Defence Report.* (16 February, 2017), https://www.defmin.fi/files/3688/J07_2017_Governments_Defence_Report_Eng_PLM_160217.pdf.

[361] France. Direction de l'information légale et administrative, *Livre blanc sur la Defense et la Securite nationale 2013, (April 29, 2013),* http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf.

[362] FR Germany. Bundesminister des Innern. *Cyber-Sicherheitsstrategie für Deutschland 2016.* (9 November, 2016.) https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf.

Sweden,[369] Switzerland,[370] The Netherlands,[371] United Kingdom,[372] and United States of America[373] (**Appendix A**). The number of states which do not publicly display their OCC but do have them is significantly higher.[374,375] It is a general rule that the development of OCC is proportional to the total military, security, and technology-related resources of states.

Actors. OCCs are implemented by military and intelligence-security agencies and units, whose different roles and responsibilities are defined by the constitutions and relevant national laws. The violation of these laws brings about internal instability and political problems.[376]

Content and Objectives. In most countries OCCs are implemented in the form of intelligence, combat, clandestine or special operations, which are by nature covert. There are few official announcements on these operations, mostly when they are undertaken against terrorists[377,378,379]

[363] Israel. *Detering Terror: How Isreal Confronts the Next Generation of Threats*; English Translation of the Official Strategy of the Israel Defense Forces. Harvard Kennedy School: BELFER Center for Science and International Affairs, (August 2016), https://www.belfercenter.org/sites/default/files/legacy/files/IDFDoctrineTranslation.pdf

[364] Malaysia, Ministry of Defence, *Malaysia's National Defence Policy*. (2010). http://www.mod.gov.my/images/mindef/lain-lain/ndp.pdf.

[365] Poland, National Security Bureau. *National Security Strategy of the Republic of Poland*. (5 November, 2014), https://www.bbn.gov.pl/ftp/dok/NSS_RP.pdf.

[366] Romania, Guvernul României, *Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetic*,(23 May, 2015), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf.

[367] Министерство иностранных дел Российской Федерации. *Военная доктрина Российской Федерации*. (26 December, 2014.), Retrieved from http://www.mid.ru/documents/10180/822714/41d527556bec8deb3530.pdf/d899528d-4f07-4145-b565-1f9ac290906c.

[368] South Africa. Ministry of Defence and Military Veterans, South African Defence Review 2015, (2016.), http://www.dod.mil.za/documents/defencereview/defence%20review%202015.pdf.

[369] Sweden, Government Offices of Sweden, *Sweden's Defence Policy 2016 to 2020*. (1 June, 2015), http://www.government.se/globalassets/government/dokument/forsvarsdepartementet/sweden_defence_policy_2016_to_2020.

[370] Switzerland. Département fédéral de la défense, de la protection de la population et des sports (DDPS), *PLAN D'ACTION CYBERDEFENSE DDPS (PACD)*, (09 September, 2017), from https://www.vbs.admin.ch/content/vbs-internet/fr/die-schweizer-armee/schutz-vor-cyber-angriffen.download/vbs-internet/fr/documents/defense/cyberattaques/Aktionsplan-Cyberdefense-f.pdf.

[371] Netherlands. *The Defense Cyber Strategy*.

[372] UK Government. National Cyber Security Strategy 2016-2021.

[373] US Department of Defense, Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934. (November 2011), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf.

[374] Ewen MacAskill, "US And UK Blame Russia For 'Malicious' Cyber-Offensive". *The Guardian*. April 16, 2018. https://www.theguardian.com/technology/2018/apr/16/us-and-uk-blame-russia-for-malicious-cyber-offensive.

[375] *Alex Hern, "North Korea Is A Bigger Cyber-Attack Threat Than Russia, Says Expert"*. The Guardian. *Last modified Februar 26, 2018*. https://www.theguardian.com/technology/2018/feb/26/north-korea-cyber-attack-threat-russia.

[376] Justin McCurry, "South Korea spy agency admits trying to rig 2012 presidential election," last modified August 4, 2017, https://www.theguardian.com/world/2017/aug/04/south-koreas-spy-agency-admits-trying-rig-election-national-intelligence-service-2012.

[377] Bradley Barth, Senior Reporter, Tom Reeve, and Tony Morbin,"U.K. Intel Director Discloses Offensive Cyber Campaign Against ISIS, Lambastes Russia". SC Media US. Last modified April 12, 2018. https://www.scmagazine.com/uk-intel-director-discloses-offensive-cyber-campaign-against-isis-lambastes-russia/article/758220/.

or criminals.[380,381] According to external sources, some countries are conducting the OCCs against political dissidents.[382, 383,384]

Power projection is achieved by operations and activities, or a combination thereof, across all layers and domains. In such organizations, any type of capability is readiness to project power, but also a process, state, competence, potential, capacity, and possession of resources to achieve a task. According to U.S. DoD, offensive cyber operations (OCO) **"**are cyber operations intended to project power by the application of force, in and through cyberspace".[385]

Regardless of the environment, achieving interests and acting against the opponent through effects and influences is accomplished through a possibility (with primarily external context) or a capability (knowledge, skills, and resources such as capital, time, people, processes, systems and technologies).[386]

Effects. According to U.S. DoD, OCCs "are concerned with using cyberspace capabilities to create effects which support operations across the physical domains and cyberspace."[387] Effects could be a sort of force application, or of related nature. The effects force the other side to act according to the intentions and ideas of the side projecting power. The effects of OCC application can be of military and non-military nature, such as:

- denial effects on people, entities, assets, and events, which may have the character of an act of aggression, use of force, or an (armed) attack;
- espionage/intelligence[388] activities;
- influence on individuals, groups, organizations, and nations, or
- combined (attacks, espionage and influence during special operations).

[378] Tom Jowitt, "UK's Offensive Cyber Warfare Ability 'More Than Doubles", Silicon UK. Last modified December 21, 2017. https://www.silicon.co.uk/e-regulation/governance/uks-cyber-warfare-ability-226365.

[379] Malcolm Turnbull, "Address to parliament: national security update on counter terrorism", 23 November 2016, transcript, https://www.pm.gov.au/media/address-parliament-national-security-update-counter-terrorism.

[380] Schwartz, Mattathias. "Cyberwar For Sale". New York Times online. Last modified January 4, 2017. https://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html?smi=%20d=3Dtw-share&_r=1&mtrref=undefined.

[381] Olivia Solon. "Police Crack Down On Silk Road Following First Drug Dealer Conviction". Wired.co.uk. Last modified on February 1, 2013. http://www.wired.co.uk/article/silk-road-crackdown.

[382] William R.Marczak, John Scott-Railton, Morgan Marquis-Boire, and Vern Paxson. "When Governments Hack Opponents: A Look at Actors and Technology." In *USENIX Security Symposium*, pp. 511-525. 2014. https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-marczak.pdf.

[383] "UK Launched Cyber-Attack On Islamic State". 2018. BBC News. Last modified on April, 12, 2018. http://www.bbc.com/news/technology-43738953.

[384] Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton. *For their eyes only: The commercialization of digital spying*. Citizen Lab, 2013.https://citizenlab.ca/storage/finfisher/final/fortheireyesonly.pdf.

[385] JP 3-12 (R), p. vii.

[386] International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC). (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary (ISO/IEC 27000:2018(en)). https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en.

[387] JP 3-12 (R), p. I-5.

[388] Depending on the angle of observation, whether this activity is undertaken by our authorities, or by foreign authorities against our country.

An example of such operation is provided in the UK MoD doctrine document, which defines the attributes of "cyber" as: "To operate and project power in and out of cyberspace to influence the behaviour of people or the course of events."[389]

Denial effects are achieved by violating the integrity, availability, authenticity, and reliability of information. Intelligence effects are achieved by violating confidentiality. By combining these activities, effects and influence of physical, logical, or cognitive nature or combined are realized.

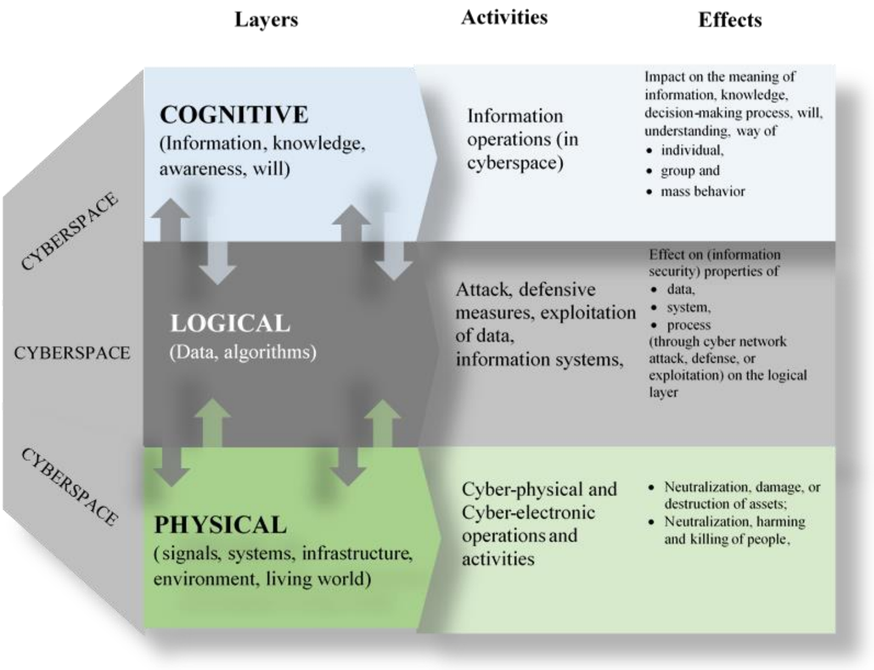
The primary (first) effect of the OCC application is always on the logical layer of cyberspace by violation of counterpart's information security, while secondary and tertiary effects manifest either in cyberspace (on the physical, logical, or cognitive layer) or in the external physical or information environment (**Appendix B**).

Theatre of operations. OCCs are performed in, through and from cyberspace. Cyberspace is an operational domain and a theatre of operations and activities for the application of OCCs. The use of offensive cyber capabilities can be achieved on layers that are not separated, but intertwined:

- logical cyber environment (computer-network related);
- cyber-physical environment, and
- cyber-information/cognitive environment.

There is a set of activities and effects on each of the layers in the application of OCC (Figure 2).

Figure 2. Graphical representation of layers of cyberspace and respective OCC and effects.



Layers	Activities	Effects
COGNITIVE (Information, knowledge, awareness, will)	Information operations (in cyberspace)	Impact on the meaning of information, knowledge, decision-making process, will, understanding, way of • individual, • group and • mass behavior
LOGICAL (Data, algorithms)	Attack, defensive measures, exploitation of data, information systems,	Effect on (information security) properties of • data, • system, • process (through cyber network attack, defense, or exploitation) on the logical layer
PHYSICAL (signals, systems, infrastructure, environment, living world)	Cyber-physical and Cyber-electronic operations and activities	• Neutralization, damage, or destruction of assets; • Neutralization, harming and killing of people,

[389] United Kindom Ministry of Defence doctrine document, Cyber Primer.

The approach of leading military forces is similar in view of the military theatre for OCC application. According to the Military Doctrine of the Russian Federation, the use of ICTs and information environment has a similar function as in the American doctrine. The trend of shifting from traditional military threats to information space and the internal state sphere is recognized,[390] putting simultaneous pressure throughout the enemy's territory on land and sea, in the global information space, airspace and outer space.[391] Conflicts are characterized by an asymmetric-hybrid conflict with integrated employment of military force and political, economic, information or other non-military measures. An important external risk is the use of ICTs for the military political purposes against sovereignty, political independence, and territorial integrity of states.[392] Activities and effects are seen on the all three layers of the theatre of operation: cognitive, logical and physical.

The Chinese approach to OCC development also envisions the use of cyberspace as the fifth domain of military operations,[393] provides it with critical strategic nature on the same level as seas, space, and use of nuclear arms. The relationship of cyber warfare (CW) with electromagnetic warfare (EW) and information warfare (IO) operations is similar to relations presented in the American and Russian doctrine.[394] Although the People's Liberation Army (PLA) does have the structure of a military organization, the roles and responsibilities in this domain are different, since the PLA centralized the field of information operations made up from space, cyber, electromagnetic, and psychological capabilities, under a unique umbrella of SSF.[395,396]

Appropriate capabilities, therefore, contain the following elements:

- way of organization (strategy, doctrine, structure, processes);
- human resources (development, training, skills);
- assets (material, financial, and technical resources to apply or support force or influence),
- space (domain, environment of operations and activities),
- time (when, how long, timelines)

[390.] Президент Российской Федерации, Военная доктрина Российской Федерации, December 25, 2014, No. Pr.-2976 11, http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf.

[391] *Ibid*. Article 15 (v).

[392.] *Ibid*. Article 12 (m).

[393] State Council of the People's Republic of China, *China Military Strategy*, May 2015, http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm.

[394] US DoD Office of the Secretary of Defense, Annual Report to Congress, *Military and Security Developments Involving the People's Republic of China 2017*, https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF?ver=2017-06-06-141328-770 . In China military doctrine, Information Operations comprising cyber, electronic, and psychological warfare capabilities.

[395] John Costello, "China Finally Centralizes Its Space, Cyber, Information Forces," *The Diplomat*, last modified on January 20, 2016, https://thediplomat.com/2016/01/china-finally-its-centralizes-space-cyber-information-forces/.

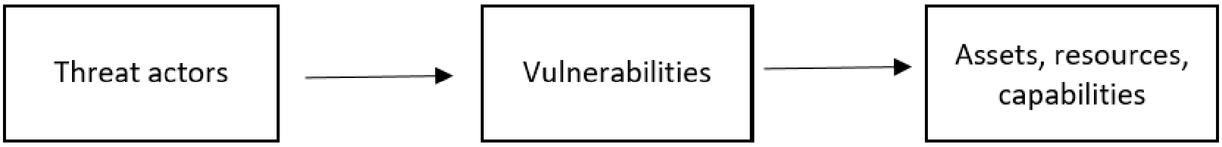
[396] Kevin L. Pollpeter, Michael S. Chase, Eric Heginbotham, The Creation of the PLA
Strategic Support Force and Its Implications for Chinese Military Space Operations, RAND, 2017, Santa Monica, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2058/RAND_RR2058.pdf.

- information resources (knowledge, necessary information for Command and Control (C&C)).

2.2.4 TECHNOLOGY AND INFORMATION SECURITY PERCEPTION

The practice in the field of information security has it that every application of the OCC is realized through a deliberate violation of information of the target. From the aspect of the target, it is realized through actions of a threat actor on vulnerabilities in information-related assets (Figure 3).

Figure 3. Process of threatening information security and cybersecurity



Although there is a similarity and overlap in the meaning between information security and cyber security, these two concepts differ in subject and content. Information security of the Russian Federation refers to the impact on the individual, society and the state, i.e. "...protection of the individual, society and the State against internal and external information threats, allowing to ensure .. the sovereignty, the territorial integrity .."[397]

The U.S. government sees information security as "The protection of information and information systems from unauthorized access .. in order to provide confidentiality, integrity, and availability."[398] Cybersecurity, on the other hand, is seen as "The ability to protect or defend the use of cyberspace from cyber attacks."[399]

According to ISO/IEC 27000 standard, information security is: "...preservation of confidentiality, integrity, and availability of information."[400] For von Solms and van Niekerk, information security is the protection of information (an asset), while cyber security is related to protection of cyberspace, and entities that function in cyberspace and of all assets that can be reached via cyberspace (information as well as non-information based assets such as people, technical and organizational systems, and infrastructure) (Figure 4).

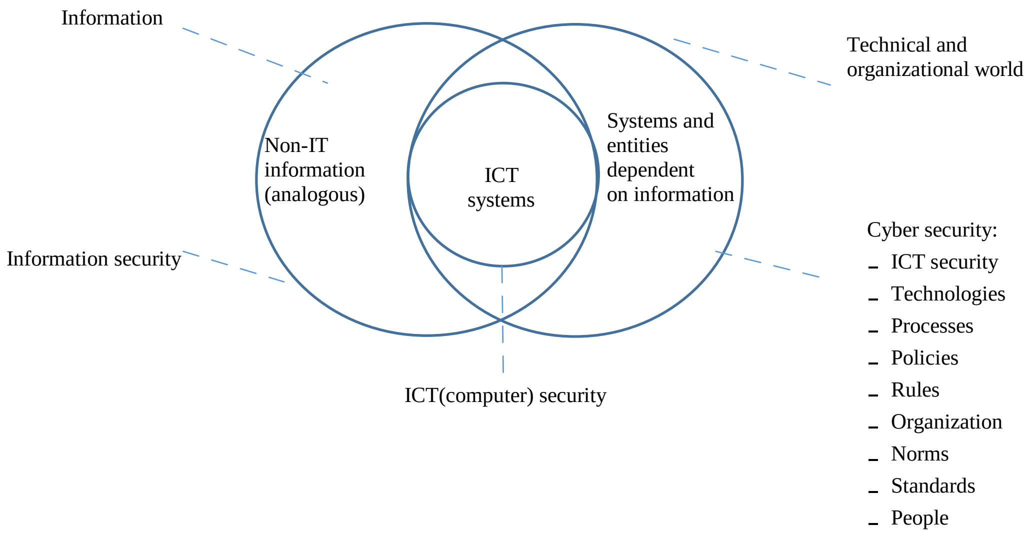
[397] Ministry of Foreign Affairs of the Russian Federation, *Doctrine of Information Security of the Russian Federation*, (5 December, 2016).

[398] 44 U.S. Code § 3544 - Federal agency responsibilities

[399] Richard Kissel, ed. "Glossary of Key Information Security Terms." NISTIT 7298 Revision 2, National Institute of Standards and Technology (2013).

[400] International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC). (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary (ISO/IEC 27000:2018(en)).

Figure 4. Relation between information security, computer, and cyber security



2.2.5 INTERNATIONAL LAW PERCEPTION

UN GGE has reached a consensus that „International law, and 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“[401] It remains unclear still, however, how to apply it and to what forms of use of force and aggression. In case of application to the OCC, these problems go to extremes, because power projection and application of force are very non-standard in cyberspace:

- cyber attacks are carried out by using and targeting ICT systems which are most often dual-use;
- cyber attack effects can be temporarily or temporally postponed;
- the notion of "weapons" and "operations" during use of force in cyberspace is very abstract and relative, only the effects are noticeable and not always immediately after the attack[402];
- effects of the OCC application, in addition to the physical area, also manifest in other layers;

[401] General Assembly 68/98, *Developments in the field of information and telecommunications in the context of international security*, A/68/98, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (24 June 2013). https://undocs.org/A/68/98.

[402] In first half of 2017, the average period for targets to identify the data breach was 191, according to a study: Ponemon Institute and IBM Security, "*2017 Cost of Data Breach Study*", (June 2017). https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf.

- unlike the physical, in cyberspace attacks and espionage are most often performed by identical techniques, with the difference being only in the payload effect at the very end of the OCC application process;
- use of weapons in physical environment signifies the existence of an armed conflict, while the use of offensive-related capabilities in international relations is carried out according to the capabilities of states, organizations, private companies and even individuals-anyone who has the capabilities during conflict and in peace.

For now, there is no consensus in the professional and international community on how the various uses of OCCs refer to the aggressive behaviour mentioned in the UN Charter, "use of force"[403], "act of aggression"[404], "armed force"[405], and "armed attack."[406] Without such consensus, even the UN Charter cannot be fully applied to situations in the context of the OCCs use.

According to Harold Koh, U.S. Department of state legal advisor, "use of force" and "armed attack" in the cyberspace are the same, and they represent equal grounds for use of self-defence by states. [407,408] In states which apply the so called "security principle" of state jurisdiction, the use of such force in cyberspace is justifiable (including the case of achieving national interests).[409]

UN GGE has succeeded to reach a consensus on a limited number of common opinions during 5 sessions over 13 years[410], including on a limited number of voluntary norms, rules or principles of the responsible behaviour of States in cyber-sphere, as well as confidence building measures, international cooperation and capacity building.[411] Several regional organisations have developed voluntary measures, such as Confidence Building Measures, which could, along with the UN GGE work, benefit from greater inclusiveness, policy coherence and comprehensive capacity building[412]. However, all these achievements are of nonbinding, voluntary nature and cannot be applied to regulation of international relations during the conflict in, through, and from cyberspace.

[403] The Charter of the United Nations, Art. 2(4).

[404] The Charter of the United Nations, Art. 1, 39.

[405] The Charter of the United Nations, Preamble, Art. 41.

[406] The Charter of the United Nations, Art. 51.

[407] Harold Honhgu Koh, Legal Advisor of the U.S. Department of State, "International Law in Cyberspace, Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012", *Harvard International Law Journal Online* 54, December 2012 (2012): 13.

[408] UN Charter, art. 51.

[409] Monika B. Krizek, "The Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice." *BU Int'l LJ* 6 (1988): 337.

[410] Digital Watch. Geneva Internet Platform. UN GGE web page. Available from: https://dig.watch/processes/ungge.

[411] General Assembly 70/174, *Developments in the field of information and telecommunications in the context of international security*, A/70/174, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (22 July 2015), available from http://undocs.org/A/70/174.

[412] Radunovic, Vladimir. "Towards a secure cyberspace via regional cooperation". *DiploFoundation* (2017). https://www.diplomacy.edu//sites/default/files/Diplo-Towards_a_secure_cyberspace-GGE.pdf.

Finally, the application of international law to the use of OCCs in specific situations is most directly aggravated by the states' inability to effectively discover cyber attacks, to identify attackers and perform attribution.[413]

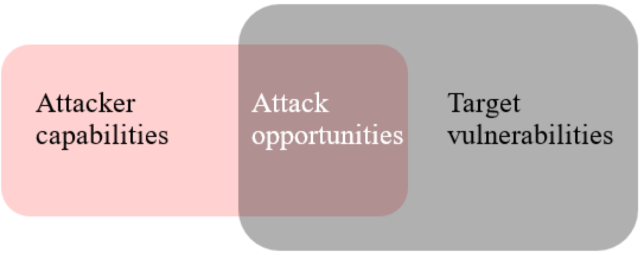
3 ELEMENTS AND CONTENT OF OCCS

Understanding the OCC requires determining its elements, their key characteristics and composition in accordance with legal and political considerations. The following section identifies the elements, processes and content of offensive cyber capabilities.

3.1 VULNERABILITIES AS A CENTRAL POINT BETWEEN AN ATTACK AND A WEAPON

A cyber-attack occurs when the attacker's (threat actor's) capabilities meet attack opportunities for malicious exploitation of vulnerabilities (Figure 5). The essence of conducting cyber-attacks is that one or more vulnerabilities are exploited in order to achieve an objective. Vulnerabilities are therefore the foundation of the OCCs development.

Figure 5. When capabilities meet vulnerabilities, opportunities are created



According to ISO/IEC 27000:2018(en) standard, a vulnerability is a "weakness of an asset or control that can be exploited by one or more threats".[414] Vulnerability is also defined as "a characteristic or specific weakness that renders an organization or asset .. open to exploitation"[415], and "property of a cyber entity that is susceptible to exploitation"[416]; it can allow "an attacker to negatively affect its normal functioning, or the confidentiality or integrity of the data it contains"[417], i.e. "to circumvent security measures"[418]. Vulnerability can, thus, be defined as any flaw or weakness in the system design, implementation, or operation and management that could be exploited to violate a system's security policy.

[413] Mladenovic, *Multidisciplinary aspects of cyber warfare,* (2016).

[414] International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC). (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary (ISO/IEC 27000:2018(en)).

[415] US, Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies, "Explore Terms: A Glossary of Common Cybersecurity Terminology" ND. Available from http://niccs.us-cert.gov/glossary.

[416] *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2.*

[417] France, *Information Systems Defence and Security: France's Strategy.*

[418] Pawlak, Patryk ed. Institute for Security Studies Paris. "Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development". (2014). http://www.iss.europa.eu/uploads/media/Report_21_Cyber.pdf.

Information security professionals increasingly believe that there are no securely connected things anymore.[419] However, vulnerabilities are not always of technological or information related. More often than not, people represent the greatest vulnerability in organizations. Therefore, vulnerabilities relate equally to system design (including its protection), their functional implementation (as well as implementation of protection measures) and to the organization itself.

Both the attack as a process, and the weapon as means, are designed to exploit one or more vulnerabilities on the attack target. The existence of a vulnerability in a target is a necessary but not a sufficient condition for conducting a cyber attack.

3.2 WHAT IS A CYBER-ATTACK?

The character of cyber attacks varies depending on the point of view. For the purpose of realizing military objectives through cyber attacks, force is projected by "cyberspace actions that create various **direct denial** effects in cyberspace (i.e., degradation, disruption, or destruction) and **manipulation** that leads to denial that is hidden or that manifests in the physical domains"[420]. Cyber attack is an activity conducted in cyberspace creating effects in, through or from cyberspace. Primary (immediate) effects are always achieved in cyberspace.

This approach is not supported by all scholars. For example, Hathaway and a group of authors suggest that a cyber attack "consists of any action taken to undermine the functions of a computer network for a political or national security purpose"[421]. In this approach, the authors accept the „U.S. objective-based approach rather than the means-based approach of the Shanghai Cooperation Organization (SCO)",[422] as more intuitive and logical. However, accepting such an approach would mean that smashing a computer within a critical infrastructure system with a hammer would constitute an act of cyber attack, which is certainly not the case. On the other hand, according to Lachow, in order to be specific in defining, cyber attacks are characterized exclusively according to the means used to perform an attack.[423]

In the practice of military art, types of operations and warfare are categorized on various basis: according to means;[424] objectives,[425] or domains,[426] and selection is made according to the most important criterion for determining nature of such a military activity.[427] Activities that are characteristic for cyberspace are, then, those conducted in cyberspace, with first and immediate effect realized in cyberspace.

[419] Debora Plunkett, cited in Adam Shostack, The evolution of information security, The Next Wave, Vol. 19., No. 2, 2012, https://www.nsa.gov/resources/everyone/digital-media-center/publications/the-next-wave/assets/files/TNW-19-2.pdf.
[420] JP 3-12 (R), p. II-5.
[421] Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. "The law of cyber-attack." *California Law Review* (2012): 817-885, 826.
[422] *Ibid.*
[423] Lachow, Irving. "Cyber terrorism: Menace or myth." *Cyberpower and national security* (2009): 434-467.
[424] For example, conventional, nuclear, infantry, armored mechanized, chemical warfare and other types.
[425] For example, economic, psychological, media warfare, electronic warfare and other types.
[426] For example, naval, land, air, space, urban, or cyber warfare.
[427] Mladenovic, *Multidisciplinary aspects of cyber warfare.*

Cyber attack objectives are offensive, to create advantages for oneself, and disadvantage for the adversary.[428] Effects of cyber attacks could be of various types:

- physical effect in the physical environment (such is Stuxnet operation);
- information effect in the social sphere (such is destabilization of a nation, elections manipulation, etc.);
- computer-network logical effect on data, system, service, of process, or
- mixed and cascading, as is the case of most cyber attacks.

In terms of practice of information security, an attack represents a violation of information security of target's information resources or an attempt to do so. According to ISO standards, an attack represents „**Attempts** to destroy, expose, alter, or disable" [429] or "**steal or gain unauthorized access** to or make **unauthorized use** of an asset"[430]. Internet Engineering Task Force (IETF) defines an attack as "An intentional act by which an entity attempts to evade security services and violate the security policy of a system"[431]

The EastWest Institute defines a cyber attack as "an offensive use of a cyber weapon **intended** to harm a designated target."[432]. U.S. Committee on National Security Systems (CNSS) and NIST define an attack as: "Any kind of malicious activity that **attempts** to collect, disrupt, deny, degrade, or destroy information system resources or the information itself".[433] Similarly to IETF, they differentiate between an active and passive attack, where an active attack is the one that alters a system or data[434], while the passive one does not alter systems or data.[435]

Austria defines the term "cyber attack" as "an attack through IT in cyber space" against IT systems which aims to "undermine the objectives of ICT security protection partly or totally",[436] while Australia defines it as "deliberate acts that seriously compromise national security, stability or prosperity by manipulating, denying access to, degrading or destroying computers or networks or the information resident on them"[437]. Romanian CERT defines it as offensive hostile action deployed to affect the other state's cyberspace and cybersecurity of people, assets and resources under its jurisdiction.[438] NATO defines a computer network attack as "Action taken to disrupt,

[428] Herbert Lin, Fundamentals of Cyber Conflict, presentation, Stanford University, CS-203, (May 23, 2017).
[429] ISO/IEC 27039:2015(en), Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS). https://www.iso.org/obp/ui/#iso:std:iso-iec:27039:ed-1:v2:en.
[430] ISO/IEC 27000:2018(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en.
[431] Robert Shirey, IETF Network Working Group, Internet Security Glossary, Version 2, https://tools.ietf.org/html/rfc4949.
[432] *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2*.
[433] Committee on National Security Systems, (CNSS) Glossary, CNSSI No. 4009, April 6, 2015, p.9. https://www.cnss.gov/CNSS/openDoc.cfm?M0+zCfvO9T1o4xRsSJyX5Q==.
[434] *Ibid.* p.4.
[435] *Ibid.* p.137.
[436] Austria, Austrian Cyber Security Strategy.
[437] Australia's Cyber Security Strategy: Enabling innovation, growth and prosperity (p.15).
[438] Romania, CERT Romania, "Resolution no. 271/2013 approving Romania's cyber security strategy and national action plan on implementation of the national cybersecurity (Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică)," CERT Romania, (2013), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf.

deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself"[439].

The previous analysis provides key characteristics of a cyber attack related to the application of OCC:

- an attempt or a violation of information security on the target side by exploiting its vulnerabilities;
- a purposeful and planned activity;
- often conducted by cyber weapon, though this is not a necessary condition;
- regulated by law even if there are no consequences;
- may be equivalent to an armed attack under the international law regulation, but also to an act of espionage or information operation.

3.3 WHAT IS A CYBER WEAPON?

A weapon is "An instrument of any kind used in warfare or in combat to attack and overcome an enemy."[440] By analogy, a cyber weapon is an instrument of power projection through attack and overcoming the adversary by creating a harmful effect in, through, and from cyberspace, where these effects could be transferred to the physical and information environment. According to Dale Peterson, in the cyber-physical realm, development of a cyber weapon is the first step towards acquiring an offensive cyber capability.[441] Generally, the attack involves an offensive activity using weapons that can be offensive and defensive in nature.[442]

Former Lead for the Aurora Generator Test[443] Perry Pederson, defines cyber weapon as "a software artefact"[444] designed to cause physical harm to objects, people, or the environment."[445] However, Pederson connects the term „weapon" only to physical harm of critical technical systems, not attacks without physical consequences.

Unlike physical environment, cyber weapon may be both a **means** and a **process** (method or technique) of an attack.

The approach of means and methods of warfare, as legal terms of military art used in the LOAC, has been accepted by international groups of experts at the invitation of the NATO Cooperative

[439] NATO, NATO Glossary of Terms and Definitions (English And French), AAP-06 Edition 2014 http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6EN.pdf.

[440] "Weapon", noun, Oxford English Dictionaly, Online, www.oed.com

[441] Peterson, Dale. "Offensive cyber weapons: construction, development, and employment." *Journal of Strategic Studies* 36, no. 1 (2013): 120-124.

[442] Herbert Lin, Fundamentals of Cyber Conflict.

[443] A famous Idaho National Laboratory test estimation of the possibility whether a cyber attack could destroy physical components of the electric grid in this case a large electric power generator. NERC Press Release, *NERC Issues AURORA Alert to Industry*, (October 14, 2010). Source: http://www.ect.coop/wp-content/uploads/2010/10/PR_AURORA_14_Oct_10.pdf.

[444] A term "software artifact" can be understood as any kind of software product or craft work in software development process, that has been documented and stored in a repository so it can be retrieved upon demand. DevOps Agenda TechTarget, (October 2017), https://devopsagenda.techtarget.com/definition/artifact-software-development.

[445] Perry Pederson. "IT vs. ICS: An Attacker's Perspective," (September 7, 2014), https://www.langner.com/2014/09/it-vs-ics-an-attackers-perspective/.

Cyber Defence Centre of Excellence (CCDCOE), the authors of Tallinn Manual: “means of cyber warfare are cyber weapons and their associated cyber systems”, and “methods of cyber warfare are the cyber tactics, techniques, and procedures by which hostilities are conducted”.[446]

The definition of “information weapon” proposed by the Russian Federation in 1999 considers it as both means and methods used for the purpose of damaging all kinds of information resources (data, processes and systems), with damaging consequences across all three cyberspace layers, and with final effects in physical and information environment.[447]

A suggested blended definition of information weapons, that takes into account major elements of various available state definitions in order to scope various views, follows a similar pattern:

Technologies, means and methods used[448]*, resources strategically developed or created*[449]*, and information and telecommunication technologies and systems*[450] *- including software, firmware or hardware*[451] *- designed or applied with malicious intent*[452]*, to exert influence over adversaries*[453] *and cause damage*[454]*,*[455] *{particularly} to state’s infrastructure and national networks*[456] *- information resources, processes and systems*[457] *(including defence, administrative, political, social, economic and other vital systems*[458] *).*

Means and methods of use are important since it is not possible to conduct a cyber attack using a universal "cyber weapon", as in the physical world, where a missile operates with the same kinetic force on all targets. In cyberspace, one weapon is usually tailor-made for one target, or a class of targets (a representative example is the Stuxnet malware spread across the globe, but it operated on only one target-the nuclear unit in Natanz)[459,460].

[446] *Tallinn Manual 2.0 on the international law applicable to cyber operations, p. 452.*

[447] Russia, Submission to the United Nations General Assembly Resolution G.A. Res. 54/213, U.N. Doc. A/RES/54/213 (August, 10, 1999), https://disarmament-library.un.org/UNODA/Library.nsf/f4c497d5f90e302d85257631005152d2/fae7e8060174f22c8525764e0051ce60/$FILE/A-54-213.pdf. p. 10.

[448] Министерство обороны Российской Федерации (Минобороны России), *Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве* (2011), http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle (accesed on 18. mart 2015).

[449] Philippines, Submission to the United Nations General Assembly Resolution A/56/164, (2001). http://www.un.org/documents/ga/docs/56/a56164.pdf.

[450] Cuba, Submission to the United Nations General Assembly Resolution A/58/373, (2003). https://disarmament-library.un.org/UNODA/Library.nsf/c793d171848bac2b85256d7500700384/b69c21ea9dcbb95785256dc10058b4c9/$FILE/sg58.373.pdf.

[451] *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2.*

[452] Philippines, Submission to the United Nations General Assembly Resolution A/56/164.

[453] Russia, Submission to the United Nations General Assembly Resolution G.A. Res. 54/213, p. 10.

[454] *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2.*

[455] Philippines, Submission to the United Nations General Assembly Resolution A/56/164.

[456] Cuba, Submission to the United Nations General Assembly Resolution A/58/373.

[457] Russia, Submission to the United Nations General Assembly Resolution G.A. Res. 54/213, p.10.

[458] *Ibid.*

[459] Langner, Ralph. "To kill a centrifuge: A technical analysis of what stuxnet’s creators tried to achieve." (2017) https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

[460] Peterson, Dale. “Offensive cyber weapons: construction, development, and employment.” Journal of Strategic Studies 36, no. 1 (2013): 120-124.

The use of cyber weapons and the conducting of cyber attacks always depend on the character of target, vulnerabilities and cyberspace layer in which the primary attack effect is achieved. Some contemporary authors believe that the idea of cyber weapons is therefore debatable.[461] Unlike the physical space, cyber weapons may be constructed from vulnerabilities, exploits and payloads discovered and developed by civilians and groups with particular knowledge, rather than by using vast (financial and human) resources such as companies or states. At the same time, however, vulnerabilities have a relatively short "life expectancy", since they may be discovered by the vendor, system manager or an ethical third party, and patched accordingly, rendering it useless for the parties possessing it within their own "cyber-arsenal".

In a cyber environment, cyber weapons need not necessarily exist in order to achieve a cyber attack; sometimes the technique or an act by the attacker or a mistake of the defender is sufficient to access physically or remotely the system processes or files (eg. through social engineering) [462]. Also, a cyber weapon can be deployed in the targeted system, but it does not ever have to be activated. In this respect, a cyber weapon is a means which gives the capability to a cyber attacker to conduct a cyber attack and to cause effects and achieve objectives of such an attack.

In some attacks, the very process of encryption has a role of a „weapon", but encryption is not a weapon.[463] However, Wassenaar Arrangement [464] restricted the export of certain types of encryption tools and products in 1998[465] and in 2013,[466,467] preventing their trade and use if they are applied in some other armed technologies for development of surveillance software which may violate basic human rights.[468] Dual-use nature of tools is one of the major challenges in regulating cyber-weapons. The existing non-cyber processes for arms proliferation control, that include examples of dual-use technology and particularly ICT tools, may provide some ideas for cyberspace as well – particularly Nuclear Suppliers Group[469] and Missile Technology Control Regime[470] with their provisions related to software associated with items on the export control

[461] Herbert Lin, Fundamentals of Cyber Conflict.

[462] Kevin D. Mitnick, William L. Simon. *The art of deception: Controlling the human element of security.* (John Wiley & Sons: 2011).

[463] Gladman, Brian. "Wassenaar controls, cyber-crime and information terrorism." *Leeds, UK: Cyber-Rights & Cyber-Liberties (UK). September 1998.*

[464] Export Controls for Conventional Arms and Dual-Use Goods and Technologies, https://www.wassenaar.org/.

[465] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies And Munition List, WA LIST (98) 1, (03-12-98). https://www.wassenaar.org/app/uploads/2015/06/Previous/1998_OK/WA-LIST%20%2898%29%201.pdf.

[466] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, (2013), https://www.wassenaar.org/app/uploads/2015/06/Previous/2013_OK/WA-LIST%20%2813%29%201.pdf

[467] http://www.cryptolaw.org/cls2.htm.

[468] Kim Zetter, Lily Newman, Brian Barrett, Louise Matsakis, and Andy Greenberg. "Why An Arms Control Pact Has Security Experts Up In Arms". Wired. Last modified on June 24, 2015. https://www.wired.com/2015/06/arms-control-pact-security-experts-arms/.

[469] Nuclear Supplier Group (NSG): http://www.nti.org/learn/treaties-and-regimes/nuclear-suppliers-group-nsg/.

[470] Missile Technology Control Regime (MTCR): mtcr.info/mtcr-annex/?lang=en .

list, as well as the Australia Group[471] related to the export of biological and chemical weapons including dual-use.

It is justified to use the cyber weapon concept in all cases when tailored software alone or its combination with hardware is used. The use of cyber-hardware systems as weapons systems is especially characteristic for military and civilian security-intelligence usage. One of the more prominent examples is the US DoD Defense Advanced Research Projects Agency's program (DARPA) called Plan X, which is a foundational cyberwarfare program to develop platforms for the Department of Defense to plan, conduct, and assess cyberwarfare in a similar manner to kinetic warfare."[472,473,474]

In any case, every means and method must be tailored for specific target and its known and publicly unknown vulnerabilities. Thus, a cyber attack is achieved by applying appropriate means and methods in cyberspace, and it exerts its effect in cyberspace, through cyberspace, and from cyberspace. In a way, a cyber attack is a "cyber weapon".

4 RECOMMENDATIONS

As concluded in the previous analysis, in international relations OCCs represent a complex application of capacities and abilities (means) by international entities for the purpose of achieving political and security-related goals (effects). In line with the previous analysis, some conclusions and recommendations will be presented in the following lines.

4.1 OCCS' NATURE

OCCs are applied based on a decision of a government authority, with the political, military and non-military goals (effects and influence), in, through, and from cyberspace, through the application of particular means, methods and tools (cyber weapons and cyber attacks). This application is always aggressive in nature, actively directed at the target. Aggressive enforcement does not make it illegal since it can be used as a right to self-defence or for the purpose of legal activities in support of the rule of law, international peace and stability. Regardless of the target, the type of military operation, and other characteristics, it must be in line with international law. (LOAC, i.e. International Customary Humanitarian Law).

Any OCC can be considered as a planned, organized, achieved and practical **ability to project power** in, through, and from cyberspace in accordance with its own **capacities**, in order to accomplish the intended **effects** and **objectives** to support its own **interests**. Such capability is achieved through constant development, improvement of knowledge, skills and availability of appropriate **means** and **tools**. In accordance with that, OCCs represent the above mentioned capabilities in, through, or from cyberspace for power projection by **use of force**, and by **influence**.

[471] Australia Group: http://www.australiagroup.net/en/.

[472] Defense Advanced Research Projects Agency, Plan X, https://www.darpa.mil/program/plan-x.

[473] Global Internet Liberty Campaign, *Cryptography is a defensive tool, not a weapon*, A statement by the global internet liberty campaign, (September 1998), http://www.cyber-rights.org/crypto/gilc-wass.htm.

[474] Shehadeh, Karim K. "The Wassenaar Arrangement and Encryption Exports: An Ineffective Export Control Regime that Compromises United States Economic Interests." *Am. U. Int'l L. Rev.* 15 (1999): 271.

Such power projection has effects in different physical or non-physical domains. The first (primary) consequences of OCC happen at the logical layer of cyberspace. They can vary in form, but they all cause the emergence of subsequent and final consequences of the OCC use, which is to provoke events; realize material and non-material consequences in the physical and information domain; violate the ability of the other party (competitor, opponent, or enemy), or otherwise force him to act in the way desired by the one using force and influence.

The practice of cyber attacks in the past few decades shows that their consequences can occur at all levels and in all environments where there is the presence of ICTs and information systems, networks, sensors and controllers and their influence on people, infrastructure, technical and organizational systems. These consequences can range from the usual annoying obstruction of system users to deactivation of nuclear facilities for the enrichment of nuclear fuel. However, what is characteristic of all cyber attacks that have occurred is the circumstance that in all of these cases the first effect occurred on the logical layer of cyberspace. Thanks to the inherent characteristic of the use of ICTs that it is possible to copy data in digital form infinite number of times and that it is possible to achieve communication between systems at data level as well as the growing capability of embedding of ICTs in all technical and organizational systems and processes in the physical and informational environment, the consequences of offensive cyber action can happen everywhere. However, what distinguishes a cyber attack from a physical attack on computer systems and infrastructure, or an information operation in cyberspace from cyber attacks is exactly the characteristic that the first effect in the cascading or chain process of cyber attacks must be achieved at the logical level of cyberspace.

4.2 IDENTIFICATION OF MAIN CHALLENGES RELATED TO THE USE OF OCCS

The basic challenges related to the use of OCC (i.e. in the information environment or through use of information and telecommunications in the context of security) are:

- international law is applicable to the use of the OCC, but their complex nature disables practical application in a large number of cases, particularly in terms of lack of States' capacity to detect attacks, and identify and attribute the attackers;
- both state and non-state actors are involved in the OCCs development and implementation process;
- there is lack of adequate specialized international regulation, and absence of practical rules, mechanisms and competent authorities of international community to regulate cyber conflict;
- with the technological development, capabilities are enhanced and the effects of their application becomes more critical;
- with the growth of ICT use (particularly the connected "smart" devices), the number of vulnerabilities enabling the use of cyber attacks increases;
- the complexity of cyberspace and the application of ICTs produces a wider set of possible forms of aggression, use of force and malicious influence in, through, and from cyberspace.

4.4 RECOMMENDATIONS FOR KEY DEFINITIONS

Successful cooperation and negotiations on rules of state behaviour in cyberspace depend on common understanding of main terminology. It is therefore necessary to define key terminology, such as “offensive cyber capabilities”, “cyber attack”, “cyber weapon”, “cyber aggression”, and “cyber conflict”, on the international level. While blended definitions suggested earlier may serve as a starting point for discussion, the recommended definitions based on the analysis performed in this paper are as follows:

Offensive cyber capabilities: capabilities to project power and influence and create effect in, through, and from cyberspace directed toward targeted objective by the use of adequate means, techniques and methods.

Cyber attack: an attempt or realization of an offensive activity by use of means, techniques, and methods with the goal to cause harmful effects in cyberspace, which can spread and cause other adverse effects for the opponent in the physical and information environment.

Cyber weapon: technologies, means and methods, including software or hardware tools, strategically developed to deliver power projection and influence in, through, and from cyberspace.

Cyber aggression: an attempt or a process of causing harm in international relations incompatible with the objectives and provisions of the UN Charter.

Cyber conflict: an international conflict involving cyber attacks in cyber space, with harmful consequences that manifest in, through, or from cyberspace.

4.5 RECOMMENDATION IN RELATION TO ADDRESSING OCC MEANS AND EFFECTS

Official state documents analysed earlier mainly define OCC and cyber weapons as means designed to project power and influence and create effect in or through cyberspace. Military art practice categorises warfare on the basis of means, objectives and domains, while dictionaries describe offense also as achieving power projection and causing effects. Finally, each cyber activity – operations, attacks, exploitations – has effect on particular layers of cyberspace. Previous analysis certifies that the relation between means and effects of OCC is intrinsic.

As discussed, there is a different focus of some of the major actors, with the U.S. objective-based approach in which OCC application intends to create effects, comparing to the SCO means-based approach in which means of achieving the goals are of key relevance. Nevertheless, both parties also put strong emphasis on the other component as well in their definitions: US on means and resources used (such as device, computer program, or technique), and Russia on effects (exerting influence over adversaries and causing damage to information resources, processes and systems), confirming the general agreement that both means and effects are of high relevance.

Particular challenge in regulating effects is that they may not be noticeable immediately after the attack, and the attacks are hard to attribute. Similarly, a challenge with regulating means is that cyber weapons are tailor-made per targets and are dual-use, and the attacks may even be conducted without a cyber weapon. Not the least, most weapons are based on exploiting vulnerabilities, which emerge due to lack of security procedures and culture in developing and using the tools and services of cyberspace.

Regulating cyber conflict, therefore, demands a combined approach to addressing both means and effects. In addition, a firm policy and regulatory approach towards intrinsically more secure cyber environment (through defined roles and responsibilities of states as well as non-state actors) is necessary.

4.6 RECOMMENDATION FOR PRACTICAL INTERNATIONAL REGULATION OF THE OCC USE

International law provides instruments for regulation of state behaviour in international relations, which is based on both interests and coercion, and which can be applied for prevention and in case of cyber conflict. The application of these instruments, however, is not entirely clear. In this regard, the key directions for further progress of the international community in this area are in the field of protection of countries which do not possess OCC, and enhanced cooperation of states which are the leading forces in the field of development and application of OCC.

The first course of recommended action is to further explore applicability of existing rules of the international law on use of force and prevention of aggressive behaviour through projection of force and influence in cyberspace.

The second course of action is to introduce new rules whenever existing international law rules cannot be effective and efficient due to specificities of cyber operations.

The third course of action is to foster bilateral and multilateral agreements, particularly between the world's leading military forces that have OCCs and practice their implementation in international relations.

The fourth course of action is enhanced dialogue and involvement of all the international actors and stakeholder groups in shaping the global and regional regulation pertaining to cyberspace.

Finally, the cyber attacker's attribution is a complex process achieved at the technical level (by determining the devices from which the cyber attack was launched), at the legal level (determining which entity is responsible in accordance with international law for the undertaken activity that led to the consequences of the attack), and political level (when states make a decision on the responsible entity for the attack, mainly on the basis of intelligence information). In the modern world, the political attribution of cyber attackers depends largely on the implementation of intelligence activities in both cyberspace and the physical environment that a limited number of countries today can do. The ability to achieve an accurate and reliable attribution of cyber attackers does not exist at a wider international level. The problem of attributing cyber attackers is not in the absence of legal provisions for determining responsibilities of entities. It is also not possible to achieve the exchange of highly confidential intelligence between all States. Therefore, the only way to solve the problem of cyber attackers at the international level in order to regulate the application of offensive cyber capabilities is to build the appropriate technical capabilities of the international community. This ability directly influences the application and development of all confidence and capacity building measures in the process of preserving peace and international stability in the field of application of information and ICTs in the context of security. It is possible and necessary to achieve the collaboration of all stakeholders, such as professional community, academic community, private business, research and development institutions, international professional organizations, governmental expert bodies and agencies and all other qualified actors. In order for this involvement and engagement to be legitimate, it must be voluntary, open, public, and based on objective principles of the profession. In that respect, it is not necessary to establish organs and institutions for performance of objective attribution, but a peer-reviewed methodology of the attribution process, as well as expert centers to provide support to those actors who do not have their own capacities and are threatened by cyber attacks. Such processes should be led by the most eminent and appropriate professional organizations.

BIBLIOGRAPHY

Alex Hern, "North Korea Is A Bigger Cyber-Attack Threat Than Russia, Says Expert". *The Guardian*. https://www.theguardian.com/technology/2018/feb/26/north-korea-cyber-attack-threat-russia.

Asimov, Isaac, and Jason A. Shulman, eds. *Isaac Asimov's book of science and nature quotations*. Weidenfeld & Nicolson, 1988.

Australian Government, *Australia's cyber security strategy: enabling innovation, growth & prosperity*, (21 April, 2016), https://cybersecuritystrategy.pmc.gov.au/assets/pdfs/dpmc-cyber-strategy.pdf

Austria, Bundeskanzleramt Osterreich, Austrian Cyber Security Strategy, (2013), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

Bacon, Francis. "Proposition Touching Amendment of Laws." *The Works of Francis Bacon* 13: 1857-74.

Belgium. Defence Strategy Department. *Cyber Security Strategy for Defence*. (2014). https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf

Bowyer, R. (2015). *Dictionary of Military Terms: Over 6,000 words clearly defined*. Bloomsbury Publishing. p. 171.

Bradley Barth, Senior Reporter, Tom Reeve, and Tony Morbin,"U.K. Intel Director Discloses Offensive Cyber Campaign Against ISIS, Lambastes Russia". SC Media US. https://www.scmagazine.com/uk-intel-director-discloses-offensive-cyber-campaign-against-isis-lambastes-russia/article/758220/

Brazil, Ministério da Defesa, Estado-Maior Conjunto das Forças Armadas. *Doutrina Militar de Defesa Cibernética.* (18 November 2014), http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf

Cambridge Dictionary online. https://dictionary.cambridge.org/dictionary/english

Canada, Government of Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (2010), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx.

Canada. House of Commons, *BILL C-59 An Act respecting national security matters*, (June 30, 2017), http://www.parl.ca/Content/Bills/421/Government/C-59/C-59_1/C-59_1.pdf

Candid Wueest, and Himanshu Anand, Internet Security Threat Report: Living off the land and fileless attack techniques, Symantec, July 2017, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf

Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits, International Court of Justice (ICJ), 27 June 1986, available at: http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

Chair: The Rt. Hon. Dominic Grieve QC MP, "Intelligence and Security Committee of Parliament Annual Report 2016–2017" (HC 655, Presented to Parliament pursuant to sections 2 and 3 of the Justice and Security Act 2013, Ordered by the House of Commons to be printed on 20 December 2017).

Charles W. Freeman, Jr., *Arts of Power: Statecraft and Diplomacy*, Washington, DC: United States Institute of Peace, 1997.

Committee on National Security Systems, (CNSS) Glossary, CNSSI No. 4009, April 6, 2015, p. 9. Retrieved from: https://www.cnss.gov/CNSS/openDoc.cfm?M0+zCfvO9T1o4xRsSJyX5Q==

Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land. The Hague, 18 October 1907.

Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, Protocol on Blinding Laser Weapons (As Amended on 21 December 2001), 10 October 1980, 1342 UNTS 137.

Cuba, Submission to the United Nations General Assembly Resolution A/58/373, (2003). https://disarmament-library.un.org/UNODA/Library.nsf/c793d171848bac2b85256d7500700384/b69c21ea9dcbb95785256dc10058b4c9/$FILE/sg58.373.pdf.

Danish Ministry of Defence, *Danish Defence Agreement 2010–2014*, (June 24, 2009), http://www.fmn.dk/nyheder/Documents/danish-defence-agreement-2010-2014-english.pdf.

Debora Plunkett, citted in Adam Shostack, The evolution of information security, The Next Wave, Vol. 19., No. 2, 2012, Retrieved from https://www.nsa.gov/resources/everyone/digital-media-center/publications/the-next-wave/assets/files/TNW-19-2.pdf.

Dictionary.com online. http://www.dictionary.com

Doctrine of Information Security of the Russian Federation, Approved by Decree of the President of the Russian Federation No. 646 of December 5, 2016.

EastWest Institute. James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko. “Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2, Issue 2.” The EastWest Institute, 2014. http://www.ewi.info/idea/critical-terminology-foundations-2

English Oxford Living Dictionaries Online. https://en.oxforddictionaries.com

Eric Talbot Jensen, and Sean Watts, "A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?" 95, no. 7 (June 2017): 1555-1578. *Business Source Premier*, EBSCO*host* (accessed April 29, 2018).

Ewen MacAskill, "US And UK Blame Russia For 'Malicious' Cyber-Offensive". *The Guardian*. https://www.theguardian.com/technology/2018/apr/16/us-and-uk-blame-russia-for-malicious-cyber-offensive.

Finland, Ministry of Defence, Secretariat of the Security and Defence Committee, *Finland's Cyber Security Strategy* (2013), 12. http://www.enisa.europa.eu/media/news-items/new-cyber-security-strategies-of-austria-finland-worldwide.

Finland. Prime Minister's Office Publications, *Government's Defence Report*. (16 February, 2017), https://www.defmin.fi/files/3688/J07_2017_Governments_Defence_Report_Eng_PLM_160217.pdf

FR Germany, Federal Ministry of the Interior, *Cyber Security Strategy for Germany* (February 2011), http://www.oed.com.nduezproxy.idm.oclc.org/view/Entry/240849?redirectedFrom=cyberspace#eid.

FR Germany. Bundesminister des Innern. *Cyber-Sicherheitsstrategie für Deutschland 2016*. (9 November, 2016.) https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf

France, Agence Nationale de la Securite des Systemes d'Information, *Information Systems Defence and Security: France's Strategy* (2011). http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world. Note: the 2015 strategy does not contain the definition of cyberspace.

France. Direction de l'information légale et administrative, *Livre blanc sur la Defense et la Securite nationale 2013, (April 29, 2013),* http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf.

General Assembly 68/98, *Developments in the field of information and telecommunications in the context of international security*, A/68/98, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (24 June 2013), available from https://undocs.org/A/68/98

General Assembly 70/174, *Developments in the field of information and telecommunications in the context of international security*, A/70/174, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (22 Juky 2015), available from http://undocs.org/A/70/174

Genrich Saulovich Altshuller, The Innovation Algorithm, TRIY Systematic Innovationa and Technical Creativity, Technical Innovation Center, Worchester, 2007, p. 86.

Gladman, Brian. "Wassenaar controls, cyber-crime and information terrorism." *Leeds, UK: Cyber-Rights & Cyber-Liberties (UK). September 1998.*

Global Internet Liberty Campaign, *Cryptography is a defensive tool, not a weapon*, A statement by the global internet liberty campaign, September 1998, Retrieved from http://www.cyber-rights.org/crypto/gilc-wass.htm

Goldsmith, Jack L., and Eric A. Posner. *The limits of international law*. Oxford University Press, 2005.

Harold Honhgu Koh, Legal Advisor of the U.S. Dep't of State "International Law in Cyberspace, Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18,2012", *Harvard International Law Journal Online* 54, December 2012 (2012): 13.

Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. "The law of cyber-attack." *California Law Review* (2012): 817-885, 826.

Herbert Lin, Fundamentals of Cyber Conflict, presentation, Stanford University, CS-203, May 23, 2017.

Herbert Lin, Fundamentals of Cyber Conflict, presentation, Stanford University, CS-203, May 23, 2017.

India, National Cyber Security Policy (2013), http://deity.gov.in/content/national-cyber-security-policy-2013-1.

International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 27032:2012, Information technology — Security techniques — Guidelines for cybersecurity* (Geneva, Switzerland: ISO/IEC, 2012).

International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC). (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary (ISO/IEC 27000:2018(en)). Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

ISO/IEC 27000:2018(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary

ISO/IEC 27000:2018(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

ISO/IEC 27039:2015(en), Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS). https://www.iso.org/obp/ui/#iso:std:iso-iec:27039:ed-1:v2:en

Israel. *Detering Terror: How Isreal Confronts the Next Generation of Threats*; English Translation of the Official Strategy of the Israel Defense Forces. Harvard Kennedy School: BELFER Center for Science and International Affairs, (August 2016), https://www.belfercenter.org/sites/default/files/legacy/files/IDFDoctrineTranslation.pdf.

ITU, *ITU Terms and Definitions*.

James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko, eds., *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2* (New York, NY: The EastWest Institute, 2014).

James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko, eds., *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2* (New York, NY: The EastWest Institute, 2014).

Japan, Government of Japan, *National Security Strategy* (2013), http://www.cas.go.jp/jp/siryou/.

John Costello, "China Finally Centralizes Its Space, Cyber, Information Forces," *The Diplomat*, January 20, 2016.

Justin McCurry, "South Korea spy agency admits trying to rig 2012 presidential election ".

https://www.theguardian.com/world/2017/aug/04/south-koreas-spy-agency-admits-trying-rig-election-national-intelligence-service-2012.

Karsten Geier, "Presentation of UN GGE Chair on the Inter-Regional Conference between OSCE and Asian Partners on Cyber/ICT" (presentation, Inter-Regional Conference between OSCE and Asian Partners on Cyber/ICT, Seoul, Republic of Korea, April 4, 2017).

Katsos, G. (January 10, 2018). Department of Defense Terminology Program. Joint Force Quarterly, No.88. http://ndupress.ndu.edu/Media/News/News-Article-View/Article/1413093/department-of-defense-terminology-program/.

Kevin L. Pollpeter, Michael S. Chase, Eric Heginbotham, The Creation of the PLA

Kim Zetter, Lily Newman, Brian Barrett, Louise Matsakis, and Andy Greenberg. "Why An Arms Control Pact Has Security Experts Up In Arms". Wired. https://www.wired.com/2015/06/arms-control-pact-security-experts-arms/. https://www.wired.com/2015/06/arms-control-pact-security-experts-arms/.

Kissel, Richard, ed. "Glossary of Key Information Security Terms." NISTIT 7298 Revision 2, National Institute of Standards and Technology (2013).

Lachow, Irving. "Cyber terrorism: Menace or myth." *Cyberpower and national security* (2009): 434-467.

Langner, Ralph. "To kill a centrifuge: A technical analysis of what stuxnet's creators tried to achieve." Online: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226, International Court of Justice (ICJ), 8 July 1996.

Malaysia, Ministry of Defence, *Malaysia's National Defence Policy.* (2010). http://www.mod.gov.my/images/mindef/lain-lain/ndp.pdf.

Malcolm Turnbull, 'Address to parliament: national security update on counter terrorism', 23 November 2016, transcript, https://www.pm.gov.au/media/address-parliament-national-security-update-counter-terrorism.

Marquis-Boire, Morgan, Bill Marczak, Claudio Guarnieri, and John Scott-Railton. *For their eyes only: The commercialization of digital spying.* Citizen Lab, 2013. https://citizenlab.ca/storage/finfisher/final/fortheireyesonly.pdf.

Matthijs R. Koot, "Progress of offensive cyber capabilities in the Netherlands' armed forces." https://blog.cyberwar.nl/2014/03/progress-of-offensive-cyber-capabilities-in-the-netherlands-armed-forces/.

Merriam-Webster online. from https://www.merriam-webster.com.

Michael N. Schmitt, "In defense of due diligence in cyberspace." The Yale Law Journal Forum, June 22, 2015, 125 (2015): 68.

Mitnick, Kevin D., and William L. Simon. *The art of deception: Controlling the human element of security.* John Wiley & Sons, 2011.

Mladenovic Dragan, Multidisciplinary Aspects of Cyber Warfare (in Serbian). Doctoral thesis, University of Belgrade, Belgrade, 2016, Available from http://nardus.mpn.gov.rs/handle/123456789/6880?show=full.

Monika B. Krizek, "The Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice." *BU Int'l LJ* 6 (1988): 337.

Morgenthau, Hans, and Politics Among Nations. "The struggle for power and peace." *Nova York, Alfred Kopf* (1948).

NATO, NATO Glossary of Terms and Definitions (English And French), AAP-06 Edition 2014 http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6EN.pdf.

Netherlands, Ministry of Defence, *The Defence Cyber Strategy* (2012), http://www.ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf.

Netherlands. Ministry of Defence. *The Defense Cyber Strategy.* (2015). https://zoek.officielebekendmakingen.nl/kst-33321-5.pdf.

Noah Shachtman, Peter W Singer, The wrong war: the insistence on applying Cold War metaphors to cybersecurity is misplaced and counterproductive, Brookings Institution, Washington DC, 15 August 2011, https://www.brookings.edu/articles/the-wrong-war-the-insistence-on-applying-cold-war-metaphors-to- cybersecurity-is-misplaced-and-counterproductive/.

Olivia Solon. "Police Crack Down On Silk Road Following First Drug Dealer Conviction". Wired.co.uk. http://www.wired.co.uk/article/silk-road-crackdown. http://www.wired.co.uk/article/silk-road-crackdown.

Organization for Secuirty and Co-operation in Europe, Permanent Council, Decision No. 1202, OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming From the Use of Information and Communication Technologies, 1092nd Plenary Meeting, PC Journal No. 1092, Agenda item 1, available from https://www.osce.org/pc/227281?download=true

Oxford English Dictionary.

Pawlak, Patryk ed. Institute for Security Studies Paris. "Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development". (2014). http://www.iss.europa.eu/uploads/media/Report_21_Cyber.pdf

Perry Pederson. "IT vs. ICS: An Attacker's Perspective," September 7, 2014. https://www.langner.com/2014/09/it-vs-ics-an-attackers-perspective/

Peterson, Dale. "Offensive cyber weapons: construction, development, and employment." *Journal of Strategic Studies* 36, no. 1 (2013): 120-124.

Peterson, Dale. "Offensive cyber weapons: construction, development, and employment." Journal of Strategic Studies 36, no. 1 (2013): 120-124.

Philippines, Submission to the United Nations General Assembly Resolution A/56/164, (2001). http://www.un.org/documents/ga/docs/56/a56164.pdf.

Poland, National Security Bureau. *National Security Strategy of the Republic of Poland.* (5 November, 2014), https://www.bbn.gov.pl/ftp/dok/NSS_RP.pdf.

Ponemon Institute and IBM Security, "*2017 Cost of Data Breach Study*", (June 2017). https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf.

Presidency of the Council of Ministers, Government of Italy, *National Strategic Framework for Cyberspace Security* (2013), https://www.ccdcoe.org/strategies-policies.html.

Radunovic, Vladimir. "Towards a secure cyberspace via regional cooperation". *DiploFoundation* (2017). https://www.diplomacy.edu//sites/default/files/Diplo-Towards_a_secure_cyberspace-GGE.pdf.

Rohan Pearce, "Cyber deterrent: PM talks up Australia's offensive capabilities", last modified April 21, 2016. https://www.computerworld.com.au/article/598443/cyber-deterrent-pm-talks-up-australia-offensive-capabilities/.

Romania, CERT Romania, "Resolution no . 271/2013 approving Romania's cyber security strategy and national action plan on implementation of the national cybersecurity (Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică)," CERT Romania, 2013, Retrieved from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf

Romania, Guvernul României, *Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetic,*(23 May, 2015), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf.

Russia, Submission to the United Nations General Assembly Resolution G.A. Res. 54/213, U.N. Doc. A/RES/54/213 (August, 10, 1999), https://disarmament-library.un.org/UNODA/Library.nsf/f4c497d5f90e302d85257631005152d2/fae7e8060174f22c8525764e0051ce60/$FILE/A-54-213.pdf. p. 10.

Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press, 2017, https://www.ccdcoe.org/strategies-policies.html.

Schwartz, Mattathias. "Cyberwar For Sale". New York Times online. https://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html?smi=%20d=3Dtw-share&_r=1&mtrref=undefined.

Shehadeh, Karim K. "The Wassenaar Arrangement and Encryption Exports: An Ineffective Export Control Regime that Compromises United States Economic Interests." *Am. U. Int'l L. Rev.* 15 (1999).

Shirey, Robert, IETF Network Working Group, Internet Security Glossary, Version 2. https://tools.ietf.org/html/rfc4949.

South Africa. Ministry of Defence and Military Veterans, South African Defence Review 2015, (2016.), http://www.dod.mil.za/documents/defencereview/defence%20review%202015.pdf.

State Council of the People's Republic of China, China Military Strategy, May 2015. Retrieved from http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm.

Strategic Support Force and Its Implications for Chinese Military Space Operations, RAND, 2017, Santa Monica, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2058/RAND_RR2058.pdf

Sweden, Government Offices of Sweden, *Sweden's Defence Policy 2016 to 2020*. (1 June, 2015), http://www.government.se/globalassets/government/dokument/forsvarsdepartementet/sweden_defence_policy_2016_to_2020.

Switzerland. Département fédéral de la défense, de la protection de la population et des sports (DDPS), *PLAN D'ACTION CYBERDEFENSE DDPS (PACD)*, (09 September, 2017), from https://www.vbs.admin.ch/content/vbs-internet/fr/die-schweizer-armee/schutz-vor-cyber-angriffen.download/vbs-internet/fr/documents/defense/cyberattaques/Aktionsplan-Cyberdefense-f.pdf.

Switzerland, Federal Department of Defence, Civil Protection and Sport DDPS, *National strategy for the protection of Switzerland against cyber risks* (2012), https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf.

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies And Munition List, WA LIST (98) 1, (03-12-98).

https://www.wassenaar.org/app/uploads/2015/06/Previous/1998_OK/WA-LIST%20%2898%29%201.pdf

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, (2013), https://www.wassenaar.org/app/uploads/2015/06/Previous/2013_OK/WA-LIST%20%2813%29%201.pdf

Tom Jowitt, "UK's Offensive Cyber Warfare Ability 'More Than Doubles", Silicon UK. https://www.silicon.co.uk/e-regulation/governance/uks-cyber-warfare-ability-226365.

U.S. Department of Defense, "All Cyber Mission Force Teams Achieve Initial Operating Capability." U.S. Cyber Command News Release, https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/.

U.S. War Department. (January 15, 1945). Russian Military Dictionary. War Department Technical Manual (TM 30-544). Washington, D.C., p. 296.

UK Government. National Cyber Security Strategy 2016-2021. (2016.) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

UN Charter

UN General Assembly, Resolution 58/32 adopted by the General Assembly on 8 December 2003, Developments in the field of information and telecommunications in the context of international security, A/RES/58/32 of 18 December 2003. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/58/32

United Kingdom Ministry of Defence, Development, Concepts and Doctrine Centre. Cyber Primer, Second Edition, 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf.

United Kingdom, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, (United Kingdom, UK Cabinet Office, 2011), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

US, Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies, "Explore Terms: A Glossary of Common Cybersecurity Terminology" ND. Available from http://niccs.us-cert.gov/glossary.

US Department of Defense, Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934. (November 2011), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf.

US DoD Office of the Secretary of Defense, Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2017, https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF?ver=2017-06-06-141328-770 .

US DoD. Joint Publication JP 3-12 (R), Cyberspace Operations. p. v. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf.

William R. Marczak, John Scott-Railton, Morgan Marquis-Boire, and Vern Paxson. "When Governments Hack Opponents: A Look at Actors and Technology." In *USENIX Security Symposium*, pp. 511-525. 2014. https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-marczak.pdf.

Министерство иностранных дел Российской Федерации. *Военная доктрина Российской Федерации*. (26 December, 2014.), Retrieved from http://www.mid.ru/documents/10180/822714/41d527556bec8deb3530.pdf/d899528d-4f07-4145-b565-1f9ac290906c

Министерство обороны Российской Федерации (Минобороны России), *Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве* (2011), http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle (preuzeto 18. mart 2015).

Президент Российской Федерации, Военная доктрина Российской Федерации, December 25, 2014, No. Pr.-2976 11, http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf.

Совет Федерации, Федералыного Собрания Российской Федерации, *Концепция стратегии кибербезопасности Российской Федерации - Проект*, (10 января 2014), 2, http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf.

APPENDIX A

List of States with Declared Offensive Cyber Capabilities

COUNTRY	QUOTE SIGNALLING OCC	DOCUMENT
Australia	Australia's defensive and **offensive cyber capabilities** enable us to deter and respond to the threat of cyber attack. (p. 28)	Australia's cyber security strategy - Enabling innovation, growth & prosperity
Austria	The term "cyber defence" refers to all measures to defend cyber space **with military and appropriate means** for achieving military-strategic goals. Cyber defence is an integrated system, comprising the implementation of all measures relating to ICT and information security, the capabilities of milCERT and CNO (**Computer Network Operations**) as well as the **support of the physical capabilities of the army**. (p. 22)	Austrian Cyber Security Strategy
Belgium	The scope of this document is the following: (1) Defining a strategic framework for the Belgian Defence approach of cyber security consisting of three pillars: Cyber Defence, Cyber Intelligence and Cyber Counter-Offensive. (p. 4)| **Cyber Counter-Offensive** (Reference document: act of 30 November 1998) "Within the framework of cyber-attacks on military computer and communications systems or systems managed by the Minister of Defence, neutralise the attack and identify its perpetrators, without prejudice to the right to respond immediately with a **counter cyber-attack** in accordance with the provisions of the law of armed conflict." (p. 18)	Cyber Security Strategy for Defence
Brazil	(Translation) Cyber Defense - set of **offensive**, defensive and exploratory actions in the cyberspace, on the strategic level of national planning, coordinated and integrated by the Ministry of Defense, with the aim to protect the information systems of interest to the National Defense, **to obtain data for the intelligence production and to compromise the information systems of the opponent**. (p. 18)	Doutrina Militar De Defesa Cibernética
Canada	The **active cyber operations** aspect of the Establishment's mandate is to carry out activities on or through the global information infrastructure to **degrade, disrupt, influence,**	BILL C-59. An Act respecting national security matters.

	respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security. (p. 61)	
Denmark	Cyberspace has, in other words, become a battlespace. This development therefore places increasing demands on the ability of the Danish Armed Forces to take defensive and **offensive measures** in cyberspace. On this basis, there is agreement that a Computer Network Operations (CNO) capability under the auspices of the Danish Ministry of Defence should be established with the aim of defending the ministry's own use of cyberspace and preventing opponents from exploiting it. (p. 11)	Danish Defence Agreement 2010–2014
Finland	Cyber-security: The national defence related sector of cyber security which incorporates the **capabilities of intelligence, surveillance, cyberattack** and cyber defence. (p. 34)	Government's Defence Report
France	(Translation) Within this national doctrine, **the offensive computer capacity, associated with an intelligence capacity**, contributes significantly to the cybersecurity posture. It contributes to the characterization of the threat and the identification of its origin. It also makes it possible to anticipate certain attacks and configure the defenses accordingly. **Offensive computing capacity** enhances the range of options available to the state. It has different stages, more or less reversible and more or less discreet, proportionate to the scale and severity of attacks. (p. 107)	Livre blanc sur la Defense et la Securite nationale 2013
Germany	(Translation) Cyber-defense comprises of defensive and **offensive capabilities** in the Bundeswehr within their constitutional mandate and the international legal framework for working in cyberspace, which are suitable and necessary for operational management or for the defense against (military) cyber attacks and thus the protection of own information, IT, as well as weapons and systems of action. (p. 24)	Cyber-Sicherheitsstrategie für Deutschland 2016
Israel	Defense and **attack in cyberspace** Capabilities enable: • Utilization of intelligence • Continuity of performance • Networking enabling cooperation • Logistics response	Detering Terror: How Isreal Confronts the Next Generation of Threats; English Translation of the

	• Investigation and learning • Operating in a coalition • Influence on perception • Achieving legitimacy • Legal response (pg. 38)	Official Strategy of the Israel Defense Forces
Malaysia	The development of a **cyber-warfare capability** is an important step towards counterbalancing the ability of other countries in the region and to defend important national targets from all forms of threats. It is important to stop any form of encroachment into national defence's computer systems and networks. Concurrently, it also provides the room for **developing offensive capabilities for conducting cyberoperations** when necessary. This capability would provide room for information fathering at strategic, operational and tactical levels. (pg. 13)	Malaysia's National Defence Policy
Poland	The cyberspace has become another area of armed struggle. The Armed Forces of the Republic of Poland must have defensive and **offensive capabilities** in this domain in order to perform the function of deterrence to potential opponents. (p. 32)	National Security Strategy of the Republic of Poland
Romania	(Translation) Computer network operations - complex planning, coordination, synchronization, harmonizing and **deploying cyber-space activities** for protection, control and security the use of computer networks in order to obtain informational superiority, concurrently with **neutralizing the opponent's capabilities**; (p. 7)	Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică
Russia	(Translation) The tasks of equipping the Armed Forces, other troops and bodies with **weapons**, military and special equipment: [...] development of the **forces and means of information confrontation**. (p.23)	Военная доктрина Российской Федерации
South Africa	The Chief of the Defence Force's ICS staff are responsible to plan, orchestrate, direct and control common defence information and communication systems through, inter	Ministry of Defence and Military Veterans, South

	alia, the provision of logistic policy, doctrine, functional and competency standards and standardisation and training curricula. This will be achieved through: […] d. Defensive and **offensive information warfare**. […] (p. 265)	African Defence Review 2015
Sweden	Cyber defence capabilities are an important part of the Swedish Defence. Vital systems must be protected from attack. This also requires the **ability to carry out active operations in the cyber domain**. (p. 5)	Sweden's Defence Policy 2016 to 2020
Switzerland	Cyber Defense: Set of measures to detect, identify and respond to threats and attacks against ICT systems and infrastructures, if necessary by **offensive countermeasures**. Actions in Cyberspace: A set of actions taken against an adversary in cyberspace to **acquire information or to undermine the availability or integrity of its ICT systems or infrastructure**. (p. 8)	Plan D'action Cyberdefense DDPS (PACD)
The Netherlands	(Translation): By **offensive cyber capabilities**, the MoD means digital means that have as purpose to influence or deny enemy action. This takes place through **infiltration of computers, networks, and weapon and sensory systems** to influence information and systems.	Defensie Cyber Strategie (2015)
UK	We have the means to take **offensive action in cyberspace**, should we choose to do so. (p. 9)	National Cyber Security Strategy 2016-2021
USA	[…] the Department has the **capability to conduct offensive operations in cyberspace** to defend our Nation, Allies and interests. (p. 5)	Department of Defense, Cyberspace Policy Report A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934 November 2011

REFERENCES

Australian Government. *Australia's cyber security strategy: enabling innovation. growth & prosperity*. 21 April, 2016. https://cybersecuritystrategy.pmc.gov.au/assets/pdfs/dpmc-cyber-strategy.pdf

Federal Chancellery of the Republic of Austria. *Austrian Cyber Security Strategy. 2013.* http://archiv.bundeskanzleramt.at/DocView.axd?CobId=50999

Belgium. Defence Strategy Department. *Cyber Security Strategy for Defence*. 30 September, 2014. https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf

Brazil. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas*. Doutrina Militar de Defesa Cibernética.* 18 November, 2014. http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf

House of Commons of Canada. *BILL C-59 An Act respecting national security matters*. June 30, 2017. http://www.parl.ca/Content/Bills/421/Government/C-59/C-59_1/C-59_1.PDF

Danish Ministry of Defence. *Danish Defence Agreement 2010–2014*. June 24, 2009. http://www.fmn.dk/nyheder/Documents/danish-defence-agreement-2010-2014-english.pdf

Prime Minister's Office Publications. *Government's Defence Report*. 16 February, 2017. https://www.defmin.fi/files/3688/J07_2017_Governments_Defence_Report_Eng_PLM_160217.pdf

Direction de l'information légale et administrative. *Livre blanc sur la Defense et la Securite nationale 2013. April 29, 2013.* http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf

Bundesminister des Innern. *Cyber-Sicherheitsstrategie für Deutschland 2016*. 9 November, 2016. https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf

Detering Terror: How Isreal Confronts the Next Generation of Threats; English Translation of the Official Strategy of the Israel Defense Forces. Harvard Kennedy School: BELFER Center for Science and International Affairs. August 2016. https://www.belfercenter.org/sites/default/files/legacy/files/IDFDoctrineTranslation.pdf

Malasya. Ministry of Defence. *Malaysia's National Defence Policy*. 2010. http://www.mod.gov.my/images/mindef/lain-lain/ndp.pdf

Poland. National Security Bureau. *National Security Strategy of the Republic of Poland.* 5 November, 2014. https://www.bbn.gov.pl/ftp/dok/NSS_RP.pdf

Romania. Guvernul României. *Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetic.* 23 May, 2015. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf

Министерство иностранных дел Российской Федерации. *Военная доктрина Российской Федерации*. 26 December, 2014. http://www.mid.ru/documents/10180/822714/41d527556bec8deb3530.pdf/d899528d-4f07-4145-b565-1f9ac290906c

Ministry of Defence and Military Veterans. South African Defence Review 2015. 2016. http://www.dod.mil.za/documents/defencereview/defence%20review%202015.pdf

Sweden. Government Offices of Sweden. *Sweden's Defence Policy 2016 to 2020*. 1 June, 2015. http://www.government.se/globalassets/government/dokument/forsvarsdepartementet/sweden_defence_policy_2016_to_2020

Département fédéral de la défense. de la protection de la population et des sports DDPS. *PLAN D'ACTION CYBERDEFENSE DDPS PACD*. 09 September, 2017. https://www.vbs.admin.ch/content/vbs-internet/fr/die-schweizer-armee/schutz-vor-cyber-angriffen.download/vbs-internet/fr/documents/defense/cyberattaques/Aktionsplan-Cyberdefense-f.pdf.

Ministry of Defence. *Defensie Cyber Strategie*. 2015. https://zoek.officielebekendmakingen.nl/kst-33321-5.pdf

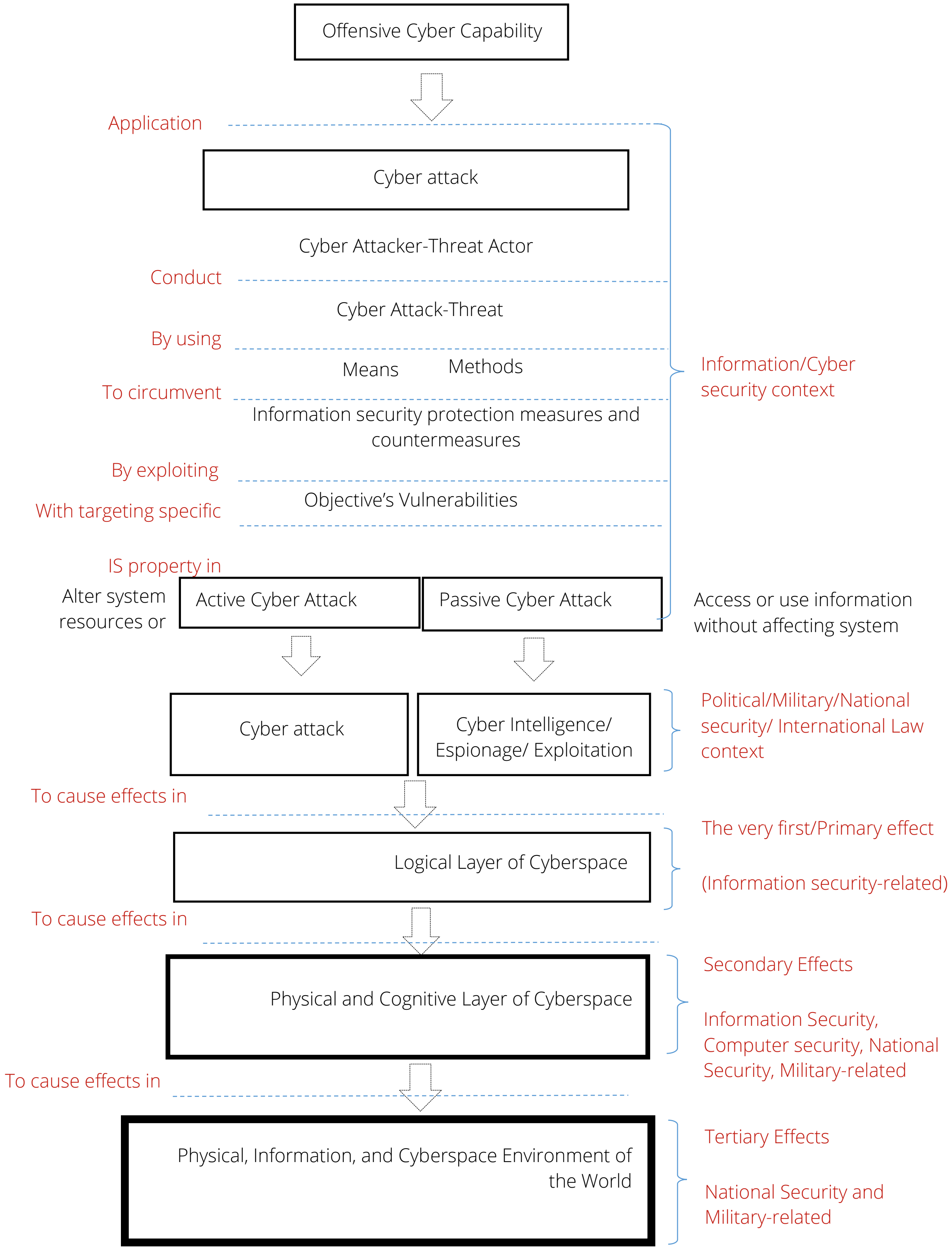
UK Government. *National Cyber Security Strategy 2016-2021.* 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

US Department of Defense. Department of Defense Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011. Section 934. November 2011. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf

APPENDIX B

Conceptual Model of the Offensive Cyber Capabilities Application

Dragan Mladenovic, Ph.D.


Offensive Cyber Capability
Application
Cyber attack
Cyber Attacker-Threat Actor
Conduct
Cyber Attack-Threat
By using
Means
Methods
To circumvent
Information security protection measures and countermeasures
By exploiting
Objective’s Vulnerabilities
With targeting specific
IS property in
Information/Cyber security context
Alter system resources or
Active Cyber Attack
Passive Cyber Attack
Access or use information without affecting system
Cyber attack
Cyber Intelligence/ Espionage/ Exploitation
Political/Military/National security/ International Law context
To cause effects in
Logical Layer of Cyberspace
The very first/Primary effect
(Information security-related)
To cause effects in
Physical and Cognitive Layer of Cyberspace
Secondary Effects
Information Security, Computer security, National Security, Military-related
To cause effects in
Physical, Information, and Cyberspace Environment of the World
Tertiary Effects
National Security and Military-related

MEMO 5
RETHINKING THE ATTRIBUTION PROBLEM - A PLAUSIBLE PROOF OF NON-INVOLVEMENT AS AN ALTERNATIVE TO CREDIBLE ATTRIBUTION

Thomas Reinhold, Fellow, Institute for Peace Research and Security Policy, Hamburg

MEMO № 5

ATTRIBUTION IN CYBERSPACE - ITS NECESSITY AND CHALLENGES

Over the past years, influence, espionage or disruptive operations in cyberspace have increasingly become a threat to states and international security. While practical measures of enhancing the IT security and fostering secure hardware and software had been taken, the answer to how to adequately respond to cyber attacks did not advance accordingly and came to a stop at the challenge of identifying the adversaries. This is so-called "attribution". In terms of rules and norms of responsible state[475] behaviour it is one of the main requirements for nations right of self-defence under article 51 of the UN Charter[476]. An armed attack needs to be credibly attributed to its origin by the attacked nation in order to permit the "inherent right of individual or collective self-defence" by appropriate countermeasures. Attribution is meant to supply valid empirical information that proves the involvement of the accused state in a specific incident. While identifying the source of an armed attack is possible for weapons like missiles or conventional military forces, many declare it as impractical for cyber attacks[477] considering the short time frame for defensive reactions and the technical difficulties, as described below. The report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) from 2015 even pointed out that "the accusations of organizing and implementing wrongful acts brought against states should be substantiated", which is seen as a statement against any kind of "probability driven approach"[478]. This "attribution problem" is currently supposed to be one of the core obstacles when it comes to applying and enforcing the established rules and norms of responsible state behaviour to cyberspace. The difficulties with attribution in cyberspace are based on some specific technical features of this domain that differ from the physical domain, and the resulting way in which cyber attacks are performed will be addressed in the following section.

TECHNICAL PROPERTIES OF CYBERSPACE

Cyberspace[479] is a "virtual" domain by design that abstracts a space from a specific real geographic location. It consists of autonomous, self-contained networks that integrate and connect groups of different IT systems, whereas each network itself can consist of smaller sub-

[475] The terms "nation" and "state" are used synonymously in this text for better legibility

[476] See exemplary L. Grosswald "Cyberattack Attribution Matters Under Article 51 of the U.N. Charter", Brooklyn Journal of International Law, Volume 36 / Issue 3, 2011

[477] For example, see : UNIDIR, Report of the International Security Cyber Issues Workshop Series, 2016.

[478]https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html

[479] The cyberspace has many definitions and is referred to by different terms. This paper refers to the definition of this domain as pointed out in the Convention on Cybercrime of the Council of Europe from 2001 (ETS No. 185). The convention defines this space as the entity of computer systems ("any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data"), computer data ("any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function"), service providers ("any public or private entity that provides to users of its service the ability to

communicate by means of a computer system and any other entity that processes or stores computer data on behalf of such communication service or users of such service") and traffic data ("any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service") networks. The networks are connected to each other via so-called gateway servers[480]. To perform any kind of data transmission between two systems, it is necessary to identify an IT system, which is done by using a technique named "IP addressing".[481] It is important to understand that the address of any IT system - in the following called (A) - is not necessarily unique. It must only be distinct within the network to which the system is directly connected, called N(A)[482] in the following. Any connection of (A) to an external IT system (B) that is not part of N(A) is transferred over the gateway servers that connect the networks N(A) and N(B). Among other functions, the gateway servers of N(A) and N(B) handle the necessary "address translation"[483]. This means the effective sender address that (B) is able to identify is the unique address of the gateway server of N(A). This technological construction of cyberspace means that from the perspective of the receiver of any data connection – or, in the scenario of cyber attacks, the attacked system - there is no clear and directly "visible" path to the origin of the connection. In practical scenarios, this address translation is performed over multiple networks which further "blurs" the force of expression of the sender address that (B) can identify. This aspect also means any kind of geographical localising based on IP addresses[484] will reveal only one of the involved networks, but not necessarily the network N(A) and in no case the specific IT system (A).

Another aspect of the technological basics of cyberspace is that it abstracts the process of data transmission between IT systems over different structural and conventional layers, and generalising specific functionalities with technical protocols. All IT systems that communicate over cyberspace have to use these common technical principles - whether these are military systems or not. From a technical perspective, exemplary sending an email uses the same technologies as triggering malicious malware that deletes a foreign hard-drive and crashes the IT system. Both tasks are performed by creating connections, sending technical instructions and responding to answers from foreign IT systems. Any IT system is theoretically capable of performing these tasks. In other words, there is no coercive connection between the observed usage of an IT system - like a cyber attack - and its real-world and intended purpose. A popular example for this case is the overused, but conceptionally still valid case of the misusage of IT systems in a hospital that had

[480] Another, more commonly used term is "router" which is technically not fully correct. The term router is used for any device within a network that connects its parts and transmits data between other devices within this network. On the other hand, the gateway servers are on the "boundaries" of a network and specifically responsible for the data transmission between different networks.

[481] IP stands for" Internet Protocol" which is the standard for transmitting data between IT systems over worldwide interconnected networks.

[482] This is a technical necessity of the quite old, but still used internet protocol address system IPv4 that limits the overall amount of unique addresses. Theoretically the newer and currently deployed internet protocol called IPv6 does not have this limitation and any IT device could have an worldwide unique ID. On the other hand, even IPv6 provides measures to mask this unique ID for privacy reasons and until all IPv4 networks are changed over to IPv6 the non-uniqueness of IP addresses will stay an important issue to consider. For an in-depth argumentation see e.g. B. Cole "Is the End of IPv4 at Hand? Not Anytime Soon… - IPv4 still has a long life ahead", EE Times, https://www.eetimes.com/author.asp?section_id=36&doc_id=1327058

[483] This is performed by a technique called NAT - Network address translation - which "masks" the addresses of a network's IT systems for connections to "outer" network structures. NAT was considered a relic from the old IPv4 technology and is theoretically not necessary for IPv6. Nevertheless, some IT experts argue that NAT must also be considered a security feature that still is important to consciously disguise the infrastructure and topology of a network. Beside the still ongoing transition phase from IPv4 to IPv6 that requires NAT, this feature could "survive" for security reasons. See e.g. F. Gont "Why IPv6 won't rid the Internet of Network Address Translation", https://searchenterprisewan.techtarget.com/tip/Why-IPv6-wont-rid-the-Internet-of-Network-Address-Translation

[484] IP-based geographic localisation is performed via official information provided by Internet service providers (ISP) and managed by so called Regional Internet Registries (RIR) that coordinate all networks for a respective service region.

been hacked to carry out cyber attacks. Even a forensically "waterproof" identification of an attack's origin cannot exclude the possibility that the identified IT system has been taken over by adversaries, and that any offensive countermeasure against this system could potentially have incalculable consequences.

The third principle of cyberspace that is part of its functionality "by design" is its distributed character, which is meant to make it robust. Any data transmitted during connections between two distant IT systems (A) and (B) is split up into a large number of small packets that are sent separately and merged at their destination. The path - in technical terms the "route" - between the networks N(A) and N(B) is not straight but consists of numerous other networks with "main roads and side streets"[485], where each transmitted package can potentially take a different route. This principle guarantees that disruptions of "main roads" can be balanced out by other transmission paths, and that the loss of transmitted data can be detected and compensated. In the context of cyber attacks, this means that re-tracing the steps of attacks to their origin equals finding the path back over multiple networks and routes.

ATTRIBUTING CYBER ATTACKS AND THE AMBIGUITY OF DIGITAL DATA

Drawing from those three technical features, many real-world cyber attack scenarios involve multiple steps of intermediary hubs of overtaken IT systems used to blur the tracks.[486] This often involves the usage of one or more so-called "command and control" servers (C2 or C&C) that are used by attackers to coordinate the progress and to collect stolen data. These servers are either hijacked systems or rented servers that do not belong to the attackers. Sometimes these servers themselves are controlled by external communication channels like a Twitter account or chat channels which are "listening for commands". The task of attributing such an attack would involve the analysis of at least some of the IT systems used as hubs, as well as the C2 infrastructure and using other diverse sources and tools like malware reversal and forensics and information from intelligence services or trusted third parties for circumstantial attribution to "encircle" the origin of an attack. Aside from the necessary time to perform these actions, each step potentially relies on the cooperation of other states to gather information from concerned systems within their jurisdiction, as well as the availability of logged information about user interactions and connections to and from other IT systems[487] on these hubs or other data samples.

[485] This metaphor reflects that the cyberspace indeed consists of big and important routes like the so-called internet backbone with high data flow rates and cable capacities, but that there are also smaller and alternative routes. A good example that illustrates this are the maps of submarine internet cables which can be found under https://www.submarinecablemap.com. Additional routes are provided by other technologies such as land-based cables or via satellite transmission.

[486] A good example is provided by the US cyber security company Mandiant's 2013 report "APT1 Exposing One of China's Cyber Espionage Units" that collects and analyses information of multiple cyber attacks against US companies which led to the revelation of the Chinese state driven cyber espionage unit PLA 61398, https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html

[487] For an in-depth analysis of the attribution problem in the context of inter-state cyber conflicts, see "Attributing cyber attacks" by T. Rid & B, Buchanan, 2015, Taylor & Francis or "The attribution of cyber warfare" by N.C. Rowe, 2015.

In the context of this paper, it is important to stress that the discussed specific features of cyberspace that hinder attribution also create a strong character of ambiguity. Available information on attacks and the traces of the offenders are either incomplete or inconclusive in terms of its interpretation. It also must be considered that digital information is easy to manipulate, and that attackers might have created false tracks by forging misleading evidence, commonly described as "false flags". On the other hand, cyber attacks against critical systems might need immediate decisions about counter measures to stop the threat. The situation is even more tense due to the several national approaches of establishing offensive cyber capabilities[488] and the lack of international binding norms for responsible state behaviour in this domain, or even a common agreement on the concept of security in cyberspace[489]. These circumstances raise the risk of misunderstandings, miscalculations and misinterpretations that could lead to wrong responses, especially if other means of crisis communication or security and trust-building measures between the adversaries are missing.

RETHINKING ATTRIBUTION: CONCEPTUAL OUTLINE FOR A SYSTEM OF PLAUSIBLE PROOF OF NON-INVOLVEMENT

The previous chapter showed that attributing a cyber attack is a complex task that can easily be brought to a halt for different reasons. The potential for a wrong attribution is high and, even under optimal conditions, it's a time-consuming task with a high amount of political pressure, especially for scenarios of an ongoing cyber attack against a state with the necessity for an appropriate response that averts the threat. Based on this, this chapter will propose a concept that, even though it cannot help diminish the "burden of proof" of the cyber attack victim, aims to help reduce the threat of a conflict escalation by mistake. The concept is seen in the sense of the CSCE Helsinki final act that recognised "the need to contribute to reducing the dangers of armed conflict and of misunderstanding or miscalculation of military activities which could give rise to apprehension, particularly in a situation where the participating States lack clear and timely information about the nature of such activities"[490] as well as the adjacent statement of the UN General Assembly on confidence and security building measures that should help "reduce and even eliminate the causes of mistrust, fear, misunderstanding and miscalculations with regard to relevant military activities and intentions of other States"[491]. Such a form of escalation reduction can be achieved if an accused state is able to plausibly prove their non-involvement in a specific attack or any other kind of cyber operation against the accusing nation. This requires the supply of tamper-proof empirical data on the cyber activities of the accused state with regard to the following parameters:

[488] For example, see "The Cyber Index - International Security Trends and Realities", UNIDIR, 2013

[489] As an example, see the difference between the Russian and Chinese concept of "information security" versus the US and European concept of "IT security" as desirable state for the cyberspace, or the recent failure of the last UN GGE as analysed in "The Alleged Demise of the UN GGE: An Autopsy and Eulogy" by E. Tikk & M. Kerttunen, 2017.

[490] Conference on security and co-operation in Europe Final Act, Helsinki 1975.

[491] General Assembly, Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmament, UN document A/S-15/3, 28 May 1988, pp. 28–33.

- The information must contain all incoming and outgoing relevant network connections of the accused state (as specified in the next points) to or from all networks of the accusing state that had been involved in the cyber attack, and to or from the IT systems that had been targeted. In addition, similar information about connections to networks or IT systems of third parties that are suspected to have been used as C2 infrastructure or any other kind of indirect attack controlling measure must be included.
- The above information must be supplied for the incoming and outgoing connections of a defined scale of networks that are under the jurisdiction of the accused state. This scale is defined by the attacked nation and is regarded as sufficient to prove the non-involvement. The scale can range from activities of all military or national intelligence networks to theoretically a nationwide network coverage.
- The information must be supplied for the time slots of the cyber attacks or the malicious activities. These time slots are defined by the attacked nation.

The information could either be supplied voluntarily by a state, or as response to a request by an accusing party or entrusted instance. The provided information can be anonymised to a degree that allows proof of non-involvement in a specific attack to be established while filtering out other irrelevant data or disguise secret information. Based on this kind of information, either the accusing party or a neutral third party would be able to assess the provided data. Instead of tracing back the path to the alleged attacker, the validation will be able to directly focus on the supposed origin of the attack path and therefore be able to validate a statement of non-involvement. As already pointed out, this will not reveal the identity of the actual offender, but can help to relieve the supposed attacker to a certain degree. The third chapter will further outline the technical specifics and necessary measures of such a system. The next section presents an analysis of inter-state conflict scenarios where these technical means of escalation reduction can be applied in a theoretical model, as well as a short analysis of two actual cases.

SCHEMATIC SCENARIO FOR USE CASES

As outlined in the introduction, the proposed measures are thought to foster the reduction of miscalculations and misinterpretations. The theoretical model of a representative scenario is therefore set in a crisis situation between two states (A) and (B) with a high potential for conflict escalation. Based on this, the model scenario contains the following events:

1. State (A) detects an incident, referred to as (x) in the following, either by own cyber defensive measures, the work of domestic intelligence agencies or by support of a third party, that is either[492]:
   a) An espionage activity: Detected by anomalies in terms of missing or corrupted digital data, stolen secrets, unauthorised access to specific IT systems or malware on internal IT systems

[492] It is important to note that until now there isn't any international binding definition of cyber attacks. Often the term is used for different incidents from disabling operations and espionage to disruptive and destructive operations. For this paper and its argumentation it is only relevant to distinguish between data theft versus IT disruptions rather than discussing the term cyber attack. A good differentiation on this behalf is given by G. D. Brown & O. W. Tullos in "On the Spectrum of Cyberspace Operations", Small Wars Journal, 2012

   b) An offensive cyber attack: Detected by harmful software activities against state-level critical IT systems.
2. Entitled authorities of state (A) are checking the logged information as well as the technical integrity of the affected IT systems and detecting unauthorised access to these systems from a foreign source over a time frame further called "T(x)"[493]. "Foreign" is understood in terms of "not belonging to any authorised part of the networks of state (A)".
3. The authorities of state (A) identify the unauthorised access from an IP address IP(x) that is registered to a third party and located[494] in an uninvolved state (C)[495].
4. Due to specific circumstances, the authorised agencies of state (A) are not able to trace back the path from (x). Possible reasons for this situation, as discussed before, are:
   a) The short reaction time that is available to decide on counter measures by state (A)
   b) The refusal of state (C) to provide further information stored on the identified systems
   c) The absence of valid logging information either on the identified systems of state (C) or on further intermediary steps.

   This situation reflects the possibilities of an attacker to hide activities as well as the problems with uncertainty and miscalculation based on missing or fragmentary data.
5. State (A) accuses state (B) of being the agent behind the incident (x) with reference to the political background situation, former incidents or former aggressive announcements by state (B) without publicly providing undeniable evidence. To bring the harmful cyber activities to an end, state (A) signals the willingness to use strong political or economic measures (the most likely reaction in the espionage scenario) or military force (more likely reaction in the cyber attack scenario).

In terms of the described scenario, the underlying question of this proposal is by what kind of information and by which technical measures state (B) can credibly prove that none of their IT systems had any connection to the identified system for IP(x) for the time frame T(x) of the incident. The third chapter will propose and discuss such measures, the possible levels of certainty, as well as potential pitfalls.

REAL-WORLD USE CASES

When it comes to cyber attacks or espionage that are supposedly carried out or orchestrated by a state and its institutions it is hard to get solid facts about the things that happened, the targets, the data loss, and the tactics. Most of the information comes from public announcements, media and, in a few cases, later published technical reviews of IT security companies that had been involved in the analytic process. Nevertheless, the following two examples should help illustrate the scenario described above with regard to these limitations.

[493] It is important to note that the detected time frame of an attack and the first observable hacking operation can exceed the stored information on the affected IT systems. Especially so-called advanced persistent threats often infiltrate IT systems but stay hidden until activated to perform their task.

[494] The geographical localisation (in short "geolocation") is usually based on the information that are available via the Regional Internet Registries (RIR).

[495] Concerning the described scenario, it should be assumed that state (C) is really uninvolved. With regard to common attacks schemas, this is most likely also a practical assumption.

A. The cyber attack against chemical plants in Saudi Arabia, August 2017[496]

In August 2017 a cyber attack was detected at a petrochemical plant that targeted the industrial control systems[497] which monitors, controls and regulates all the different aspects of the industrial process. In contrast to former attacks against such systems that often tried to silently manipulate the controlled processes, the aim of the detected attack presumably was to deliberately destroy the industrial hardware by triggering explosions. This would most likely have produced significant damage to the plant as well as possible human injuries or losses. The available public information is that the malware did not work due to a programming mistake by the attackers, whose advance, tactics and alleged resources point at a state agent. Investigators blamed Iran for the attack due to former events and alleged hacking attacks against governmental institutions[498] and industrial facilities[499], as well as overall political tensions[500]. On the other hand, the official attribution of the attack against the petrochemical plant is not as conclusive as it needs to be, and other nations like China, Russia, the United States and Israel, maybe even North Korea, are presumably able to perform similar cyber attacks. Press reports suggested that the investigators feared an immediate second attempt of sabotage if the first attempt failed, and that the company therefore had to decide quickly if and how to respond, whereas official communication channels between the nations that might have been used for direct communication are scarce since an attack on the Saudi Embassy in Tehran in 2016[501]. This situation illustrates the introduced scenario very well due to its lack of significant evidence and political crisis communication channels. Thankfully, it did not lead to an offensive reaction.

B. The cyber attack against the Ukraine power grid, December 2015[502]

A second illustrative example is the cyber attack against up to five power supply companies in the Ukraine that took place on December 23rd, 2015. The attack itself targeted control systems of the power plants and their supply infrastructure as well as the call-center services of the companies that shut down any customer information possibilities. In total, up to 230.000 people had been cut off from electricity for one to six hours. The attack happened in the context of the ongoing crisis between Ukraine and the Russian Federation and had been immediately attributed to hackers from Russia based on the geolocation of the attackers' IP addresses. As argued above, this is no valid proof at all and - due to its obvious character in these times of political crisis - could have been a put out of false tracks by attackers from a third party. The second example demonstrates the ambiguity of available information when analysing cyber attacks.

[496] https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

[497] Such systems are often summed up by the term SCADA that stands for "Supervisory Control and Data Acquisition" (https://en.wikipedia.org/wiki/SCADA).

[498] As an example, see https://www.thetimes.co.uk/article/iranians-blamed-for-saudi-cyberattack-nmrjhj3xj

[499] See the hacking attack from 2012 with a malware called Shamoon against the Saudi company Aramco.

[500] See a detailed excursion at "Why Saudi Arabia and Iran are bitter rivals", BBC http://www.bbc.com/news/world-middle-east-42008809

[501] https://en.wikipedia.org/wiki/Iran–Saudi_Arabia_relations

[502] https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack

Both examples illustrate the described ambiguity of attributing cyber attacks and situations, where the overall political scenario suggests obvious answers to the question of the attacks' origin. In both cases, no verifiable information had been published that would allow an independent analysis of the attack.

TECHNICAL OUTLINE FOR A SYSTEM OF PLAUSIBLE PROOF OF NON-INVOLVEMENT

CONCEPTUAL AND TECHNICAL REQUIREMENTS

To outline approaches that allow the proof of non-involvement in a cyber attack, it is necessary to highlight the required capabilities that are needed for such measures to be effective, plausible and applicable. The key for plausibility lies in the level of detail and the coverage of the information provided by a state as proof for non-involvement. Therefore, this data needs to fulfil the following requirements:

- It has to cover a time frame that is long enough to satisfy the accusing state and their analysis of the attack.
- It should contain data from all relevant national IT networks like military, state and intelligence service networks to avoid the accusation that the attacks had been performed from "hidden" networks. On the other hand, it should be restricted to sensitive, relevant networks and must not support civilian censorship or surveillance.
- The information needs to contain at least the details on the endpoints of all connections that had been established from the IT networks. On the other hand, the measure as well as the potentially revealed information need to respect the national secrecy.
- It must not be possible to modify or manipulate the collected and provided information, either at its time of creation or later, and the logging mechanisms must not be possible to circumvent.

In terms of crisis reduction and conflict escalation prevention, the measure as well as the provided data should ideally prove non-involvement without the necessity of trust in the compliance of the accused state. This also requires that the measures are effective even when established unilaterally.

Beside these conceptual requirements, the measure also has to fulfil some technical needs:

- It must work for encrypted and unencrypted connections from IT systems, therefore it should rely only on information that is always visible in the network-based data transmission and can always be stored in logging mechanisms.
- It must be applicable to IT systems and networks without hindering their functionality.
- In supplement to the demand of unilateral effectiveness, the measures need to work without the necessity of any kind of technical "pairing" with foreign IT systems, like the exchange of cryptographic keys or any kind of necessary technical adjustments.

APPROACHES TO A SYSTEM OF "PLAUSIBLE PROOF OF NON-INVOLVEMENT"

The main approach behind the proposed measures is the generic possibility of basically all IT network technology to gather and potentially store information on the established or performed network connections. As already pointed out, this information analysis and storage often already takes place as a measure of IT security to be able to oversee the connections, to identify malicious activities, and to reconstruct hacking attacks or attempts. Under these prerequisites, the capability to gather data is taken for granted and will not be described any further. In terms of the proposed context as a risk reduction measure, this data acquisition and storage is interpreted as a measure to store the proof of one's own "digital innocence" for specific incidents. The following questions therefore emerge: Where within a network the data needs to be collected, what kind of data needs to be stored and to which level of detail, for which period the storage should take place, and how a tamper-proof storage can be performed to fulfill the requirements discussed above. These questions will be discussed in detail with regard to the described conceptual and technical requirements:

I. At what points within an IT network does data have to be gathered?

As described earlier, connected IT systems are always topologically organised in network structures, on a physical level[503] as well as on a higher logical level[504]. Networks usually have one or more connection points to other networks[505] and these gateway servers process every data transmission. They "know" about any outgoing and incoming connections and, in terms of the proposed measure, need to store this information. With regard to the network-sub-network topology, it is only necessary to store the information about connections and transferred data at the logically "outermost" gateways, where data leaves the IT system of an organisation or institution and is transferred to external systems. In the context of this paper, this means the gateways where military, governmental or intelligence service networks are connected to civilian or commercial networks. With regard to the described requirements, it is important that on the one hand, this storage is performed on all gateways that connect these specific networks to the "outside world" to prevent "hidden channels". On the other hand, in terms of data privacy and personal rights, it must not be established on civilian, public or commercial networks. The measure itself may need additional capacities for data storage but does not affect the functionality of the gateways.

II. What kind of data has to be gathered and stored, and to which level of detail?

[503] The physical level describes the hardware of the IT systems within a network as well as the connection and transportation hardware. These can be mixed technologies from wired to wireless or even satellite connections.

[504] The logical level describes the way in which the devices within a network are organized and grouped, for instance by their identification numbers. This reflects the way data (or in technical terms "signals") acts on the network, and how it is processed and transmitted. The logical level does not necessarily reflect the technical level but is seen as the higher organisational level.

[505] Exceptions are "off-line networks" where no outgoing connections exist, either because no physical connection to other networks exists at all, or the connection is a so-called "unidirectional security gateway" (or "data diode") where special hardware assures that only one-way connections are technically possible.

The process of network data transmission is structured in different abstract layers, often represented as the so-called OSI model that "characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology"[506]. Each layer describes the way data is handled conceptionally (from physical signals to logical data packages), how it is transferred, which software technology and work-flow is used, as well as the necessary hardware. In correspondence to this layer model, the transmission of any data is also performed gradually from one layer to the next, where the transmitted payload is embedded and extended by necessary transportation information like "nested envelopes". Each "envelope" carries all relevant information that is necessary for the next lower level of transportation logic to process the data. On the highest level, the "envelope" contains only the pure data that needs to get transmitted (like e.g. a digital file) and carries the information of the data package sender, its destination (both via their IP addresses) and the application for which this data is meant[507]. This kind of information is available even if the transmitted payload itself is encrypted. A typical connection between two IT systems consists of multiple data packages with different purposes that establish the connection, transfer the data in multiple single packages, acknowledge the successful transmission of the packages, and finally close the connection. Additionally, gateways know about the time stamp when a specific connection has been established, as well as the amount of overall data that has been transferred over an established connection. In terms of the proposed measure, the following information is appropriate to prove for a given time-stamp that no data transmission had been performed to a specific IT system or network, and therefore needs to be stored by the gateway servers:

- When the connections have been established and closed, either from within the network or by request from "outer" IT systems.
- To which destination (for outgoing connections) or from which origins (for incoming connections) connections have been established.
- How much data has been transferred and for which protocol

For an effective application of the proposed measure, it is not necessary to store information on all packages, only on the connections. In terms of secrecy, this connection data would reveal a lot of potentially sensitive data because it contains details on the quantity and types of IT systems and services within the network, as well as the quantity and locations[508] of systems that the specific gateway usually "talks to". To maintain secrecy, IP addresses can be anonymised to contain only information on the sender and destination networks, or the type of transmitted data (that could be identified via the protocol) can be hidden by using so called VPN tunnels[509]. The stored data would still contain sufficient information to provide proof of non-involvement.

[506] OSI stands for "Open Systems Interconnection model", see https://en.wikipedia.org/wiki/OSI_model

[507] The reference to a specific application is done via the so-called protocol which defines the technical work-flow as well as the specific data configuration. Common protocols are HTTP for a request for a web page that will get handled by a web server, IMAP for email, FTP for a file server, or SSL/TLS for a login to a foreign IT system.

[508] IP addresses can be assigned to geographical locations to a certain degree of accuracy. A good source for a brief explanation is https://whatismyipaddress.com/geolocation

[509] VPN stands for "virtual private networks" and is a technology where two endpoints create a virtual "tunnel". Every transmitted payload data is encrypted, embedded in data packages of a specific protocol and transferred over this tunnel. Although VPN tunnels contain sender and destination IP addresses, the data protocol does not allow any conclusion on the real payload.

III. How long does data need to be stored?

The question of the storage duration cannot be answered definitively and is rather a task of consideration. On the other hand, this parameter is easily adjustable and affects only the necessary storage capacities of the logging algorithm. Ideally, logging files of accused agents last as long as the attack persists to be able to present data for the proof of non-involvement over the whole runtime of the analysed attack. A solid basis for the storage time estimation can be provided by studies that are regularly performed by IT security companies which analyse hacking incidents. As an example, a report by Mandiant Consulting[510] estimated that in 2016, cyber attacks had lasted 146 days in the worldwide average before they were detected. The same report calculated the average detection life span of hacking attacks for Europe and the Middle East to be up to 469 days. For the year 2017[511], the analysts calculated a worldwide average of only 99 days and came to the conclusion that the life span of attacks significantly dropped due to higher sensitivity for IT security. Another approach to further specify the necessary logging time frame could be taken from recommendations[512] for the size and time frame of logging data structures for IT security reasons. They influence how long in time (going backwards) a hacked target is able to trace back steps within its own systems that an accused state needs to argue with. Furthermore, it is necessary to point out that for an ongoing attack, it can already be a measure for reducing the risk of conflict escalation if an accused state is able to provide data on their current gateways activities (a "live view") and prove their non-involvement in the current communication of the attacker with their command and control infrastructures.

IV. How can the process of data gathering and storage be technically tamper-proof?

As already pointed out, the acquisition and storage of logging information is hardly new and a common feature of IT security toolkits. In the context of this proposal, it is the credibility of such data that decides whether a targeted victim believes the "digital facts" that an accused agent provides as proof for their non-involvement. Credibility can be reached by technically ensuring that neither the process of the logging data acquisition is tampered with (e.g., connections to some specific endpoints get excluded from logging) nor that logged information can be manipulated afterwards.

Preventing and ensuring tamper-proof data storage is a problem that can be solved with a relative new technology called "blockchain". A blockchain "is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a time-stamp and transaction data. By design, a

[510] M-Trends 2016 – EMEA Edition, https://www.fireeye.com/current-threats/annual-threat-report/mtrends/rpt-2016-mtrends-emea.html

[511] M-Trends 2017 Report, https://www.fireeye.com/company/press-releases/2017/fireeye-releases-mandiant-m-trends-2017-report.html

[512] Estimating the log file size highly depends on the used hardware, the logging algorithm and other variables. A more generic approach is described in "Estimate the size and number of log files" for IBM network hardware https://www.ibm.com/support/knowledgecenter/en/SSGU8G_12.1.0/com.ibm.admin.doc/ids_admin_0715.htm

Blockchain is inherently resistant to modification of the data."[513] A "hash" can be seen as a technical way of "sealing" information that can be used to ensure for any kind of delivered data that it has not been modified. In the blockchain, each new data entry is verified by its previous entries via a process of so-called cryptographic signatures[514]. This means that a digital key is created based on previous entries and then used to cryptographically sign the new entry. This prevents any alteration of stored data because any modification would invalidate all following entries in the blockchain. Using this kind of technical verification for streams of logging data is a concept that had already been described as "audit log" or "audit trail" for use cases in safety or secrecy critical scenarios[515].

An additional degree of credibility can be achieved by ensuring that the mechanism which collects the logging information (commonly defined by so-called logging rules) itself has not been modified in any way to hide activities. This is possible by including the logging rules definition as well as a hash of the logging software into the blockchain[516]. This would provide tamper-proof copies of the logging process and its configuration for a comparison to a later version of the rules and the logging software. To ensure that the initial submit of code, rules definition and hashes comes from the software that creates the log files, the software itself can be adjusted to include hashes of relevant parts of its source code or executable binaries into the blockchain on a regular basis. This data can then be used to compare if the initial code and the hashes still match later stored versions to prove its validity.

In terms of the defined requirements for the proposed measures, creating and securing logging data with a blockchain mechanism results in a significant increase of the necessary processing and the storage capacities[517]. These capabilities should also be taken into account for the storage time frame, but they do not affect the functionality of the systems.

SUMMARY OF THE TECHNICAL PROPOSAL

The analysis presented above discussed a system of network connection logging and tamper-proof storage that can enable an agent to prove their non-involvement in a given cyber attack. We showed that already applicable technological solutions exist which in combination can provide the necessary conceptual requirements like plausibility and validity on the one hand, while offering anonymising features to sustain the necessary secrecy on the other hand. The coverage and plausibility of any argumentation depends on the establishment of the logging mechanism on

[513] https://en.wikipedia.org/wiki/Blockchain

[514] A brief overview of digital and cryptographic signatures is given in "An Introduction to digital signatures" from https://www.trustzone.com/sites/default/files/uploads/trustzone_introduction_to_digital_signatures_2017_1.pdf

[515] A theoretical and crypto-analytic explanation is delivered by Bruce Schneier and John Kelsey in "Cryptographic Support for Secure Logs on Untrusted Machines", https://www.cs.jhu.edu/~fabian/courses/CS600.624/paper-secure-logs.pdf

[516] If open-source software is used, which is often the case for network technology, the source code of the software could also be included in the blockchain.

[517] As an example, the bitcoin blockchain that uses the same mechanism to store every transaction of the digital currency from its beginning contained nearly 310 billion transaction entries on April 6th, 2018. The overall size of the Blockchain file where these transactions are stored is about 160 gigabytes of text. Sources: https://Blockchain.info/de/charts/n-transactions-total and https://Blockchain.info/de/charts/blocks-size

all relevant gateway servers to circumvent any accusation of attacks via hidden routes. It also depends on the time frame in which logging data is stored and kept. In any case, the stored information stays with the establishing agent and is therefore hidden from external parties, until it may be used to counter misinterpretations about the origin of malicious cyber activities.

LIMITATIONS AND POTENTIAL PITFALLS

The proposed measures face some potential pitfalls that need to be considered. First of all, the radius of their possible implementation is limited to institutions that are under direct state legislation or governance, and that legally permit such level of data storage. The measures therefore can neither prevent states from performing cyber attacks by using civilian systems or systems of foreign nations, nor can they control non-state activities. On the other hand, the proposed approaches are supposed to provide measures for conflict escalation prevention for state-level activities and for networks or IT systems that are under a state's direct control, where technical adjustments are applicable and legally indisputable. Furthermore, the measures are envisaged as an approach in the sense of confidence and trust building for cyberspace by restricting the states' own capabilities for cyber attacks. The compliance of a state that decides to establish such measures is taken as a premise and its inherent self-interest. Also, with regard to the usage of non-state third parties for covered activities, it needs to be highlighted that this is per se not solvable by such measures if not applied to the IT networks of the state as whole - which cannot be in the interest in terms of personal rights and data privacy. Therefore, the plausibility of any non-involvement argumentation still depends on the reliability of the accused agent, while the provided data can offer only partial exoneration. It cannot compensate the necessity of politically binding rules of responsible state behaviour and responsibility. A last political double-edged aspect that needs to be considered is the extent of collected, stored and potentially committed information about network activities that could contain secret information. As explained, this can be diminished to a certain degree by anonymising the stored information. Furthermore, these information stay in secret with the party that deployed the measure until needed in "high times" to prevent an imminent crisis.

A technical limitation can be derived from the time frame of the logged data: The non-involvement in cyber attacks that are older than the stored information cannot be proven. This also affects the coverage of the logging IT systems. A valid and credible argumentation is only possible when the logged information contains any relevant gateways. Another limitation is given when cyber attacks involve anonymisation services like the Tor network[518]. The principle of such service lies in the routing of any internet connection over specific servers that in theory remove any information which would allow tracing it back. These anonymisation networks often utilize a "cloud" of different hubs where connections are additionally routed over to disguise its path. These "disguise clouds" use different cryptographic technologies in a way that the endpoint of the connection does not have any information about its origin. These technologies undermine effectively the approach of linking cyber attacks to their origin. On the other hand, the weak spots of these anonymisation services are the entry points, thus the servers that connect the "disguise

[518] https://www.torproject.org/

cloud" with regular networks. Even if an attacker used anonymisation services, an accused state might be able to provide credible information to prove that no connections between their gateways and the servers of the anonymisation services existed for the specific time frame of the attacks. If the accused state itself operates such anonymisation services, its gateway servers should be included in the proposed data storage of this paper. At least it needs to be pointed out that the proposed measures need an adjustment of existing IT network infrastructures with an extension of the necessary processing and storage capabilities. These expenditures, as well as the associated costs to sustain the storage capacities, need to be taken into account. On the other hand, they are based on already existing IT security measures that can be integrated into the proposed approach without the need for complex IT infrastructural changes. And – an optimistic thought - the cost pressure of "peace preserving measures" could help to reconsider the current run for offensive cyber capacities.

CONCLUSION AND OUTLOOK

Despite their limitations, the proposed measures can provide a significant tool to circumvent the inherent problems of data interpretation concerning cyber attacks, and therefore a way to prevent conflict escalation due to miscalculations. On the other hand, storing possible secrets as well as the consideration of possible consequences for personal rights and data privacy suggest their prevailing application in highly critical scenarios where no other communication channels for crisis reduction like "cool-headed" bilateral consideration of information on malicious cyber activities exist. If established by a state, it might also be a strong signal to potential conflict parties for trust-building due to its characteristic of self-restricting the capabilities for offensive measures in cyberspace against external IT systems. As pointed out, the approaches might also get implemented in "cyberspace safeguard agreements" for further fact-based verification measures.

Further research could be put into the question whether and how traces of malware samples or logging information collected during cyber attacks from third parties could be forensically matched against logging information as provided by the proposed measure to detect compliance violations. Such comparison could offer additional tools to verify if an attack had been allegedly performed by a state over the detected third party, and to further reduce the possibilities for "hidden attacks". Additionally, the proposed approach could be extended to a state whose IT systems had been verifiably used for cyber attacks to prove that these had been performed by external hackers who misused the state's IT systems. This could provide a relevant forensic approach to bypass the current third party-based hacking methods that are commonly used. Another issue could address the minimisation of the proposed data storage either in terms of reducing necessary resources and - more importantly - in terms of secrecy. This can be performed for instance by differentiating the storage of data connections into separate lists of addressed networks and connection meta data like the application types. These lists could enable an accused party to provide precise data for specific incidents and prevent the handover of excessive, irrelevant or potential secret information. With regard to the analysis of provided information to prove the non-involvement it can be further examined how this approach can be extended to regulate and formalize the exoneration of trusted third parties or entitled international organisations. The measures could also be used to push on the further development of digital trust and confidence-building measures as well as verification regimes that monitor and control the compliance of states. In this regard it will be necessary to develop and establish practical control measures, like on-site inspections of gateway servers by neutral third parties in the sense of the safeguard agreements performed by the International Atomic Energy Agency (IAEA) to control the nuclear program of Iran, or the verification regimes performed by the Organisation for the Prohibition of Chemical Weapons (OPCW) under the Chemical Weapons Convention (CWC). Given the current military developments in cyberspace, such actions of arms control and non-proliferation are long overdue.

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

GLOBSEC

Ministry of Foreign Affairs

Of Estonia

SUPPORTERS

Black Hat USA

Packet Clearing House