DRAFT – shared with the participants of the ICT4Peace Workshop on

Existing and future norms on international ICT infrastructure and data integrity

PERSPECTIVES

on Responsible Behavior in State Uses of ICTs

ICT4Peace Foundation

2017

FOREWORD

The ICT4Peace Foundation stands for an open, neutral and inclusive promotion of a peaceful cyberspace through international negotiations with governments, companies and non-state actors, in particular on norms and confidence building measures and capacity building.

Our roots in the UN World Summit on the Information Society in 2003 placed upon us the task of carefully considering all different viewpoints, arguments and proposals and to promote a broad societal acceptance of standards of responsible behavior in uses of ICTs.

With the support of the Dutch Government, Microsoft and the Cyber Policy Institute, in 2014 ICT4Peace launched a process to promote and support the international cyber norms dialogue. This publication contains a collection of papers developed during this process. We offer the 'Perspectives on Responsible Behavior in State Uses of ICTs' as a collaborative contribution to the international community, hoping to enrich and inform further discussion of the theme.

Sincerely,

Dr. Daniel Stauffacher

Founder and President, ICT4Peace Foundation

DRAFT – shared with the participants of the ICT4Peace Workshop on

Existing and future norms on international ICT infrastructure and data integrity

FOREWORD

It seems that in the cyber community everybody is talking about norms. The roots of this global discourse lie in fast development of information and communication technologies (ICTs). Since the early steps to create information societies in the late 1990s and early 2000s, we have heard the voices of civil society groups, business community, regional and international organizations, and the States.

Cyber Policy Institute (CPI) would like to hear more. We want to contribute to an open and inclusive dialogue on responsible State behaviour in the context of ICTs. We want to promote systematic studies of norms and State practice that bypasses disciplinary, administrative and national boundaries. We seek to achieve a dialogue that acknowledges our individual differences as strengths rather than weaknesses. We seek to enhance constructive dialogue that moves mountains.

CPI shares the ICT for Peace Foundation's view that information and communication technologies are first and foremost tools of peace and development. It was the *Leitmotiv* of the Conference on State Practice and Future of International Law in Cyberspace we organized for the Estonian Ministry of Foreign Affairs in 2016.

I hope that views from this Conference trigger fruitful dialogue where arguments and claims are shaped by shared convictions and mutual understanding.

Sincerely

Mika Kerttunen

Director, Cyber Policy Institute

TABLE OF CONTENTS

DRAFT – shared with the participants of the ICT4Peace Workshop on

Existing and future norms on international ICT infrastructure and data integrity

KEY PROBLEMS OF APPLICATION OF INTERNATIONAL LAW TO ICT ENVIRONMENT

KEYNOTE AT THE CONFERENCE ON STATE PRACTICE AND DEVELOPMENT OF INTERNATIONAL LAW

TALLINN, ESTONIA MAY 5-6, 2016

Anatoly Streltsov

Dear hosts of the conference!

Dear participants!

Ladies and gentlemen!

I truly appreciate the opportunity to make a speech at such a high-level conference and talk about our point of view of the key problems arising from the application of international law to the ICT environment. This issue appears of great interest, and it has been pointed out in the Reports of the 2010, 2013 and 2015 UN Group of Government Experts.

I would like to raise a few questions and offer answers that reflect our way of thinking about these issues.

1. Do the established principles and norms apply to ICT?

I think that the established principles and norms apply to ICT, because of three main reasons.

First. In modern conditions it is almost impossible and inexpedient to create a new branch of international law. It is not possible because the world is so changeable today and it is unreal to achieve an agreement on such complicated issue. It is inexpedient because everything new that we create will be based on existing principles and norms of international law.

Second. We think that the established principles and norms of international law may be used in state practice. They have stood the test of time and reflect a certain consensus of the states concerning regulation of international relations. The states have a great experience of applying them to real causes related to maintenance of international peace and security.

Third. The great challenge in this application is that there is a prominent possibility of mistake in assessment of situation, considering the misuse of ICTs for military and political purposes and attribution of the actors responsible for this activity. Such mistake may provoke international conflict and as a consequence – a threat for international peace and security.

We prefer the approach of the adaptation of international law to a new field of application. It is intended to reduce the possibility of this situation. Adaptation requires interpretation of some terms from the sources of international law and development of harmonious judicial principals and procedures for fulfilment of correspondent actions. I think that such approach could help us to get the necessary effect, but also will reduce duration and cost of the task.

2. What is the environment of ICT from the standpoint of international law?

In my opinion, the environment of ICT is a legal fiction, which consists in the fact that ICT environment is considered as a part of the territory of the state. This allows us to extend the concept of "sovereignty" to the ICT environment. It should be understood that the ICT environment includes two components – the cyberspace and the media sphere. Here we limit ourselves to cyberspace.

The main differences of cyberspace from the other components of territory are as follows.

- Cyberspace is created and exists through the efforts of people. Its creation caused the emergence of new objects of international relations (for example, an incident in the cyberspace, information system).

- Objects of international relations, legal facts that determine the dynamics of changing the legal relationships and their subjects have a virtual character that is in large part invisible. This greatly limits our ability to use the witnesses and the means of objective control during investigation of incidents in cyberspace.

- Cyberspace as an object that is covered by sovereignty of the state and is characterized by such aspects as inclusion in the global cyberspace and the safety of its use. They are the analogues for such properties as territorial integrity and political independence. From this point of view, a disruption of national inclusion in global cyberspace, as well as violation of the safety of its use, are similar to violation of territorial integrity and political independence.

3. What is the problem in application of "sovereignty" concept to cyberspace?

It is necessary to note several aspects.

First. Lack of territorial constraints of sovereignty limits the implementation of certain rules and principles of international law. For example, documentation of state border violations as a means of exercising territorial authority, as well as assurance of compliance with international obligations in the sovereign territory.

Second. There are some deficiencies in the international legal regulation. Primarily it concerns the legal relations in the field of sustainability and safe use of the DNS system. Some states, for historical reasons, believe that this system falls within their jurisdiction, but there are no international obligations to ensure the stable functioning of and safe use of the system for the benefit of the entire international community. The lack of international regulation in this area limits the sovereignty of states in cyberspace.

Third. The lack of legal guarantees for the respect of human rights of citizens outside the national territory (for example, privacy, the right of authorship). As you know, states are obliged to respect these rights, but when for technical reasons data leaves national territory, the implementation of international commitments becomes physically impossible. This applies to personal data, the results of creative activity and certain other rights and freedoms.

Forth. The limited jurisdiction of states in identifying legal relations and persecution of entities responsible for their occurrence. It is known that a significant portion of incidents in the cyberspace is caused by activities of foreign entities. To investigate such incidents we must use information located at cyber facilities of foreign countries. Existing methods for solving this problem are not effective enough. We understand that the drafters of the Budapest Convention on Cybercrime wanted to overcome this disadvantage. It is known, that the Russian Federation has not signed the convention. As I see it, the only obstacle to this was the lack of confidence that the subjects of investigation of incidents in the cyberspace will limit themselves only to the task of incident investigation.

Perhaps it makes sense to return to this issue and create a system that has the same advantages as the Budapest Convention, but does not create additional concerns in the field of national security. In my opinion, a corresponding initiative of the Russian Federation creates some basis for this.

The lack of state borders in the cyberspace cannot determine where the sovereignty of one state ends and the sovereignty of another begins. This is especially important in determining, for example, the boundaries of the armed conflict in cyberspace.

4. What directions of adaptation of international law to cyberspace may we prefer?

It seems that the main direction of adaptation of international law to cyberspace is the adaptation of the key sources of the law. For example, we can discuss some of the sources of international law. It enables us to see the sketch of the basic directions of their adaptation to cyberspace.

DRAFT – shared with the participants of the ICT4Peace Workshop on

Existing and future norms on international ICT infrastructure and data integrity

UN Charter. All the provisions of the UN Charter can be applied to cyberspace.

At the same time it is important to further consolidate the construction of the use of ICT as a means of "force" (Article 2 (4) and "armed attack" (Article 51).

We believe that ICTs are not, by definition, weapons, but may acquire such properties by making a weapon of some devices and non-military mechanisms and therefore be used for the organization of an armed attack.

The precedent of such an interpretation of an "armed attack" was created by UN Security Council resolutions (1368 September 12, 2001, 1373 September 28, 2001) following the results of the discussion of the tragic events in the United States on the 11th of September. This attack was carried out using civilian aircraft, which obviously is not a weapon.

The principles of international law embodied in the Declaration of 1970 do not create obstacles to their use in the regulation of international relations in the cyberspace. At the same time, in view of their application in a new area of international life, which has a number of specific features, they need to be supplemented. This addition could clarify the interpretation of certain formulations of the declaration in relation to cyberspace.

For example, to clarify the interpretation of territorial integrity, political independence, sovereign equality and some others – with regard to cyberspace.

Hague and Geneva Conventions. The principles and rules of the law of armed conflict and international humanitarian law are also consistent with the use of ICTs as a means of "force" against the enemy. However, due to the specific features of ICTs they need to be clarified.

For example, it is necessary to clarify how to separate in cyberspace the zone of armed conflict and the territory of neutral states. What should be the mechanism for the identification of civilian and military sites in cyberspace, which is essential to the implementation of the main constraints imposed by international humanitarian law on military action? What procedures should be performed by authorized bodies for international investigations on the grounds of violation of these restrictions by one of the belligerents?

Procedural principles and norms of the objectification of the hostile use of ICTs and attribution of the subject of this activity.

Nothing prevents the states from taking policy decisions on the use of available means to repel an "armed attack", but, as it seems, it is useful to base these policy decisions on international law.

There are two basic approaches to the objectification of the hostile use of ICTs and attribution of the subject of this activity:

- presumption of confidence in the forces of national security;

- presumption of confidence in the third party, such as an authorized international organization.

To minimize the risks of an erroneous assessment of the situation, like the discovery of the WMD in Iraq (2003), and to identify non-state actors operating in this field, it seems preferable to create a system of objectification and attribution on the basis of a combined approach.

Given the characteristics of ICTs as a factor of power, the struggles between the states are important, so that the procedural rules and principles, including participation of national service providers and network operators in the process, have been approved by the international community.

In particular, I would like to express the position on the question of **countermeasures** in the sense of the draft convention on international legal responsibility of the states. With regard to cyberspace, the adoption of such measures is dangerous, because it can trigger the "war of all against all."

In conclusion of my presentation, I would like to speak about the question of the rules of responsible behavior of states in ICT environment. It seems that their advancement, research of the problems of their application and development of the necessary conditions for this, are among perspective directions of effort of the international community, to prevent international conflicts in cyberspace.

Thank you for your attention!

DRAFT – shared with the participants of the ICT4Peace Workshop on

Existing and future norms on international ICT infrastructure and data integrity

COMPREHENSIVE NORMATIVE APPROACH TO CYBER COMPLEXITY

Eneken Tikk

Technological innovation defines and influences modern Statecraft and lifestyle. More interconnected, multi-actor world order blurs the boundaries between international and domestic, public and private, social and political affairs. Governments are thus compelled to acknowledge new themes and questions as national concerns. When addressing composite issues such as cyber security, States are faced with the reality of parts and parcels of this multifaceted issue being distributed among different international and regional organizations. When examining power in world affairs, Nye concludes that the convergence of computing and communication technologies change the nature of government and accelerate the diffusion of power.[1] As societal affairs and individual behaviour undergo constant upgrades with the help of technological development, the expansion of points of potential contestation, the fragmentation of mechanisms of control and governance as well as the diffusion of power are likely to continue.

Recognizing globalized life and international relations having led to the "emergence of specialized and relatively autonomous spheres of social action and structure", a United Nations Study Group on Fragmentation of International Law pointed out legal significance of this development.[2] The Study Group identified the emergence of "rules or its complexes, legal institutions and spheres of legal practice". The Report went on to observe that specialized law-making and institution building tends to take place "with relative ignorance of legislative and institutional activities in the adjoining fields and of the general principles and practises of international law" resulting in conflicts "between rules and rule-systems,

---

[1] Joseph S. Nye, Jr., *The Future of Power* (New York: Public Affairs, 2011), pp. 114-118.

[2] United Nations General Assembly, International Law Commission, "Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law", Finalized by Martti Koskenniemi, A/CN.4/L.682 13 April 2006.

deviating institutional practises and, possibly, the loss of an over all perspective of the law."[3] Multiplicity of international regulatory instruments results in nested and overlapping authorities and lack of normative interoperability. These, in turn lead to forum-shopping as well as administrative difficulties of enforcement.[4]

Considering the complexity of legal relations in a globalized and interconnected world, the dogmatic lines between international and municipal law, as well as between public and private law are diffusing. Added to that are the known challenges of legal uniformity and level of 'hardness' of existing norms. While such pluralism challenges jurisprudence and legal certainty, it also offers opportunities for critically approaching the evolution of norms in the absence of international consensus on the issue(s).

Cyber is an area that benefits and suffers from expansion and fragmentation of international law and of the state regime complex, and in fact that these specialized, narrow and loosely coupled regimes coexist in the same issue-area without clear hierarchy.[5] Some of the posited effects of international regime complex—bounded rationality, small group dynamics, feedback effects, and a renewed attention to the politics of implementation— are said to have contradictory or crosscutting effects. Further effects of regime complex—cross-institutional strategizing, the asymmetrical distribution of legal and technical expertise, the fragmentation of reputation and conflicts between individual regulatory elements—can undermine the significance of institutions in complex environments.[6] As a result, same normative instruments are by default interpreted in logical and legitimate but often in an incommensurable way in different contextual environments.[7]

As advanced ICTs penetrate all areas of social and political activity, it is hardly surprising that over time a rich body of norms has emerged to address aspects of uses of ICTs, such as data protection and privacy, communications and network security or cyber crime. In addition to these are the long-established principles and norms of international peace and security that apply to uses of ICTs. It has been observed that cyber security is covered by multiple rules and principles deriving from most diverse subject areas of international law, whose principal applicability to cyberspace and whose concurrence have not yet been fully

---

[3] Ibid.

[4] Daniel W. Drezner, "The Power and Peril of International Regime Complexity", *Perspectives on Politics*, Vol. 7, Nr. 1, March 2009.

[5] Robert Keohane and David G. Victor, "The Regime Complex for Climate Change", *The Harvard Project on Climate Agreements*, 2010; Joseph Nye Jr., "The Regime Complex in Managing International Cyber Activities", Centre for International Governance Innovation, May 2014.

[6] Drezner (2009), "The Power and Peril of International Regime Complexity"; Keohane and Victor (2010), "The Regime Complex for Climate Change".

[7] United Nations General Assembly, International Law Commission (2006), "Fragmentation of International Law".

analyzed.[8] Additionally, hundreds of politically binding instruments have been adopted by various international and regional organizations in the past three decades to address desirable and undesirable uses of ICTs by state and non-state actors.[9]

There are enough of views on the applicability and implementation of various norms in the cyber context. The *Tallinn Manual on International Law Applicable to Cyber Warfare* elaborates in-depth how norms of International Law of Armed Conflict and the International Humanitarian Law can be applied in cyber operations.[10] The UN Human Rights Council has confirmed that human rights apply online the same way they apply offline.[11] The CODEXTER experts of the Council of Europe have concluded that existing international conventions and other instruments that promote the harmonization of national substantive and procedural law and international cooperation are applicable to these misuses of the Internet for the purposes of terrorism.[12] Further scholarly work explains how the provisions of ITU treaties apply to cyber security.[13]

To sum up, the issues and solutions of cyber security are distributed between various normative instruments and authorities. In the absence of understanding and consensus on responsible behavior of states, latter are likely to interpret cyber instruments inconsistently and take advantage of inconsistencies and gaps in legal frameworks. The resulting lack of legal certainty results in devaluation of the existing international legal regime. Along comes the lack of legal deterrence, as actors involved as well as players contemplating similar operations will gain confidence for perpetrating it. Disconnects between interpretation and implementation of different regimes may inhibit balanced and comprehensive solutions and in turn benefit evil-doers who are searching for legal loopholes and enforcement vacuum.

PROPOSED SOURCES OF LEGAL CERTAINTY

Treaties and conventions in international law create and guarantee legal consistency and certainty very well. Therefore, it is hardly surprising that scholars and States alike have called for new treaty law to shape behavior of State. The Russian Federation was the first

---

[8] Wolff Heintschel von Heinegg, Protecting Critical Submarine Cyber Infrastructure, In Peacetime Regime for State Activities in Cyberspace, Tallinn: CCD COE, 2014), p. 291

[9] C-Source database, Cyber Policy Institute.

[10] Michael N. Schmitt (general editor), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).

[11] A/HRC/20/L.13 (June 29, 2012).

[12] CODEXTER (2007) 03 (Strasbourg, April 2, 2007).

[13] See Anthony Rutkowski, "Public International Law of the International Telecommunication Instruments: Cyber Security Treaty Provisions Since 1850"

country to raise the issue of international law and information security in the context of peace and security at an international level. In 1999, Moscow proposed a draft resolution of developments in the field of information and telecommunications in the context of international security[14], seeding international dialogue there is a need for new norms to address the development and uses of ICTs in the context of international security.[15] More recently, Russia has co-sponsored a Code of Conduct[16] and tabled a Concept Convention on International Information Security[17].

On the other hand, the proponents of existing international law as a preliminary solution to international cyber security issues and a guide of responsible State behaviour in cyberspace that heavily focus on interpretation of treaty law.

Scholars like Schjolberg and Ghernaouti-Helie[18], Hollis[19], Gaycken and Lindner[20], Arimatsu[21] and others have further contributed to thinking about treaty law in the context of cyber security. However, as extensively elaborated by the early critics of 'cyberlaw', it is doubtful whether calls for new instruments would offer satisfaction of challenges deriving from the interaction of technology and law. As Sommer notes, technological transition brought by the Internet is likely insufficient to justify development of a new bodies of law: 'few bodies of law are associated with only one technology, and few technologies are associated with only one body of law'.[22] Moreover, although carrying the best promise for legal certainty *international conventions and treaties* will inevitably never be precise and dynamic enough to resolve practical and urgent issues of cyber security. There will be inevitably limits to how far the existing treaty provisions can be stretched, and the legal certainty offered simply by intellectual interpretations may remain thin.

The so far cultivated 'new treaty' and 'no treaty' claims both put extensive emphasis on treaties as the source of international law and largely fail to initiate a broader conversation

---

[14] Adopted as A/RES/53/70

[15] Adopted as A/RES/53/70

[16] A/66/359 (14 September 2011) and A/69/723 (13 January 2015)

[17] Available at www.mid.ru.

[18] http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf

[19] https://citizenlab.org/cybernorms2012/esos.pdf, http://law.lclark.edu/live/files/9551-lcb114art7hollis.pdf

[20] http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_gaycken-lindner.pdf

[21] https://ccdcoe.org/cycon/2012/proceedings/d3r1s6_arimatsu.pdf

[22] Joseph H. Sommer, *Against Cyberlaw*, 15 Berkeley Tech. L.J. 1145 (2000). Available at: http://scholarship.law.berkeley.edu/btlj/vol15/iss3/6

about norms formation in international law. Legally binding regional or global treaties require political will and commitment as well as demand long time to negotiate. As cyber security and the development of information society are acute and urgent issues for countries at the right time may not be suitable for legal purity or diplomatic finesse. Given the still relatively low socialization of this complex set of issues in the international community, lack of understanding and uncertainty inhibit states to engage in and strive for strict normative instruments. Especially in the short run, nations with differing capabilities and priorities may be less receptive to legally binding mechanisms, but more open to discuss non-legal frameworks for shaping behavior.

Moreover, a new, technology-driven and enabled reality may reduce the prospect for prevalently treaty-based solutions. Lack of consensus itself is a rule rather than an exception in interstate cyber relations, especially as absence of precise law can in itself constitute a sufficient legal predictability for some actors. Finally, a treaty approach to relatively unsettled issues is predicated by remaining incommensurability about concepts and definitions and the scope of applicability of already existing treaty-based norms.

Propositions have also been made for customary law to emerge in the context of cyber security. Brown and Poellet have taken notes of 12 years of general practice to consider when determining what constitutes customary law in cyberspace. [23] They conclude that incidents that have occurred during that period, have set precedent for what states consider acceptable cyber behavior and propose that in the absence of formal international agreements, cyber custom is beginning to develop through the practice of states. [24] Schmitt and Vihul, although admitting the role of this source of law in shaping future State behavior in cyberspace, foresee obstacles in the path of customary norm emergence vis-à-vis cyberspace, in particular due to the opacity of cyber activities.[25] Polanski has concluded that due to the complexity of legal requirements accompanying to the emergence of international customary law, online practices are unlikely to satisfy the standards of custom.[26]

A customary law approach as well as treaty approach, will inevitably be not a solution itself. *The prospect of emergence of international custom* from the general and consistent practice of States is dim with the lack of transparent practices and understanding of operations in and through cyberspace. Of course, one should not underestimate how quickly the perception of law and policy may change or emerge – incidents like the Morris Worm and

---

[23] http://www.au.af.mil/au/ssq/2012/fall/brown-poellet.pdf

[24] http://www.au.af.mil/au/ssq/2012/fall/brown-poellet.pdf

[25] https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%205%20Schmitt%20and%20Vihul.pdf

[26] Paul P. Polanski, Customary Law of the Internet: In the Search for a Supranational Cyberspace Law. TMC Asser Press (2007).

Estonia 2007 rank in the 'cyber' world where the 9/11 attacks rank in the 'real 'world – they all triggered significant legal and policy responses with wide international consequences. Such developments may emerge in the private sector, as evidenced by the purportedly Iranian attacks against the US banking sector in early 2013, or by the international diplomacy surrounding the Sony attacks in 2014. In general, however, regime complex, capability gaps and political value and interest-based differences are likely to prevent rapid progress in determining and acting upon the similarities found in approaches thus far.

In conclusion, the currently mainly exploited sources of international law are unlikely to offer a clear and specific rule readily applicable to every international situation. Lack of normative clarity, however, is an unhealthy condition for international law, both because it runs the risk of undermining the implementation of already existing binding norms and because it promotes practices that fall under the misconception according to which all that is forbidden would be permissible. Therefore, transitory studies of international law are likely to best speak to the future of law and international affairs, providing valuable guidance both for the purposes of treaty interpretation and treaty making.

FURTHER CONTRIBUTIONS TO NORMATIVE COMPLEMENTARITY

Another logical and mandatory path for rules of underdeveloped questions to enter into international law is through tracing municipal practices and instruments sufficiently widespread as to be considered "recognized by civilized nations" as enshrined in Article 38 (1) c of the Statute of ICJ. Friedman considers general principles a potentially very fertile source of development in international law, especially in the context of development of new branches of international law.[27] Despite their relatively little recourse and recognition by international tribunals, general principles of international law are likely to gain increasing relevance in the world that is less concerned with formal regulation of diplomatic relations between states and more oriented towards resolving complex and multi-pronged issues between public and private stakeholders and they are often more interested in temporary balance than finite consensus.

Examining acute issues in international law from the angle of general principles that may provide a source of inspiration and direction thinking further about norms of responsible State behaviour. It is widely acknowledged that municipal systems of law are in many cases more developed than the international system. As a 'primitive' law, international law can

[27] Wolfgang Friedman, "The Uses of 'General Principles' in the development of international law"

turn to state practises to resolve doubt or disagreement, especially 'to overcome a deadlock, in relations between states pursuing conflicting ideological and/or economic aims'.[28]

General principles of law are therefore likely to supplement, not subtract from the corpus of international law, allowing to give greater completeness to other sources of international law, predicting its development and in some limited degree extending it, as general principles are likely to become a habit. Thus, general principles offer another valuable and suitable tool for understanding, building and thinking further of permissible and desirable behaviour under international law.

There are obvious caveats related to the use of general principles of law in search for legal clarity and completeness. Many authors see in the application of this source of law a tendency to set legal limits to the freedom of action of states otherwise than by treaty or custom.[29] As any other currently explored legal source, general principles are likely to prove an unsatisfactory guide in vacuum. Reference to domestic law might give uncertain results and the choice of models might reveal ideological predilections.[30]

However, without seeking to upgrade general principles of law in the hierarchy of sources of international law, it is important to acknowledge the value they carry as a model of thought about emerging legal consensus or the potential lack thereof. Article 38 (1) c could therefore be regarded as a complementary avenue to on-going searches of treaty law and predictions of customary law. Finally, strictly speaking, Article 38 (1) c is a tool for ICJ and therefore applicable in case of dispute.

Visiting this source of law is likely to offer valuable guidance according to treaty interpretation and current consensus-formation among the international community. Denying the value of general principles would be to deny underlying calculus of national positions regarding the development of international law and to abstain from tracking the formation of legal norms and more broadly observing international law in development. The approach of general principles might also empower proposals of analogy that would find some relevant ground for implementation under other sources of international law.

Examining the use of general principles of international law understanding between civilized nations directs us to practical solutions adopted at national level and allows us to assess the merging pockets of consensus to affect and define the development of hard law in the future. Such examination of general principles might reveal otherwise hardly discoverable facts about the treaty law. While it is likely that analysis of domestic legal approaches restate the existing international legal norms and principles, they are also susceptible to challenge the

---

[28] Sources & evidence of international law" Section 4

[29] Sources & evidence of international law, Section 4

[30] Ian Brownlie, *The Principles of International Law,*

treaty law by demonstrating significant deviations from the proposed interpretation in practice or underlying reality of operations that cannot be overcome by simple norm interpretation. Therefore, the principles test offers a way to re-validate existing treaties for new circumstances and identify leads for customary law studies, thus providing a mechanism for renewal of international law.

Shaw has observed that principles of mature legal systems can serve as general guideposts to the interpretation and evolution of international legal rights and duties, thus serving as "jural postulates of civilized society" reflecting implied consensus of the relevant community.[31] Nothing prevents future law-makers to accept principles of selected municipal approaches and reject others, thus gradually building on a common reasonable nominator. In the context, where not all municipal systems may demonstrate fully developed thinking on the matter, law of selected communities, such as the regulation of European Union on the matter of network and information security, are likely to gain shaping value, provided they appear pragmatic and ideologically neutral in their approaches.

For the purposes of legal complementarity, general principles of law can refer to both national and international principles of law. The greater scope the phrase possesses, the greater the chance of filling gaps in treaty law and customary law. Therefore, Article 38 (1) c can be thought of as a method of using all existing sources of international law and guidance to extend searches to auxiliary sources of law under Article 38 (1) d. Identifying the existence or emergence of such rules or principles would bear witness to the fundamental unity of law and reinforce the existing system of international law.

FURTHER NORMATIVE INSTRUMENTS

Searches for norms of responsible State behaviour should not stop at legally binding 'hard norms'. Although there are strong views among legal scholars according to the value and even existence of 'soft law', relevant norms could play an increasingly prominent role in contemporary international relations and their influence would increase in the future. [32]

"Soft law" consists of written instruments that spell out rules of conduct that are not intended to be legally binding, so that they are not subject to the law of treaties and do not generate the *opinio juris* required for them to be state practise contributing to custom. Not being legally binding, they cannot be enforced in court, although they may have legal

---

[31] Malcolm N. Shaw, International Law, page 98.

[32] On soft law and hard law see, e.g. Oscar Schachter, *The Twilight Existence of Nonbinding International Agreements*, 71 Am. J. Int'l L. 296, 299 (1977); W. Michael Reisman, *A Hard Look at Soft Law*, 82 Proc. Am. Soc. Int'l L. 371, 376 (1988); John F. Murphy, *The Evolving Dimensions of International Law* (Cambridge: Cambridge University Press, 2010); and Fabien Terpan. "Soft Law in the European Union Changing Nature of EU Law", *European Law Journal*, Wiley-Blackwell, 2014.

relevance in a concrete case. The following examples can be mentioned when talking about "soft law": United Nations General Assembly Resolutions, Helsinki Final Act 1975 or the Bonn Declaration on International Terrorism 1978.

The factual legal relevance of many political norms is undisputed. Recommendations may not be legally binding, but it would go against the standards of legal professionalism to advise a government that it may simply ignore them. Commentary to Article 38 of the ICJ Statute concludes that General Assembly resolutions, even if they are not binding, may sometimes have normative value. As part of "international *soft law*, recommendations produce legal effects and merit due consideration in good faith".[33]

As Sztucki has observed, there are risks associated with reliance on vague and not directly binding norms. However, the neglect of international binding norms, and the erosion of international law have materialized even in the absence of coordinated efforts to seek for additional legal clarity and support the completeness of international law as a system, as follows from the analysis of the UN Study Group. Therefore, a structured search for additional normative guidance in the spirit of complementarity could not hurt but benefit the existing international legal order.

Including both legal and political norms in the fundament of normative consensus allows identifying and building on the smallest common nominators and creating pragmatic, flexible and feasible mechanisms to mitigate immediate security and other vital concerns in the absence of universal hard commitments. Gradually, consensus emerging around most relevant and impactful practices will pave way to broader and more binding arrangements. Creating legally non-binding, "political", norms may prove more feasible and effective approach than grand treaties or implicit and questionable customs.

For legal positivist, the lack of legally non-binding force of soft law, such as resolutions, communiqués and memorandum of understanding, make it an apprehensive and unclear term. Treaties and conventions being explicit and explicitly agreed upon also make them relatively easy sources of interpretation and application. Murphy leaning on Weil's definition of soft law concludes that soft law is imprecise, ambiguous and not really compelling. Murphy nevertheless refers to opinions that note "the capacity of soft law in the form of resolutions of international organizations or other non-binding international documents [that they have a capacity] to become hard law" as well as to Reisman who has observed that "even if soft *law does not harden up*, soft law performs important functions, and, given the structure of the international system, we could barely operate without it." In line with the notions of regime complex and the comprehensive normative approach emphasized in this analysis

[33] Page 771-772.

Murphy's opinion is that "perhaps increasingly often legally non-binding international instruments serve as a substitute for rather than a step toward binding international law."[34]

A COMPREHENSIVE NORMATIVE APPROACH

Recognizing the debilities of both treaty and customary law approaches for the purposes of informing expectations of appropriate behaviour in cyberspace, broadening the surface of the on-going norms investigation to other legal and political normative instruments is a necessity. The paper therefore outlines and offers a comprehensive normative approach as a method for further debate about consensus on responsible State behaviour in cyberspace.

Such an approach acknowledges international law with all its sources of origin but expands the scope of accepted and appropriate mechanisms to soft law and other legally non-binding instruments. This broadened approach is outlined below by categories of international norms. The categorization presented belongs to the conceptual work of Terpan who recognizes soft law covering both legally binding and non-binding norms.[35]

Figure 1.1 Categories of norms. Author's compilation following Terpan (2014)

<table>
<tr><td colspan="4">NORMS</td></tr>
<tr><td colspan="2">Binding
(legal)</td><td colspan="2">Non-binding
(political)</td></tr>
<tr><td>Hard law</td><td colspan="2">Soft law</td><td>Non-legal norms</td></tr>
<tr><td>Binding norms</td><td>Binding norms with a soft dimension</td><td>Non-binding norms with legal relevance</td><td>Non-binding norms</td></tr>
</table>

Applying a broader approach to rules and normative instruments would serve the purpose of norms economy but would also correspond to the reality of emerging understanding of feasible and functional remedies. General principles of law, soft law and even non-binding

[34] Murphy (2010), *The Evolving Dimensions of International Law*, pp. 20-23.

[35] Terpan (2014), "Soft Law in the European Union The Changing Nature of EU Law, pp. 8-9. See also K. W. Abbott, R. O. Keohane, A. Moravcsik, A.-M. Slaughter and D. Snidal, 'The Concept of Legalization', (2000) *International Organization,* vol. 54, issue 3: 401-419.

norms can be examined, developed and deployed as gap fillers but they are to be employed because of their intrinsic and instrumental utility. A comprehensive normative approach allows to embrace the current normative reality, where existing norms pertaining to uses of ICTs as explained are found in multiple international and regional instruments, both binding and non-binding. When applied, it would facilitate differentiation between legal, political and technology-driven gaps in legal implementation and determine which types of norms will be best to address particular challenges.

For example, were studies of general principles of law or national and corporate approaches to reveal significantly diverging pockets of practice, this would signal for a needed unification of views in those particular areas. Should examination of domestic practices evidence predominant unity in any given question, that unity as a common nominator could be usefully turned into the next international consensus development platform and utilized as treaty or custom base. Were we to discover that countries lack any substantially new views on matters of international cyber security, this would seriously indicate of prematurity to seek international agreements of any kind, while also fortify the hypothesis that new law might not be necessary to accommodate change resulting from development and uses of ICTs in this particular area.

When implemented the comprehensive normative approach would serve those states wanting to act despite the lasting ideological polarization and inertia upon the treaty approach. A broadened view would similarly support those who want to understand the current dynamics of norm development and those interested in shaping *lex ferenda* and further thought on the issue. To serve these practical interests, one needs to ask substantive rather than normative questions. Such research would be able to examine the existence of norms, their utility as well as limitations and identify areas of conflicting claims and interests or further normative development and political rapprochement.[36]

Law being and developing behind technology is a virtue of the former. Change in law is not implicated primarily by norm aggregation but a qualitative change in legal thinking and application of existing legal bodies to be changed in social circumstances.

CONCLUSION

The proliferation of international law and regulatory mechanisms has manifested in the increase of legally binding international treaties and conventions as well as legally non-binding instruments. Because of norm complexity, the variety of special and general norms

[36] See ICT4Peace working papers analysing the normative foundations in three rule-complexes: international cooperation; freedom of information, privacy and national security interests; and the expectation to be protected against malicious uses of ICTs, are modest examples of such conceptually demanding and politically relevant work. www.ict4peace.org.

and the unclear hierarchy between them, it is highly unlikely that one-rule-fits-all solution can be found. Managing broadening and politicized content, diversified authorities and distributed norms by one instrument or one narrow mechanism is utopia.

Change in normative thinking is called for by the very emergence and proliferation of advanced ICTs as well as their growing centrality to world economy, development and security. This change necessitates critical approaches to established normative tools and techniques, such as State-centric accountability models in international treaties or formation of customary international law. By the way of narrow normative interpretations, we might be left to conclude that existing legal and political frameworks offer no remedy to the increasingly technology-enabled way of life.

It is therefore essential to chart and connect the existing normative instruments that address various aspects of cyber security at the international level. It is equally essential to keep in mind all normative avenues for promoting responsible state behavior in cyberspace, using both legal and political norms to achieve an open, resilient, peaceful and secure cyberspace.

PATTERNS OF BEHAVIOUR: STATES IN, THROUGH, AND ABOUT CYBERSPACE

Mika Kerttunen

INTRODUCTION

State behaviour matters. In particular in the context of information and communication technologies (ICT) responsible State behaviour has become an issue of political-practical as well as legal-theoretical importance. Responsible State behaviour is needed, codes of conduct have been forwarded, and new treaties and cyber regimes have been considered necessary. Three claims argue of State behaviour being a politically relevant object of study: the novelty, the significance and the instrumentality of State behaviour.

The novelty claim pays attention to new era in international relations combined with the widening employment of advanced technologies. The claim notices the rise of non-state actors and technologies shaping individual, societal and international life.[37] Nations and decision-makers are also seen to struggle to understand the direction, speed or impacts of technological development.

The significance claim stresses that the development, availability and the use of information and communication technologies are issues of significance for international peace and security, regional stability and national and individual development. ICT used for malicious purposes ranging from cyber crime, terrorist use of ICTs to alleged cyber war are regarded as threats.[38] On the other hand, the mastery of ICTs is seen as tools of economic and societal

---

[37] See for example Marina Kaljurand, "Foreword" in Eneken Tikk-Ringas (ed.), The Evolution of Cyber Domain (London: International Institute for Strategic Studies/Routledge, 2016).

[38] In particular the debate initiated by the Russian Federation at the UN First Committee in 1998 and in the Group of Governmental Experts on International Information Security in 2001 testifies of this line of thinking. See also the U.S. International Strategy for Cyberspace that sets an ambition to "build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace" needed to "promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation". (The

development, even enabling developing nations to leapfrog over some stages of development.[39]

Firstly, the instrumentality argument points to the doctrine of responsibility as a preventive, self-repairing or procedural institute to maintain peace, peaceful co-existence and peaceful settlement of disputes.[40] In the field of ICTs/cyber affairs the essential questions asked include not only the responsibility of the self but also of the other, especially non-state actors such as proxies. Secondly, instrumentality refers to the methodological connection between State practise and the development of International Law. State action constitutes international custom, which potentially can be accepted as law, an important linkage between practise and law of the Statute of International Court of Justice makes in it Article 38 speaking of the sources of law to be applied in ICJ decisions.

Canons of International Law explicitly acknowledge State behaviour. Oppenheim's definition of custom as "a clear and continuous habit of doing certain actions" that has "grown up under the aegis of the conviction that these actions are, according to International Law, obligatory or right" outlines the linkage between behaviour, custom and law.[41] Oppenheim also notices the letter of the Law, "its past and present" as well as the desires of States in the forms of the "past and present conferences" as guides to the future of International Law.[42] Moreover, Koskenniemi's observation of the interplay of rule based, utopian, and policy based, apologetic approaches also recognize State behaviour as an empirical and political aspect of International Law. Most importantly the advocates of policy approach, such as Politis, Scelle, and McDougal, regard International Law to be or only to be relevant, when firmly based on the social context of international policy.[43]

This study of State behaviour, its nature, structure and modalities, intends also to promote methodological thinking and precision in cyber security studies. Too often authoritative statements and market-oriented claims rather than critical, methodological or evidence-

---

White House, International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World (May 2011), p. 8-9.)

[39] World Economic Forum, The Global Information Technology Report 2015. ICTs for Inclusive Growth (Geneva: World Economic Forum, 2015); see also Rwandan National ICT Strategy and Plan.

[40] See Ian Brownlie, System of the Law of Nations. State Responsibility (Oxford: Clarendon Press, 1983), p. 1-2, 22-24, on responsibility as simple yet sophisticated idea of being liable, answereble and accountable and as a "matter of insistence on performance or restoration of normal standards of international conduct".

[41] Lassa Oppenheim, International Law (London: Longmans, Green & Co, 1955), p. 26.

[42] Lassa Oppenheim, The Future of International Law (Oxford: Clarendon Press, 1921), p. 1, 8, 24. In the time of Oppenheim's analysis, before the First World War (the original German edition was published in 1911), international conferences, the few of them, were the primary venues for wider international exchanges of legal and political opinions.

[43] Martti Koskenniemi, "The Politics of International Law", European Journal of International Law, Volume 1: 1 (1990), p. 9-11.

based research occupy the field.[44] Acknowledging international affairs constituting of words and deeds, the study offers three perspectives of State behaviour.[45] It firstly contextualizes and defines State behaviour as precautionary and reactionary action (and inaction) taken to run and manage day-to-day cyber affairs. Acknowledging the notion of self-interest as a central theme in State behaviour, the analysis secondly revisits theories of International Relations and International Law to account plausible motivations of behaviour.[46] A developed ontology of State power projection leads the analysis to identify State activities in, through and about cyberspace. Thirdly, signifying States' normative aspirations and concerns key domestic and international debates in the field of information and communication technologies are detected.[47] Political, legal and doctrinal claims are thus seen as State continuous and uniform behaviour. Drawing from the three perspectives analysis of State, doings and wants patterns of State political, operational and legal behaviour will be discussed.

ONE: MANAGEMENT

Policy can be understood to constitute of regulatory-normative and managerial-empirical measures. The former refers to legislative and policy frameworks that set precautionary and reactive measures, the basis of Statehood and sovereignty of being the ultimate political decision-makers. The latter denotes to the use of the measures to run and manage cyber affairs, including incidents; the exercise of sovereignty. Accordingly, practice the necessary, "constant and uniform", element to have potentially a custom building force that constitutes a segment of State behaviour.[48]

---

[44] On distinguishing the methodological use and force of concepts and their limited empirical accuracy, see Raymond Aron, The Opium of the Intellectuals (New York, NY: W.W. Norton & Company, 1957) and Introduction to the Philosophy of History: An Essay on the Limits of Historical Objectivity (Boston MA: Beacon Press, 1961).

[45] The research builds its framework for analysis from theories of International Law and International Relations. Empirically the research draws from the official State documents as well as on observed State practise within international cyber security processes and mechanisms in 2015-2016.

[46] State motivation also matters in regard of practice as custom-creating. Motivational claims support or exclude State pronouciations or actions and provide foundational and cumulative evidence to form opinio juris and most importantly customary rule. (Hugh Thirlway, The Source of International Law (Oxford: Oxford University Press, 2014), p. 70-71.)

[47] The debates are reagerded as independend variables of the study and therefore are not subject to detailed analysis. While recognizing the linkage between technology and geopolitics, mainly technological depates, such as e.g. on standards and protocols, are excluded from this study.

[48] Thirlway, The Source of International Law, p. 64-79; International Court of Justice, Right of Passage over Indian Territory, ICJ Rep 40 (1960), cited in Thirlway, p. 64. Custom to grow requires also acceptance of other similarly sovereign State actors and, according to many scholars, opinio juris accompanying and conceptualizing such practise. Thirlway regards practice as States acting in relation towards each other or "other recognized international actors susch as international organizations". He notices the tendency to regard State practice in the custom establishing sense to cover also action towards citizens, a take both the apperance of the human rights agenda and the proliferation ICTs support.

This policy-centric understanding does not separate law from policy but sees law as one form and format of policy.[49] The notion of managerial measures implicitly follows Chayes and his managerial model and its "problem-solving approach" but without adhering to its exclusively cooperative and compliant nature.[50]

State behaviour within the context of regulatory and managerial policy is developed in the table below. The levels of action, international society,[51] states, corporates, and individuals represent relevant agencies regarding the development and deployment of ICTs.[52] The politics of ICT and cyber are executed in various international arenas, from the United Nations to regional organizations and international conferences as well as in forms of cooperation and contestation, even conflicts and wars. National legislative and policy-making is an obvious focal point, since the States are the primary stakeholder in international relations and international law.[53] Corporate level adds the private sector essential for the advancement of technologies but here it is also to include other organized non-state actors such as non-governmental organizations. Finally, individual level brings in citizen-user who

---

[49] This stand should not be interpreted to align the practise of law and practise of politics or law and politics as disciplines. On the nature of international law, including the relationship between law and politics/policy see David Kennedy, "When Renewal Repeats, Thinking against the Box", New York University Journal of International Law and Politics , Vol 32: 335 (2000), p. 335-389.

[50] Abram Chayes and Antonia Handler Chayes, "On Compliance", International Organization, Volume 47:2 (1993), p.175-205.

[51] The notion of international society applied here is admittedly impresice but it offers agency which the often used international level is missing. International society constitutes of States and international governmental and non-governmental organizations which have a role in the politics of ICTs, for example in Internet governance and within the UN First Committee processes. See Hedley Bull, The Anarchical Society: a study of order in world politics (London:Macmillan,1977) also for elaboration of the institutions of international society: diplomacy, war, international law, the great powers, and balance of power.

[52] In the discipline of International Relations and in foreign policy analysis and security studies in particular it is common to recognize levels of analysis. For example Holsti studying national role speaks of regional and systemic levels; and Buzan in his study of post-Cold War security and insecurity identified the levels of individual, national (state), regional, and international political system. Buzan and Hansen note the common moves within early modern International Security Studies between different levels of analysis on the individual, the state and interstate relations. Within military sciences it is common to differentiate strategic, operational, and tactical levels of war. (Kalevi Holsti, "National Role Conceptions in the Study of Foreign Policy", International Studies Quarterly, Vol. 14, No. 3 (Sep., 1970), p. 233-309; Barry Buzan, People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era (Boulder, CO: Lynne Rienner, 1991); Barry Buzan and Lene Hansen, The Evolution of International Security Studies (Cambridge: Cambridge University Press, 2009), p. 25.))

[53] Luigi Condorelli and Antonio Cassese, "Is Leviathan Still Holding Sway over International Dealings" in Antonio Cassese (ed.), Realizing Utopia: the Future of International Law (Oxford: Oxford University Press, 2012), p. 14-25. Alvarez conforms to the centrality of the State but notices three challenges to the concept of a Westphalian statehood, human rights regime, the impacts of globalization, and internal strife, all interestingly amplified by the employment of ICTs and related services. Alvarez also pays attention to the proliferation of "diverse regulatory methods demonstrate the extent to which today's sovereigns"… "Are being governed by others". (José E. Alvarez, "State Sovereignty is Not Withering Away: A Few Lessons for the Future, " in Cassese (ed.), Realizing Utopia: the Future of International Law, p. 26-37.)

shapes the regulatory domain by her opinions and social behaviour as well as manages her own ICT environment.[54]

AGENCY	REGULATORY ACTION	MANAGEMENT
International society	Treaties, convention and other legally as well as politically binding measures	State-to-state interaction: peaceful co-existence, cooperation, conflict, and war
State	National legislative and regulatory action	State behaviour as precautionary and reactionary action taken to run and manage day-to-day cyber affairs, including incidents as well as inaction
Corporate	Private, organizational standard operating procedures and other administrative rules and regulations	Private, organizational precautionary and reactionary measures to develop and maintain system and services
Individual	Public and private opinion to shape rules and regulations	Private individual precautionary and reactionary measures to manage individual ICT affairs and environment

Table 1. Contextualizing State behaviour in regulatory – managerial and international – state – corporate – individual frameworks in the context of ICT/cyber affairs. Author's compilation.

The conceptual clarity of (any) model should not prevent us from discerning the dualistic input-output dynamics between the agents and between the measures. The model reminds of the close relationships between State behaviour and international relations, between State behaviour and national legislation, and between national legislation and International Law; national legislation and practise being one of the avenues to International Law as well as towards responsible State behaviour. It also reminds of the relatively long distance repeated, but by nature particular State behaviour needs to travel to become generally accepted as evidence of custom, and thus a recognized source of International Law.[55]

[54] Societal level as an independent layer is excluded from the framework as the role of societal inputs and actors are included in the layers and actors of corporates, in specific non-governmental organizations, and individuals.

[55] On the particularism of universal claims, see Martti Koskenniemi, "The Subjective Dangers of Projects of World Community" in Cassese (ed.), Realizing Utopia: the Future of International Law, p. 3-13.

TWO: PROJECTION

State action is often associated with self-interest and the exercise of power. Power is a descriptive concept used to portray and even explain political behaviour,[56] state behaviour, state relations,[57] and the international system itself.[58] As an abstract notion power is confusing and contested; its existence is proved by the (alleged) effect-influence and the attributed instruments that easily become synonymous to the concept. Individual decision-makers and states, the users of power, are accordingly being referred and regarded as 'powers'.

The descriptive notion of power is taken very seriously in international affairs. Power is usually regarded as a latent ability, objective[59] or mean to an end[60] state and other rational and self-interested actors to pursue.[61] Most often the interests are security related or of economic or other materialistic nature. Without power one is powerless, impotent, poor in efficacy. The exercise of power inevitably taking place in interactive subject-object setting that makes actual power relative and contingent; the ability to make others act according to will of self, often against their authentic will, is a function of this power interplay.[62] Hence, the balances of power as well as military are being assessed and the detected or interpreted changes are carefully taken into strategic considerations.[63]

Theoretical literature recognizes several elements and instruments of power. Morgenthau, the founding father of political realism, identified as the elements of national power: geography, natural resources, industrial capacity, military preparedness, population,

---

[56] For example Carl Schmitt, The Concept of the Political (Chicago: University of Chicago Press, 2007 (1932)).

[57] Of the notions of power politics and balance of power see for example, Hans J. Morgenthau, "Alliances in Theory and Practice" in Wolfers, Arnold (ed.), Alliance Policy in the Cold War (Baltimore: The Johns Hopkins Press, 1959), pp. 184-212; Hedley Bull, The Anarcical Society. A Study of Order in World Politics (London: Macmillan, 1977), and John J. Mearsheimer, The Tragedy of Great Power Politics (New York: W.W. Norton & Company, 2014).

[58] For example Kenneth Waltz, Theory of International Politics (New York: McGraw-Hill, 1979).

[59] In particular Hans J. Morgenthau, Politics among Nations: The Struggle for Peace and Power (New York: Alfred J. Knopf, 1954).

[60] Waltz, Theory of International Politics.

[61] Merriam-Webster Dictionary offers three main clusters of definitions relevant to this elaboration: i) power as an ability to act or produce an effect; ii) power as possession of control, authority, or influence over others and; iii) power as physical might, mental or moral efficacy, and political control or influence. This paper does excessive elaborate the 'power-accounts' uttered, as many textbooks justifiable do, but only anchors some of its key assumptions and claims to influential arguments.

[62] Cf. Nye's definition of power as "the ability to effect the outcomes you want and, if necessary, to change the behavior of others to make this happen." (Joseph S. Nye Jr., The Paradox of American Power: Why the World's Only Superpower Can't Go It Alone (New York: Oxford University Press, 2002), p. 4.)

[63] For example, the US National Intelligence Estimate (Washington: Office of the Director of National Intelligence), The Military Balance (London: International Institute for Strategic Studies), and The Global Competitiveness Report (Geneva: World Economic Forum) all represent this tradition of material accounting and estimatiing national power, capacity and prowess.

national character, national morale, the quality of diplomacy, and the quality of government. For him the quality of diplomacy was the most important of these factors. A latter-day realist Mearsheimer on the other hand distinguishes only two kinds of power states as: latent power and military power. The former he sees to consist of predominately materialistic, 'socio-economic ingredients that go into building military power'. He recognizes and measures wealth and population but also acknowledges industrial capacity to produce "the newest and most sophisticated technologies' as they would 'inevitably get incorporated into the most advanced weaponry". In sum, for Mearsheimer's offensive realism of State effective power in international politics is a function of its military forces.[64] Gilpin, who has rather focused view on power as "the military, economic, and technological capabilities of states", argues that prestige instead of power constitutes "the currency in international relations". This claim recognizes that prestige is at least partially dependant of the distribution of power set as key factor in the changing equilibrium of international system.[65]

Liberal approaches take notice of widened state and international practises and speak for example of civilian (vs. military) and normative power,[66] and soft and hard power.[67] The more nuanced readings of power are perhaps most obvious in Keohane's and Nye's analyses of interdependency. Without disregarding military power and economic instruments, they regard manipulation of interdependencies, international organizations and transnational actors as major instruments of power. Focusing on state sensitivities and vulnerabilities, they pay attention to the dynamics between states and between power resources as well as the translating process where power resources turn into power outcomes. Moreover, they notice the importance of agenda setting; "how issues come to receive sustained attention by high officials", a form of influence increasingly used in international politics.[68]

While observing increased practise and importance of agenda setting, Keohane and Nye mention the process of politicization,[69] but do not develop the theme further towards

---

[64] Mearsheimer, The Tragedy of Great Power Politics, p. 55-62.

[65] Robert Gilpin, War and Change in International Politics (Cambridge: Cambridge University Press, 1981), p. 13, 30-31. Prestige-as-currency claim finds supports in nuclear literature explaining State behaviour and in particular decisions of acquiring nuclear weapons.

[66] See for example, Ian Manners: "Normative Power Europe: A Contradiction in Terms?", Journal of Common Market Studies, vol. 40(2) (2002): 235–258; Felix Berenskoetter, "Thinking about Power," in Felix Berenskoetter and M. J. Williams, eds., Power in World Politics (New York: Routledge, 2007); Eneken Tikk-Ringas, "International Cyber Norms Dialogue as an Exercise of Normative Power", Georgetown Journal of International Affairs (Forthcoming, Summer 2016).

[67] Robert O. Keohane, International Institutions and State Power: Essays in International Relations Theory (Boulder: Westview Press, 1989); Joseph S. Nye Jr.,

[68] Robert O. Keohane and Joseph S. Nye Jr., Power and Interdepedence (Boston: Longman, 2012), p. 9-16, 26-28, 31.

[69] Keohane and Nye, Power and Interdepedence, p. 26-28, and 83-84 where they discuss the agenda changes in oceans politics and the development and non-development of respective International Law.

normative power and a process which could be named as normativization, the tendency of regarding issues requiring formal legitimization by normative processes and regulatory instruments. As normative regimes and international governance mechanisms have become an expanding pattern of international life, normative power as an ability to create favourable norms and interpretations, but also as a skilful use of the existing body of normative instruments, has become a hallmark of State prowess.[70] The exercise of normative power can also be seen as a manifestation of statehood: becoming and being an international actor has alongside become instrumental in its own intrinsic value.[71]

Simmons argues that the effect of international law on state behavior should be a central concern of international relations scholarship, but that few studies have systematically examined this issue. She notices that international legal scholars tend to view law compliance as the norm, but political scientists being far more skeptical.[72] Ohlin in his analysis of the U.S. early 2000s speaks of shared conservative lawyers' hostility toward and suspiciousness "of international law and its infringement of American sovereignty".[73] Guzman differentiates Realist theories being more sceptical towards International Law than the Liberalist.[74] While for the former International Law may seem irrelevant in the state of war, the latter building from Kantian normative notions of international order can place international peace and individual freedom at centre of it.[75]

Goldsmith and Posner, the main culprits in Ohlin's Assault, in their analysis of State compliance argue that international law is intrinsically weak and unstable. They regard States complying with international law, only when they fear that noncompliance will result in retaliation or other reputational injuries. For them International Law has no special normative authority, it is but an extension of international relations to deal with inter-state problems. In general and specifically for them State behavior in relation to International Law is based on interests and power. The realm of international life is yet not fully anarchical.

---

[70] For example In explaining State approaches to international agreements Raustiala notices three separate dimensions, elements of regimes, the form of the agreement; the substance of the agreement, and the structure for review of performance, that States trade off one another. Any failure to control for substance or structure can confound efforts to assess compliance; and similarly the choice between hard and soft law. (Raustiala and Slaughter, "International Law, International Relations and Compliance", p. 552.)

[71] Approxiamately fourty countries seeking for the twenty available slots for the 2016-2017 UN GGE on International Information Security testifies not only of the importance of the ICT issues but also of the importance of being chosen and becoming.

[72] Beth A. Simmons, "International law and state behavior: commitment and compliance in international monetary affairs", American Political Science Review, Vol. 94: 4 (2000), p. 819-835.

[73] Jens David Ohlin, The Assult on International Law (Oxford: Oxford University Press, 2015), p. 8-14.

[74] Guzman, "A Compliance Based Theory of International Law", p. 12.

[75] Fernando R. Tesón, "The Kantian Theory of International Law", Columbia Law Review, Vol. 92: 1 (Jan., 1992), p. 53-102; Amanda Perrau-Saussine, "Immanuel Kant on International Law" in Samantha Besson and John Tasioulas, The Philosophy of International Law (Oxford: Oxford University Press, 2013), p. 53-75.

States' patterns of bi- and multilateral cooperation can harden into customary international norms. Thus, International Law can influence state behavior, but Goldsmith and Posner remind that such law-respecting and norms-complying behavior is subject to contingent assessment of national interests.[76]

Chayes and Chayes regard States calculative, but compliance is seen to avoid the need to recalculate the costs and benefits of a decision, and therefore, can lead to saving of transaction costs, thus generating efficiency based rationale for compliance. Secondly, they argue that treaties are consent-based instruments that, therefore, serve the interests of the participating states. Finally, they claim that compliance is furthered by a general acceptance of norm of compliance.[77]

The established ontologies and typologies of power are not sufficient to fully describe the means and ways States exercise power and behave in contemporary international politics. The notion of power needs an update. The continued relevance of e.g. military and economic power does not need to be questioned, but the layered, paralleled and too often incommensurable elaborations of power need clarification. Identifying trends and developments within international relations and governance mechanisms, State and social practises and in the increased use of advanced technologies, the following account recognizes Policy, technological Capability development, Military capacity, Normative, (intelligence, law enforcement, and military) Operational, and Industrial as vectors of State exercise of power.[78] These vectors, combined with levels of engagement, National and International, enable to identify State activities in, through and about cyberspace as exemplified in the following table.[79] This identification can in turn function to detect and map repetitive State practise.

VECTOR/LEVEL	NATIONAL	INTERNATIONAL
Policy	Authoritative allocation of values	Taking obligations and implementation

[76] Jack Goldsmith and Eric Posner, The Limits of International Law (Oxford: Oxford University Press, 2005); see also Guzman who similarly regards States self-interested and complying in fear of sanctions and reputational loss. (Guzman, "A Compliance Based Theory of International Law", p. 4-5.)

[77] Chayes and Chayes, "On Compliance", p.175-205.

[78] The notion of vector here refers to a line or avenue of policy action to be taken. The notion of vector should not be mixed with the notion of tool that can interchangeably refer to a method and a particular instrument. Thus within a vector State can employ one or several tools and methods.

[79] The rather usually mentioned aspects or elements of political and economic have been diluted from this framework as, firstly, all aspects of State behaviour are by default political (in Schmittian and Lasswellian senses), and, secondly, the use of economic tools are considered to be employed in all represented vectors.

	Issuing national information and cyber security strategies, military strategies and doctrines	Engagement and advocacy in international foray Coordination
		Controlling Persuasion Coercion Deterring by denial and punishment
Capability development	Issuing and implementing action plans and development programs	Capacity-building
Military capacity	Developing defensive, offensive and intelligence capacities	Allied and partner capability development Cooperation
Normative	Legislation Regulation Litigation	Regime management Norms, rules, principles, and standards development Litigation
Operational	Countering cyber crime Critical infrastructure protection Controlling content and access (e.g. banning services) Surveillance	Intelligence collection and espionage Critical infrastructure protection Joint Cyber Operations (law enforcement, military) Deterrence
Industrial	Facilitation Licencing Prioritization Standardization	Protection Marketing
		Controlling Economic espionage

Table 2. Examples of State activities as functions of state power vectors and levels of engagement. Author's compilation.

THREE: ARGUMENT

The intertwined ideological and methodological debates of ICTs and cyber are normative in the legal and political senses of the notion. They take place internationally and within domestic political systems, and are recognized here as shapers as well as indicators of normative thought and often consistent with State pronunciations. Following Kuhn's thought of scientific progress, debates can ultimately seen to reveal "the nature of things", represent and explain fundamentally different views, paradigms, or lead to a paradigmatic change. They also allow a necessary level of scrutinization under the new, changed circumstances.[80]

The five main debates, Political equality, Economic equality, The role of the State, Military use of cyberspace, and Development of International Law, presented below, do not intent to be an exclusive but a representative collection of normative thought and claims. The issues covered are intertwiningly political and philosophical as well as of political and legal significance. The most philosophical of them deal with human rights and the relationship between the State and the Individual. The political of them focus on the equality of States within the international system and equal distribution of technology and information. The scope, future and development of International Law are also explicitly and implicitly debated within the context of ICTs and cyber affairs.[81]

POLITICAL EQUALITY

The debate of sovereignty in cyberspace balances among claims of equality, exceptionalism and universalism. Sovereign equality of nations is the foundation of political sovereignty, and States recognize other States acknowledge them not only ultimate political authorities within their territory and jurisdiction,[82] but as equal actors and members of the international society. The exceptionality claim lays weight on the particular political, cultural and religious systems and beliefs that the countries as equal sovereigns are entitled to maintain. This argument underlines the unique character and application of sovereignty as well as democracy. The Universalist argument pays attention to the rights and freedoms of the

[80] Thomas S. Kuhn, The Structure of Scientifc Revolution (Chicago: University of Chicago, 1962), p. 2-5.

[81] Compared to the scholarly debates of International Relations, the debates presented here are highly and foremost political and the debators primarily States, i.e. State representatives.

[82] Harold D. Lasswell and Abraham Kaplan, Power and Society. A Framework for Political Inquiry (New Haven: Yale University Press, 1950), p. 177-185; David A. Lake, Hierarchy in International Relations (Ithaca: Cornell University Press, 2009), p. 45-51.

individual and finds support in the Universal Declaration of Human Rights; for this argument sovereignty is hardly absolute but relative and shared.[83]

The equality and exceptionalism arguments merge in modern understanding of sovereignty, explicitly expressed for example in the Conference for Security and Cooperation in Europe 1975 Final Act Article I on Sovereign equality, respect for the rights inherent in sovereignty:

> The participating States will respect each other's sovereign equality and individuality as well as all the rights inherent in and encompassed by its sovereignty, including in particular the right of every State to juridical equality, to territorial integrity and to freedom and political independence. They will also respect each other's right freely to choose and develop its political, social, economic and cultural systems as well as its right to determine its laws and regulations.
>
> Within the framework of international law, all the participating States have equal rights and duties. They will respect each other's right to define and conduct as it wishes its relations with other States, in accordance with international law, and in the spirit of the present Declaration. They consider that their frontiers can be changed, in accordance with international law, by peaceful means and by agreement. They also have the right to belong or not to belong to international organizations, to be or not to be a party to bilateral or multilateral treaties including the right to be or not to be a party to treaties of alliance; they also have the right to neutrality.[84]

In the context of ICTs, the equality debate has culminated in the issue of Internet governance: whether ICANN as an U.S. based and expert organization is the right venue to deal with issues that are of significant importance to whole mankind. The main alternative offered is a multi-lateral model where the UN agency International Telecommunication Union would have the main role in designing and deciding of the future of the Internet.[85]

The 'Colour Revolutions' in former Soviet Union countries of Ukraine and Georgia and the uprisings know as the 'Arab Spring' in Tunisia and Egypt have made Russia, China and many developing countries regimes insecure. This concern is expressed for example in the Russian 2015 National Security Strategy as "activities connected with the use of information and communication technologies to disseminate and promote the ideology of fascism, extremism, terrorism, and separatism, and to endanger the civil peace and political and

---

[83] See also United Nations General Assembly, "Calling of an International Conference on Freedom of Information", Sixty-fifth plenary meeting, 14 December 1946. See also Kennedy, "When Renewal Repeats, Thinking against the Box", p. 363-365.

[84] Conference for Security and Cooperation in Europe Final Act, Article I (Helsinki, 1975).

[85] "VII BRICS Summit Ufa Declartion", Ufa (17 July 2015).

social stability in society".[86] In defence of their sovereignty against foreign interference and interventions and within such as rather absolutist reading of sovereignty information has become suspicious commodity.

Information, technologies and market, can be seen to change the practise of both sovereignty and territorialism but not necessarily challenge sovereignty as an absolute value.[87] Claims and reclaims of sovereignty have yet become common. Communal voices of local autonomy and national authority target cosmopolitanism in India and federalism in the EU, shout often against globalization, liberalism and market economy, and oppose Western, that is American unilateralism and hegemony.

ECONOMIC EQUALITY

The right to share the benefits of scientific and technological development has been on the UN agenda since 1946. The right became a binding norm in December 1966, when it was included in Article 15 of the International Covenant on Economic, Social and Cultural Rights recognizing "the right of everyone to enjoy the benefits of scientific progress and its applications".[88] Similar proclamations are found in the Article 13 of the 1948 American Declaration of the Rights and Duties of Man stating every person's right "to participate in the benefits that result from intellectual progress, especially scientific discoveries", in the Article 27 of the 1948 Universal Declaration of Human Rights stipulating everyone's right "to share in scientific advancements and its benefits" as well as in the 1975 Helsinki Final Act calling for scientific cooperation.[89] The debate has remained on the UN Educational, Scientific and Cultural Organization (UNESCO) agenda.[90]

Referring the right to development and modern technologies, developing countries have been requesting transfers of modern technology and capacity-building. In the field of ICTs the quest to close capability gaps started with the establishment of the UNESCO International

---

[86] President of the Federation of Russia, "The Russian Federation's National Security Strategy", Presidential Edict 683 (31 December, 2015); see also "Remarks by H.E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference", Wuzhen (16 December 2015).

[87] Barry Buzan, An Introduction to the English School of International Relations (Cambridge: Polity, 2014), p. 139-143.

[88] United Nations General Assembly, "International Covenant on Economic, Social and Cultural Rights" (16 December 1966, entering force in 3 January 1976).

[89] Organization of American States, "American Declaration of the Rights and Duties of Man" (Bogota, 1948); United Nations General Assembly, "Universal Declaration of Human Rights" (Paris, 1948); Conference for Security and Cooperation in Europe Final Act, Article IX and "Co-operation in the Field of Economics, of Science and Technology and of the Environment", Chapter 4.

[90] Julian Huxley, "UNESCO Its Purpose and Its Principles", Preparatory Committee of the United Nations Educational, Scientific, and Cultural Organization (UNESCO, 1946); UNESCO, "The Right to Enjoy the Benefits of Scientific Progress and its Applications" (16-17 July, 2009). See also United Nations General Assembly, "Calling of an International Conference on Freedom of Information", Sixty-fifth plenary meeting (14 December, 1946).

Computation Centre in 1951. The Centre was to support the development and diffusion of informatics, and to advise, promote and recommend national and international actions concerning the adoption of informatics policies as well as to the enhance administrative methods through informatics, improve education in and through informatics, and research, education and development programs. Similarly, a UNESCO based entity, the International Federation for Information Processing was founded in 1960, with a mandate to support information processing within its member countries and to encourage technology transfers to developing nations, enhancing and assisting in the development, exploitation and application of information technology for the benefit of everyone.[91]

Technological capability and performance gaps have always existed not only between industrial and developing countries but also between the western nations. In the 1960s American mainframe computer technology surpassed the European one leading to the gradual demise of European indigenous computing industry;[92] on the other hand European nations have been more agile than the U.S. to develop and deploy mobile technologies and e-services. In the field of military cyber performance the U.S. remains ahead of its allies and partners.

The West has taken a lukewarm stand on the pleas of technology transfers. Industrial countries have been protective for economic reasons and restrictive for political-strategic reasons. To restrict the harmful proliferation of dual-use technologies, Western countries have imposed export controls. One of the key objectives of the Cold War export-control system was to prevent the Soviet Union from using Western-made microprocessors and computers as components of weapons systems or for air defence, anti-submarine warfare, battle management and weather prediction. Restrictions on access to advanced and sensitive technology provoked countermeasures by the Eastern Bloc. In 1975 the UN General Assembly adopted a Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind. The draft declaration was presented by the Soviet Union, together with its allies, and adopted without the support of Western states. The declaration began a divergence between East and West in the UN debate on human rights and scientific and technological developments that would last for many years. The socialist countries endeavored to link human rights with peace and disarmament, emphasizing the benefits of development made possible by the transfer of science and technology.

---

[91] UNESCO, "International Computation Centre", http://atom.archives.unesco.org/international-computation-centre.

[92] See Commission of the European Communities, 'Community Policy on Data Processing', SEC (73) 4300 final (21 November 1973), where the European Commission expresses its concern of the IBM market dominance and ensures to be vigilant in the matter.

THE ROLE OF THE STATE

Among the first recorded public concerns of the use of computers in summer 1966, centred on the relationship between the State and the individual. The Johnson administration had initiated a plan to computerize public administration, a decision that led to critique from the right and the left. Many republicans feared that federal data centres would pave way to Orwellian big government, and many defenders of civil liberties feared of Benthamian surveillance society. In the US House of Representatives hearings on the loss of individuality and privacy in the context of the potential establishment of a centralized national database Paul Baran, one of the leading computer scientists, considered the problems of privacy significant, especially where individual data systems were tied together into a network. He warned computer and communications systems being open to tampering and exploitation and suggested proceeding "slowly and cautiously to insure that proper safeguards are built into the systems for the outset".[93]

The enhanced State intelligence gathering and big data analytical capacities, and the Snowden revelations tabling the U.S. and U.K. government mass surveillance practices, have increased the demands to limit or better define the powers of the security state. More mature analyses call for nations to agree upon a point-of-balance between as such legitimate demands of freedom of information, right to privacy, and national security.[94] Such a social contract between the State and the citizen needs constant revision as our political and social pattern of behaviour and levels of tolerance can change rather fast as smart and connected technologies develop and as violent extremist organizations exploit technologies and services. Many governments have recently revisited or redrafted their intelligence legislation and surveillance practises.[95] Culminates in the EU-US safe harbour and data centre disputes

MILITARY USE OF CYBERSPACE

Two fundamentally different claims set the scene. China and Russia, in particular, want to avoid legitimizing the deployment and employment of cyber or information weapons and warfare. They regard any explicit reference to International Humanitarian Law (the Law of

---

[93] The Computer and Invasion of Privacy, hearing before a subcommittee of the Committee on Government Operations, US House of Representatives, 26–28 July 1966 (Washington DC: US Government Printing Office, 1966), pp. 119–35.

[94] Eneken Tikk-Ringas with Agnes Zaure, "Norms for International Peace and Security: Privacy, Freedom of Information and National Security", The ICT4Peace Norms Project (April 2015 in conjuction with the 2015 Global Conference of Cyber Security, The Hague).

[95] Her Majesty's Government has introduced a new bill; the Finnish government has proposed a foreign intelligence act authorizing the Defence Forces to conduct network intelligence operations for the puposes of national defence, but being cautious of police on-line operations. On the other hand many developing countries governments are eager to acquire network intelligence and mass surveillance capabilities.

Armed Conflict) and its principles permissive. This absolutist stand to war and peace is countered by the United States and the like-minded who regard its principles prohibiting. They notice the employment of cyber capabilities in conflicts and consider the substantiating International Humanitarian Law offering protection to civilian population and property.

The discussion is also about solving the issues by banning 'cyber weapons' or specific use of them contra issuing rules of engagement to regulate their use, for example targeting in line with the International Humanitarian Law.[96] Russia and China paint a picture of unlawful use of ICTs to threaten not only international peace and security but also the very existence of mankind with references to weapons of mass destruction. Russia is nevertheless more permissive to rules of engagement than China, which rather categorically refuses such relativist openings to "legitimize cyber war".

DEVELOPMENT OF INTERNATIONAL LAW

The three claims on the importance of State behaviour, novelty, significance, and instrumentality, converge in the demands for new International Law, a treaty, to define and govern State behaviour and inter-state relations. The core issue stems from regarding the Law either as dead or alive: is the existing Law sufficient to be applied also in cyberspace. Whereas the Russian Federation has advocated for a new treaty, the United States has held a firm stand that the question is not whether, but how the International Law applies.

After a lengthy debate launched by the 1998 Russian letter expressing concerns on "the creation of information weapons and the threat of information wars", the UN GGE concluded in 2013 and reiterated in 2015 that "international law and in particular the United Nations Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment".[97] This recognition has not ended but enhanced discussion of the applicability of IL. The focus is shifting to specific issues, such as the exercise of sovereignty and neutrality, non-intervention and territoriality in cyberspace.

One way the international community has tried to move forward is to develop norms, rules and principles. The UN GGE, for example, was mandated to "identify further voluntary, non-binding norms for responsible State behavior" which were seen to "reduce risks to

---

[96] Andrey Krutskikh and Anatoli Streltsov, "International Law and the Problem of International Information Security", International Affairs, No. 6 (2014) p. 64-76.

The 2015 GGE Report balances between the absolutist and relativist stands by not explicitly referring to IHL/LOAC by name but referes to some principles of Jus ad bellum and Jus in bello.

[97] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/68/98 (24 June, 2013), also the 2015 Report (UNGA, A/70/174 (22 July, 2015)) with one chapter elaboration how international law applies to the use of ICTs.

international peace, security and stability" as well as "to prevent conflict in the ICT environment".[98]

Referring to the legal concept of due diligence the White House international cyber strategy (2011) calls for responsible State behaviour. It links international behavior in cyberspace to norms by calling for clearly agreed norms of acceptable state behavior, which would be grounded "in the principles of responsible domestic governance, peaceful interstate conduct, and reliable network management".[99]

The Russian Federation together with China, Tajikistan and Uzbekistan submitted "Code of conduct", a set of eleven voluntary measures countries should take "to identify the rights and responsibilities of States in information space, promote their constructive and responsible behaviors and enhance their cooperation in addressing the common threats and challenges in information space, so as to ensure that information and communications technologies, including networks, are to be solely used to benefit social and economic development and well-being of people, with the objective of maintaining international stability and security".[100] The "International code of conduct for information security" has been noted in the UN GGE reports, but otherwise it has not gained wider traction. For the west its maxims stressing State sovereignty, territoriality and national exceptionalism are not explicit and binding enough.

The debate of hard law or non-binding instruments being appropriate ways to develop IL is rather scholarly one; it follows the fault lines of 'dead law' vs. 'live law' and lex late v. lex ferenda. On the one hand the existing International Law, the Treaties, are read and re-read in a hermeneutic manner,[101] on the other hand the advocates of comprehensive normative approach want a wider platform to develop international normative instruments.[102] Norms

---

[98] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174 (22 July, 2015)); Andrey Krutskikh, "Remarks", UNIDIR Workshop on (March 2016).

[99] The White House, International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World (May 2011), p. 9-10.

[100] "The Code of Conduct in the Field of Ensuring International Information Security: Letter dated September 12, 2011 from the permanent representatives of Kazakhstan, Kyrgyzstan, China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General". A/66/359.

[101] Tallinn Manual (complied by Michael N. Schmitt (Tallinn: CCDCOE, 2012)) offering interpretations of twenty Western legal experts follows this suit. See also Michael N. Schmitt and Liis Vihul, "The Nature of International Law Cyber Norms", Tallinn Papers no. 5, CCDCOE (2015)

[102] Eneken Tikk-Ringas, "Comprehensive Normative Approach", The ICT4Peace Norms Project (April 2015 in conjuction with the 2015 Global Conference of Cyber Security, The Hague).

serve the purposes of both schools of thought: they can develop, harden, to treaty law and they deal, as soft law instruments, with issues at hand.[103]

The following example illuminates how technological, political and legal claims and discourses intertwine and can create amplifying effect across the domains: The ability to conduct cyber forensic investigations and attribute a cyber incident to an actor is a critical and evolving capabilities. Lack of sufficient attribution limits States ability to detect in explicitly unauthorized access, intrusion and exploitation of State systems and networks by State or State sponsored actors. Developing capacity to attribute States would increase deterrence in cyberspace and lift the threshold of such potentially coercive and destabilizing activities. With improved attribution States could also start to address such acts as breaches of sovereignty. Repeatedly taking a stand against e.g. State espionage or other exploitation of computerized system would create custom and opinion juris which could enable to close a gap between unauthorized behaviour and the existing International Law. A relevant to International Law observation is that the advancement of technology has enabled capable States to employ means and methods claimed legal that otherwise would have been considered illegal.[104] These are not limited to attribution but can include the capabilities of prevention, detection and response (of/to cyber attacks). Such potential and temptation of malicious use exists in every asymmetrical relationship.

CONCLUSION: MODELLING STATE BEHAVIOUR

The theories of International Relations and International Law easily identify [national/self] interest as an instrumental and egoistic reason of State behaviour. In particular power and economic prosperity are acknowledged as objectives of their own right but also as instruments. Policy and action based analysis inevitably approximates rational and strategic behaviour assuming State interest theories. States, i.e. governments also eagerly label their actions as well as normative intentions as interests. States are, however, not monolithic actors and national decision-making as extensive studies show is more based on multiple actor bargaining, bureaucratic politics and far-than optimal compromises than pure reason and calculation.[105] The notion of self-interest as a Meta theory remains too blunt an instrument to explain State behaviour as doings and wants.

---

[103] The 'cyber discource' reflects the geneal discourse on the development of international law that has emphasised either norms development, treaties or institutionalism. See Kennedy, "When Renewal Repeats, Thinking against the Box", 350-354.

[104] Louis Henkin, How Nations Behave, Second edition (New York, NY: Columbia University Press, 1979), p. 103-104.

[105] See for example Graham T. Allison and Philip D. Zelikow, The Essence of Decision (New York, NY: Longman, 1999); Morton H. Halperin and Priscilla Clapp, with Arnold Kanter, Bureaucratic Politics and Foreign Policy (Washington, D.C.: Brookings

On the other hand, International Law contains a belief in and a doctrine of altruism. States are considered in consenting to norms and legitimate processes also to act on principal and virtuous reasoning. Internalization of norms and patterns of behaviour takes place through multi-stakeholder and international processes. State behaviour, thus, can be as much of prestige and self-image, than on self-interest. Whether and how much ideational and material consideration condition or determine actor's behaviour is a debate that cannot be in this field either.[106]

States can also act to enhance or maintain functionality of the international political and legal system, and in the context of ICTs, the functionality of e.g. cyberspace, the Internet and global information infrastructure. Similarly, domestic political, administrative and technical system functionality are enhanced. The difference between interest and functionality as primary reasoning is that whereas the self-interest is often regarded absolute, a zero-sum equation functionality is more permissive to shared interests and relative gains.

Combining motivations with the level of engagement a State has provides a framework to conduct more nuanced analysis of State behaviour and attitudes. The values attached to particular kind of State behaviour are methodological characterizations that help to construct a typology of greater precision and penetrative force.[107]

	SELF-INTEREST	**VIRTUE**	**FUNCTIONALITY**
Extreme	Opportunist	Evangelist	Technocrat
Strong	Pursuant	Shaper	Exporter
Weak	Adapter	Follower	Importer
Non-existent	Impotent	Withdrawn	Dysfunctional

Table 3. State role as a function of the primary reasoning (Self-interest, Virtue, Functionality) and level of engagement (Non-existent…Extreme). Author's compilation.

Institution, 1974); and Martha Finnemore, National Interest in International Society (Ithaca, NY: Cornell University Press, 1996).

[106] Koskenniemi, "The Subjective Dangers of Projects of World Community", p. 3-13; Guzman, "A Compliance Based Theory of International Law", p. 11. On ideational and material consideration in International Relations, see for example Alexander Wendt, The Social Theory of International Politics (Cambridge: Cambrigde University Press, 1999).

[107] Holsti, "National Role Conceptions in the Study of Foreign Policy", p. 233-236. The table does not indicate any preference or horizontal or vertical progression.

Two country examples help to show how the model functions. Another analysts may come up with different questions and answers as the matrix operates as a methodological framework of inquiry. In developing public e-services Estonian state has a strong self-interest to have a resilient and lucrative national administrative system and services. It has for the sake political interest and technical functionality exported, for free, the backbone of the system, X-Road to Finland. This move helped to create compatible services for the residents of the both countries encouraging cross-border economic activities. Estonia is also eager to develop and market its e-government experience. Drawing from the dynamics of the model, one can, for example, ask how global or encompassing does this virtuous effort in terms of international capacity building or domestic research and education, need or has to be. On the other hand Singapore, another top ranked ICT/cyber nation has taken a functional approach to its infocomm as well as cyber security plans. The government is advocating for technology - first policy where even economy comes second to technological advancement. Despite of being capable in applying ICTs Singapore does not have impetus to promote its solutions. Its self-interested cyber strategies are very inward looking.[108]

As patterns of State behaviour we can firstly identify States either to adapt their behaviour to the operating environment or seek to adapt the operating environment to their ambitions.[109] Secondly, States can be seen to maximize their effect while minimize adversary effects. These dualistic patterns materializing, for example, in national cyber or information security strategies constitute the third pattern: to support national ambitions States seek to shape cyberspace though advocacy of values such as ideology and belief systems, selling or transferring technology and capabilities, or promoting economic, governance and development models. This positive pursue of interests takes place at the same time with the efforts to reduce malicious use through deterrence by denial and making the threat of punishment more credible, in short making non-compliance more expensive than compliance. States also conduct targeted operations in and through cyberspace to reduce threat actors and vectors. Fourthly, cyberspace is for States and lucrative environment to conduct political information operations as well as to operate below the already unclear thresholds of use of force and armed attack. Finally, and perhaps most importantly in this context, the use of normative power is an increasing feature. Although, or because a Treaty approach to en masse cyber affairs is unlikely, the power and skillset to develop and deploy normative instruments across the fragmented and complex regime field has become a necessity, even a virtue. The majority of countries are yet not capable to explicitly express

---

[108] On Singaporean thinking see "Realising the iN2015 Vision. Singapore: An Intelligent Nation, a Global City, Powered by Infocomm", Infocomm Development Authority of Singapore (2010); "Singapore's Infocomm Security Masterplan 2018", Infocomm Development Authority of Singapore (2013); Opening Speech by Dr Vivian Balakrishnan, Minister-In-Charge of the Smart Nation Initiative at IoT Asia 2016 (30 March 2016).

[109] See for example Alabama as an example where Britain was able to create for her a favourable legal opinion strengthening neutrality of neutral State's in conflitcs.

their legal opinions or particular concerns regarding the use of ICTs and subsequent rules, norms and principles. This tends to leave the discourse and the development of International Law to the hands of vocal legal experts or aligned groups of countries, most importantly the U.S-led camp of the like-minded, and the BRICS led by China and the Russian Federation.

Accepting the claim that the on- and off-line politics of foreign relations and security do not differ, leads to assume that the potential and the limits of Law in cyber domain and affairs are similar as elsewhere. States effectively exploit law for their self-preservation. The 1923 Permanent Court of Justice the Wimbledon ruling recognized not only the customary rule of the Kiel Canal, as an international waterway, but also that the Court declined "to see in the conclusion of any Treaty by which a State undertakes to perform or refrain from performing a particular act an abandonment of its sovereignty."[110] States taking or not taking legal responsibilities, leaving or not leaving reservations, or recognize or not recognizing jurisdiction of international courts or other arbitration mechanisms are exercising their sovereignty. For example, the U.S. has due to its concern about possible charges against U.S. nationals no intention to join the International Criminal Court, China "does not accept the arbitration initiated by the Philippines" on the South China Sea issue,[111] and whereas Sweden, i.e. the current Swedish government, recognized the Palestinian state as equal and sovereign, Finland has not.[112]

Are international relations doomed to the geopolitical game of the powerful or can International Law provide protection and predictability? A rather permissive note would echo Louis Henkin's maxim that "almost all nations observe almost all principles of international law and almost all of their obligations almost all of the time."[113] Compliance to laws, rules, norms and principles is, in other words, not absolute. To enhance the protection and predictability the International Law could provide, we need not only to understand State behaviour sui generis but also the modalities of behaviour. State behaviour, although, not always pre-planned is nevertheless not accidental and in forms of words and deeds reflect their ambitions and concerns.

The main limits of International Law, according to this study, are, firstly International Law that is what States make of it. Static modus operandi is not of that of a legal scholar but

---

[110] Permanent Court of Justice, Case of the SS "Wimbledon" (17 August, 1923), p. 25.

[111] Permanent Court of Arbitration, The Republic of Philippines v. The People's Republic of China, case no 2013-19. The SS Wimbledon ruling continues as follows: "But the right of entering into international engagements is an attribute of State sovereignty" (Permanent Court of Justice, op.cit.).

[112] See also Ralph, "International Society, the International Criminal Court and American Foreign Policy", for an argument of a tension between sovereignty in the context of international society and individual rights in the world society. (Jason Ralph, "International Society, the International Criminal Court and American Foreign Policy, Review of International Studies, Vol. 31, No. 1 (Jan, 2005), pp. 27-44.)

[113] Henkin, How Nations Behave.

that of a politician. The respect of and adherence to Law is calculative. In the context of ICTs and in cyberspace States are as self-interested, virtuous or functional as elsewhere: behaviour on-line is as good, bad or ugly as behaviour off-line. Secondly, the claims of responsible State behaviour or conduct are contingent, lessening the prospects of agreement. Thirdly, claims and concepts used and uttered are far from substantiated: what are we talking about when we are talking about e.g. sovereignty. Finally, the narrower our reading of International Law is, the narrower its windows of opportunities appear. A permissive view on International Law recognizing soft law, working on politically binding and voluntary instruments, and applying rigorous methodologies to study the principals of International Law, national legislation as well as national custom, beliefs and behaviour, are needed to take us forward.

COMMENTARY

TO RECOMMENDATIONS FOR VOLUNTARY, NON-BINDING NORMS, RULES OR PRINCIPLES OF RESPONSIBLE BEHAVIOR OF STATES AIMED AT PROMOTING AN OPEN, SECURE, STABLE, ACCESSIBLE AND PEACEFUL ICT ENVIRONMENT

(PARAGRAPH 13 OF THE REPORT OF GROUP OF GOVERNMENTAL EXPERTS ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY,SEVENTIETH SESSION OF THE UN GENERAL ASSEMBLY, 22 JULY 2015, A/70/174)

A. A. Streltsov

The proposed commentary is an article-by-article analysis of the content of the recommendations for voluntary, non-binding norms, rules or principles of responsible behavior of states aimed at promoting an open, secure, stable, accessible and peaceful ICT environment. The recommendations proposed by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (paragraph 13 of the Report of the Group of the Seventieth session of the UN General Assembly, 22 July 2015, A / 70/174).

Commentary was prepared considering the provisions of the UN Charter, Declaration on Principles of International Law[114], Convention on the Law of Treaties[115] and other sources of international law.

The Commentary contains author's views on the content of norms, rules and principles of responsible behavior of states from the position of their use together with the provisions of the norms and principles of international law when regulating international relations in the ICT environment.

---

[114] Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations. UN GA Resolution 2625 of 24 October 1970.

[115] Convention on the Law of Treaties. Vienna, 23 May 1969.

DRAFT – shared with the participants of the ICT4Peace Workshop on

Existing and future norms on international ICT infrastructure and data integrity

The Commentary is addressed to all professionals in the field of international law concerned with its application to the ICT environment, scholars and other citizens interested in the development of international law in the context of globalization of information space.

1. General provisions

1. Responsible conduct of states in international relations consists, above all, of compliance and respect to principles and norms of international law, the sources of which are: general and specific international conventions; international custom, as evidence of general practice accepted as
2. Law; general principles of law recognized by civilized nations. Decisions of the International Court of Justice (for parties participating in a case and just in the present case) and doctrines of the most highly qualified public law experts stand as auxiliary aids for determination of legal norms.

2. The intensive development of information and communication technologies (hereinafter referred to as ICTs), expansion of the use of ICTs for meeting needs of a person, organizations and a state stipulating emergence of the ICT environment and its increasing influence on development of modern society, emergence of ICTs designed to use by states as "force" in international relations, significant distinctions between ICTs and other means of "force" action against an opposing state as well as caused by those distinctions, complexity of the application of norms and principles of international security law and international humanitarian law to international relations in the ICT environment require improvement of the relevant international norms, principles and practices.

3. The term "ICT-environment" is not explained in universal international acts.

In the Russian legislation and information materials in English ICTs is explained as processes, methods of research, collection, storage, processing, reporting and distribution of information, and approaches towards implementation of these processes and methods[116] [117].

ICT-environment (hereinafter referred to as ICT sphere) is formed, on the one hand, by combination of objects related to ICTs and providing application of these technologies in all spheres of society, and, on the other hand, by plurality of public relations concerning the

---

[116] Federal law of July 27, 2006, no. 149-FZ "On Information, Information Technology and Information Protection"

[117] ICT (information and communications technology - or technologies) is an umbrella term that includes any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on as well as the various services and applications associated with them, such as videoconferencing and distance learning. ICTs are often spoken of in a particular context, such as ICTs in education, health care, or libraries. The term is somewhat more common outside of the United States. www.earchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies.

use of ICTs in order to contribute to achieving goals of public life actors (citizens, organizations, public authorities) constituting the ICT sphere of society.

3. In the ICT sphere, there are two main components - "cyberspace" and "space of expression, freedom of association, privacy and other human rights, education, promotion of ideas (including religious and political, promoting hate, inciting to discrimination and violence) on the Internet"[118], in other words "space of information and meanings".

The term "cyberspace" can be explained as a part of information space featuring "an electronic (including photoelectronic and etc.) medium through which information is created, transmitted, received, stored, processed, and deleted"[119]. Therewith, "electronic environment" is a collection of systems of technical means ensuring propagation of electromagnetic waves through wired and wireless communication channels for transmission of information (means of communication) as well as systems of technical means ensuring implementation of data processing algorithms (electronic computing machines), i.e. "technical equipment and systems of creation, conversion, transmission, use and storage of information" forming "information infrastructure" of the society.

4. As part of cyberspace, one distinguishes:

Technical environment of collection, transmission, storage and processing of information, formed by a set of networks of computer equipment, networks of communications equipment and networks of means of information storage;

ICTs defining methods and ways of use of engineering environment to meet needs of a particular actor in cyberspace (person, organization, public authority as well as actors of armed conflicts, and criminal, including terrorist organizations) related to collection, transmission, storage, receipt or distribution of information;

Local or distributed information systems, automated control systems of production and human activities.

Cyberspace features by globality which express in integration of cyberspaces of various states into a single cyberspace providing possibility of information interaction of people in different countries; use of ICTs with the assistance of means of computer technology, network communications and networks of means of information storage as well as

---

[118] The promotion, protection and enjoyment of human rights on the Internet. Resolution adopted by the Human Rights Council. 14 July 2014. A/HRC/RES/26/13.

[119] Russia – US Bilateral on Cybersecurity. Critical Terminology foundations. East West Institute World wise Cybersecurity Initiative, Moscow state university information security institute. November 2013. http://wiki.informationsecurity.club/lib/exe/fetch.php?media=documents_all:russia-u_s_bilateral_on_terminology_rus.pdf.

information systems, automated control systems of production and human activities located in different countries.

Globality of cyberspace is supported by logical and physical integration based upon unified systems of digital labeling of objects, network communication protocols, computing systems and communication devices of national electronic environment in a single electronic environment of collection, transmission, storage and processing of information.

5. "Space of information and meanings" is formed by a set of social relations regarding freedom of thought, content of messages and data. Information is the result of reflection of the world, including messages and data, in the human body and can manifest itself in the form of his or her thoughts. Thereby, "message" consists of a set of characters which with the help of information can be transferred from one person to another and perceived by him/her, "data" consists of messages presented in a form accessible to treatment with the use of computer and communication equipment[120].

In dictionaries, the term "meaning" is explained as "internal, logical content (words, speech, phenomena), sense comprehended by reason"[121]. At the same time, it is possible to define this term as a logical-emotional reflection of information in mind and the "unconscious" of human being generating his or her interests and motives of his or her actions.

"The space of meanings" includes both the subjective spaces of information and meanings of an individual, and the public space of this information and meanings.

The subjective "space of information and meanings" is formed by a set of ideas about environment, laws of its development as well as thoughts associated with needs, interests and human actions aiming to meeting these interests and carrying them on his or her own initiative, i.e. freely, or with impact of external circumstances, i.e. under duress.

The public "space of information and meanings" is formed by a set of common (similar in content) ideas for certain social groups or masses of people about environment, laws of its development and ideas related to common needs and interests as well as conforming actions of people towards meeting common interests, and are manifested in the form of concerted actions of this group or mass of people.

6. "Space of information and meanings" can be interpreted as "media sphere", a set of ideas, topics, opinions and other intangible entities represented by media texts that have

---

[120] Streltsov A.A. Ensuring Russia's Information Security. Moscow: Moscow Center of Continuing Mathematical Education. 2002. (Стрельцов А.А. Обеспечение информационной безопасности России. М., МЦНМО, 2002.)

[121] http://slovarsbor.ru/.

signs of importance, significance for different groups of audiences, immediacy, actuality and are open to numerous interpretations[122] (hereinafter referred as "media sphere").

7. As an object of state sovereignty the ICT sphere (cyberspace, media sphere) is a legal fiction that assumes possibility of considering this area as an integral part of the state territory.

In internal affairs, state sovereignty in the ICT sphere is expressed in the form of state jurisdiction (legislative, administrative and judicial).

In external relations, state sovereignty in the ICT sphere is expressed in its jurisdiction, the complex of its rights and duties defined by the principles and norms of international law enshrined in the state-recognized international treaties and international customs.

Currently, state borders outlining the spatial limit of state sovereignty in the ICT sphere are not defined.

There are no universal international treaties enshrining interpretation of norms and principles of international law and enabling to consider specifics of the ICT sphere of composition and structure, when applying principles and norms.

2. Preamble of paragraph 13 of the Report – "Taking into account existing and emerging threats, risks and vulnerabilities, and building upon the assessments and recommendations contained in the 2010 and 2013 reports of the previous Groups, the present Group offers the following recommendations for consideration by States for voluntary, non-binding norms, rules or principles of responsible behavior of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment"

Comments to the Preamble of paragraph 13 of the Report

1. Group's recommendations related to the norms, rules and principles of responsible behavior of states in the ICT sphere are described in the form of the "soft law".

2. The proposed norms, rules and principles of responsible behavior of states are not provided under duress and, therefore, are not norms of international law[123], but may be considered as a kind of basis for beginning of discussions on formation of customary international law for regulation of relations in the ICT sphere.

---

[122] Buryak M.A. Media Sphere: Conceptualization of the Term. Vestnik of Saint Petersburg State University. Ser. 9, 2014. No. 2. (Буряк М.А. Медиасфера: концептуализация понятия. Вестник СПбГУ. Сер. 9. 2014. Вып.2.)

[123] International Law. Edited by K.A. Bekyashev. Moscow: Prospect, 2015. P. 32. (Международное право. Под ред. К.А.Бекяшева. Проспект, М., 2015, стр. 32.)

3. **The object of international legal regulation** is cooperation of states in the ICT sphere.

4. **The subject of international legal regulation** is international relations in provision of open, secure, stable, accessible and peaceful ICT sphere.

5. The openness of the ICT sphere means accessibility of this sphere for people living in all countries of the world which is achieved through integration of national cyberspaces and media spheres in the global ICT sphere.

6. Security of the ICT sphere means protectability of society actors, who use cyberspace and the media sphere to address challenges they face from threats to national security of each of the states that are integrated into the open ICT environment as well as threats to international security and peace.

7. Stability of the ICT sphere means its property to promote completion of tasks faced by society actors under conditions of malfunction (temporary) of specific elements of cyberspace and media sphere.

8. Accessibility of the ICT sphere means constant ability to use cyberspace and media sphere to meet legitimate interests of society actors including interests related to implementation of human rights and freedoms.

9. Peacefulness of the ICT sphere means that states use potential of cyberspace and media sphere for peaceful settlement of international disputes in such a way that it doesn't endanger international peace and security, and justice[124], it avoids threat of force or its use both against territorial integrity or political independence of any state and in any other manner, which is inconsistent with the Purposes of the United Nations[125].

3. Subparagraph a) "Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security"

Comments to subparagraph a) of paragraph 13

1. **The object of regulation** in this norm is international relations in the field of cooperation.

[124] UN Charter. Article 2(3).

[125] Ibid. Article 2(4).

DRAFT – shared with the participants of the ICT4Peace Workshop on

Existing and future norms on international ICT infrastructure and data integrity

In accordance with the Declaration on Principles of International Law,[126] *international cooperation of States for maintenance of international peace and security* is one of the purposes of the UN. in accordance with the principle of international cooperation states that have the duty to cooperate with one another, irrespective of the differences in their political, economic and social systems, in the various spheres of international relations, in order to maintain international peace and security and to promote international economic stability and progress, the general welfare of nations and international cooperation, free from discrimination based on such differences.

2. This principle essentially expresses the underlying mechanism of the UN functioning, all activities of which in any field are based on cooperation of the member states of the Organization.

3. Based on the fact that threats to stability and security in the ICT sphere are among the most serious problems of the XXI century, the implementation of which can cause serious damage to the economy, national and international security, and taking into account that these threats equally focus against individuals and legal entities, national infrastructure and governments, public safety, state security and stability of the international community as a whole united by the global network, **the subject of regulation** in the commented principle is cooperation on issues of increasing stability and security of the ICT use.

4. **The purposes of regulation** are to enhance international cooperation in the areas of:

development and implementation of measures to increase stability and security in the use of ICTs;

prevent actions in the ICT sphere that can be considered as malicious or actions that can pose a threat to international peace and security.

5. Development and implementation of measures to increase stability and security in the use of ICTs assume joint activities of states to counteract the most dangerous threats that breach stability and security within the use of ICTs.

6. The analysis of the Group's reports allow outlining the following threats:

use of ICTs by states as a tool of prosecuting a war and directing reconnaissance and for political purposes;

acting of individuals, groups or organizations, including criminal organizations as agents in performing network subversive activities causing willful damage on behalf of other actors (public and non-state);

---

[126] Declaration on Principles of International Law. UN GA Resolution 2625 of 24 October 1970.

ability to create and use by states or non-state actors on large-scale base sophisticated malware tools and means that increase risk of misidentification of actors of malicious use of these means and unintended escalation of incidents in the ICT sphere;

uncertainty in terms of identification of source of malicious activities and a lack of common understanding of features of state actions in the ICT sphere creating risk of instability and misperception of these actions.

7. The following measures can be included to international cooperation actions of states to reduce threats and, consequently, to strengthen stability and security of ICTs:

political decisions of states to restrict or reject the use of ICTs as force or threat of force in international relations, to improve coordination of law enforcement bodies and special services activities aimed at identification of individuals, groups or organizations that perform intermediary functions in preparation and implementation of acts of malicious use of ICTs, when performing network subversive activities on behalf of other actors;

preparation and adoption of international treaties on criminalization of activities of persons and organizations associated with the development of the most common and complex ICTs, implementation of which is based on the development of botnets;

improvement of the efficiency of cooperation with the International Criminal Police Organization to prosecute those who are responsible for the preparation and commission of unlawful acts, which are based on malicious use of complex network ICTs.

8. Cooperation in the field of preventing the commission of actions in the ICT sphere that can be considered as malicious or actions that can pose a threat to international peace and security, can be done by performing series of measures for international cooperation of states, primarily such as:

identification and consolidation in a universal international treaty, characteristics of activities in the ICT sphere that are harmful or can pose a threat to international peace and security;

assumption of an obligation by states not to commit harmful and dangerous to peace actions in the ICT sphere;

development of the system of the facts (evidences) investigation of violations of obligations by states in preventing the commission of illegal acts in the ICT sphere.

4. Subparagraph b) "in case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences"

Comments to subparagraph b) of paragraph 13

1. **The object of regulation** in the commented norm is international relations in the field of investigation of incidents in the ICT sphere.

2. In international law, the term "incident" is quite widely used. Thus, the term "incident (international incident)" is usually defined as small or limited actions or accident that results in a wider dispute between two or more nation-states[127].

Incidents may not acquire the level of "international incident". Thus, a marine incident means an event, or sequence of events, other than a marine casualty, which has occurred directly in connection with the operations of a ship that endangered, or, if not corrected, would endanger the safety of the ship, its occupants or any other person or the environment[128].

In oil pollution, the term "incident" means any occurrence, or series of occurrences having the same origin, which causes pollution damage[129].

In marine pollution - an event that causes the actual or probable discharge into the sea of harmful substances or effluents containing such a substance[130].

In carriage – any occurrence or series of occurrences having the same origin, which causes damage or creates a grave and imminent threat of causing damage[131].

In bunker oil pollution – any occurrence or series of occurrences having the same origin, which causes pollution damage or creates a grave and imminent threat of causing such damage[132].

In the civil aviation, there are two terms[133] to name hazardous events in sphere of exploitation of the air equipment: aircraft incident and accident.

3. Taking into consideration the structure of the ICT "incident", it can affect both cyberspace and the media sphere.

---

[127] An international incident is a seemingly relatively small or limited action or clash that results in a wider dispute between two or more nation-states. en.wikipedia.org/wiki/International_incident.

[128] Code of International Standards and Recommended Practices for a Safety Investigation into a Marine Casualty or Marine Incident. 2008.

[129] International Convention on Civil Liability for Oil Pollution Damage (CLC).

[130] Convention on the Protection of the Marine Environment of the Baltic Sea.

[131]Convention on Civil Liability for Damage Caused during Carriage of Dangerous Goods by Road, Rail and Inland Navigation Vessels.

[132] International Convention on Civil Liability for Bunker Oil Pollution Damage.

[133] Convention on International Civil Aviation. Annex 13. Aircraft Accident and Incident Investigation. International Standards and Recommended Practices. July 2010.

Incident in cyberspace, generally, is associated with violation of functioning of the components of cyberspace – the electronic environment of collection and automated processing of information, ICTs defining processes of implementation of these operations as well as information systems and automated control systems.

Incident in the media sphere can be associated with the violation of the confidentiality of information, attempts to change its significance for a person, violation of freedom of speech and expression of thought as well as the abuse of this freedom.

4. The subject of regulation consists of relations within investigation of incidents in the ICT sphere including the general context of the event, the problem of responsibility attribution in the ICT sphere, as well as the assessment of nature and scope of consequences.

5. The general context of "international incident" in the ICT sphere is defined, above all, by the nature of international relations between the states affected by the "incident". This event can be caused by unforeseen government actions in the ICT sphere, which harm interests of individuals, government or armed forces of one or more states or, conversely, can be one of many deliberate, but minor provocations carried out by agents of one state against another state.

In the latter case, the incident can have more significant meaning.

6. Assessment of nature and scope of consequences of an incident in the ICT sphere, as well as attribution of responsibility for the incident to a state is intended to define a subject of international law, to which international legal responsibility in connection with the incident can be applied.

International legal responsibility of a state is legal consequences, which may ensue for a subject of international law as a result of acts or failures to act in case they violate international legal norms applicable to this legal relationship.

These consequences provide duty of a subject of international law to eliminate damage caused by it to another subject of international law through the breach of legal international obligation, or obligation to compensate material damage caused by actions that do not violate norms of international law, if such compensation is stipulated by a special international treaty.

7. Rules and principles of international law of state responsibility, including the ICT sphere, are mainly featured as international legal custom, although some of them are captured in conventional rules. Act of state could be characterized as internationally wrongful only on the basis of international law. Violation of international obligation occurs, when behavior or

act of the state does not comply with requirements of the obligation. Implementation of liability is based on customary and conventional law[134].

8. Considering that international relationships within incidents of the ICT sphere are not regulated by international treaties, international custom serves as the basic and, in fact, the only source of the law of international responsibility in this case. However, its use is associated with difficulties caused by peculiarities of the ICT sphere as an object of regulation.

9. The problem of responsibility attribution to a state in connection with an incident in the ICT sphere resides in qualification of acts of bodies, agents, representatives of a state and other persons and entities as an act of a state[135]. As a general rule of international responsibility attribution, a state is responsible for acts of all its bodies and officials. Therewith, a state cannot be attributed responsibility for behavior of individuals, but it can be attributed international responsibility for its actions in connection with actions of individuals.

Due to the foregoing nature of the ICT sphere, the issue of attribution of incident actors in the ICT sphere, as well as attribution of international responsibility of a state in connection with an incident in the ICT sphere, is very complex.

10. Investigation of an incident can be based on two assumptions:

presumption of credibility of an injured state to its law enforcement and special bodies responsible for investigating the incident and having come to certain conclusions;

presumption of confidence in the third party (such as an authorized international organization).

Issue of responsibility attribution can be resolved by using techniques of peaceful settlement of international disputes: negotiation, inquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional bodies or other peaceful means at one's own option.

11. Use of peaceful means of settling international disputes on the basis of discussion of investigation results of an incident in the ICT sphere obtained on the basis of presumption of confidence in law enforcement bodies of an injured state is difficult due to:

lack of standardized methods and means of conducting such investigations and, consequently, forms of presentation of investigation results;

---

[134] Responsibility of state for internationally wrongful acts. Report of the Sixth Committee of the UN General Assembly. Moscow International UN Model. 2012. Moscow, 2011. (Ответственность государств за международно-противоправные деяния. Доклад 6 комитета Генеральной Ассамблеи ООН. Московская международная модель ООН. 2012. М., 2011.)

[135] International Law. Edited by K.A. Bekyashev. Moscow: Prospect, 2015. (Международное право. Под ред. К.А.Бекяшева. Проспект, М., 2015.)

possible mistrust to investigation results from other countries due to lack of means for objective monitoring of the ICT sphere facilities.

12. **The purpose of regulation** of the commented norm is to reduce risk of international disputes or conflicts through binding obligations on a state to examine all the relevant information in case of an ICT incident.

Basically, we are talking about development of certain international procedural norms governing enforcement activities of actors of international law in investigation of incidents in the ICT sphere.

13. These norms of procedure may, for example, include:

study of international obligations of states to prevent incidents and extent of their implementation;

determination of conditions and guarantees of fair fulfillment of obligations including in use of information obtained during execution of operational and investigative actions;

establishment of legal regime of computer data including traffic data that are of interest for investigative purposes;

determination of order for provision computer data of interest for persons authorized to carry out an investigation of an "international incident" in the ICT sphere, as well as provision of personal data necessary for investigation that is held by service providers or providers of Internet services, search and seizure of computer data by authorized bodies upon investigation of an "international incident" in the ICT sphere;

organization of collecting real-time data on traffic of objects in the ICT sphere that is of interest for authorized bodies carrying out investigation of an incident.

5. Subparagraph c) "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs"

Comments to subparagraph c) of paragraph 13

1. **The object of regulation** of the commented norm in terms of international security are international relations regarding obligations of states[136] to maintain international peace and security as well as upholding the restrictions imposed on states in armed conflicts.

[136] UN Charter. Article 2(4); Declaration on Principles of International Law. UN GA Resolution 2625 of 24 October 1970. The principle, according to which states shall refrain in their international relations from the threat or use of force against the

2. **The subject of regulation** are relationships in the ICT sphere that are considered as a part of the state territory to be used by the other states for commission of internationally wrongful acts.

3. State territory is a part of the globe with the Earth's interior and air space above it, which is legally located under the sovereignty of the state; it consists of land (with the interior), water and air space. Land area includes all land space with its interior within the state borders, as well as costal islands and enclaves. The Earth's interior under land and water surface of a state is under its complete and exclusive sovereignty. This right of peoples and nations is enshrined in many international legal acts. Water areas of a state include waters of rivers, lakes, bays, coves, ports and territorial waters (that have special regime). Surface and interior of the continental shelf as well as economic zones have special regime. The air space is space located above land and water areas (including territorial waters).

4. The ICT sphere, as a new component of the national territory, is a legal fiction that enables extension of the "sovereignty" concept of a state on it. According to some experts, the location of the physical components of the ICT sphere within the state territory (computer equipment, servers, channels and communication devices, etc.) allows considering it as part of this territory. At the same time, technical devices that have significant customer value are, in the first place, subjects of public relations, including international relations, because they allow exchanging of information, executing of access algorithms and processing information disposed in the global cyberspace, providing reliable information storage with the capacity of technical devices located in different states.

5. Identification of the objects of the ICT sphere in the process of information exchange is performed not through territory address of its location that is registered by public authorities, rather than through digital address issued by the American non-governmental organization Internet Corporation for Assigned Names and Numbers (ICAAN), which in accordance with the charter documents, exercises activities to support and develop the system of distribution and use of digital address space (domain name system).

Basically, the legal regulation in this case is based on the international custom as display of the general practice accepted as a law. In accordance with this custom, the ICAAN provides creation and updating of the global space of digital addresses (domain names) of actors and objects of the global cyberspace. This activity is an important factor of use of national cyberspaces' resources in the interests of different actors of society and state. At the same

---

territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations Organization.

time, the ICANN is not an international organization and, therefore, is not a subject of international law that has the international legal and passive dispositive capacity.

International relations in the field of operation of the digital system address space (domain name system) and provision of sustainability of this process are not regulated by universal international treaties.

6. Jurisdiction of a state related to usage of its territory is based on the state sovereignty. Providing state territory to another state for any purpose is related to the state's jurisdiction.

7. It can be assumed that within the jurisdiction of a state, the ICT sphere can be used by other states, for example, through providing:

the right to place objects of computer equipment or communication networks of these states within the sovereign territory;

the right to use digital addresses or objects of the ICT sphere to perform certain actions in the ICT sphere of another state.

8. An internationally wrongful act is an act or failure to act of a state which[137]:

is attributed to the state under international law;

is considered as a breach of an international obligation of this state.

9. Granting the sovereign ICT sphere to another state is performed on the basis of the relevant decisions of the authorized state bodies and from this point of view it can be considered as a deliberate action.

10. **The purpose of regulation** in the commented norm resides in expansion of international obligations of states in the ICT sphere as a new component of sovereign territory of a state and the sphere of display of threats to international peace and security.

11. There is no evidence of acts within application of ICTs in universal international treaties, which could be qualified as a breach of international legal obligations of a state, except, perhaps, the use of ICTs in the process of aggression[138] or carrying out a terrorist act[139]. For other cases, the possibility of practical application of the commented norm does not exist yet.

12. It is important to note that during investigation of facts of the usage of states' territories to commit internationally wrongful acts with the use of ICTs, one should consider that both subjective and objective components of these facts can have virtual character. In this

---

[137] International Law. Edited by K.A. Bekyashev, 2015. (Международное право. Под ред. К.А.Бекяшева.М., 2015.)

[138] Definition of Aggression. UN GA Resolution 3314 of 14 December 1974.

[139] Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations. UN GA Resolution 2625 of 24 October 1970.

regard, it is advisable to investigate these facts on the basis of the universal system of procedural rules.

6. Subparagraph d) "states should consider how to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect"

Comments to subparagraph d) of paragraph 13

1. The object of regulation are international procedural relations in the provision of legal assistance to states in fight against terrorist and criminal use of ICTs.

2. The main burden of struggle with these unlawful acts is laid upon a state.

In the Russian legislation:

a socially dangerous act, committed with guilt and prohibited by the Criminal Code of the Russian Federation under threat of punishment, is deemed to be a crime[140];

terrorism is called the carrying out of an explosion, arson or other actions creating the threat of human death, of infliction of significant property damage or the onset of other grave consequences, for the purpose of violating the public security, intimidating the population or influencing the taking of a decision by authorities and also the threat of commission of the said actions for the same purposes[141].

The law identifies three basic elements of a crime in the field of computer information, the performance of which involves the use of ICTs:

illegal access to legally-protected computer information, if this deed has involved the destruction, blocking, modification or copying of computer information (computer information means information (messages, data) presented in the form of electric signals, regardless of the facilities used for their storage, processing and transmittance)[142];

creation, dissemination or use of computer programs or other computer information, which are knowingly intended for unsanctioned destruction, blocking, modification or copying of computer information or for balancing-out of computer information security facilities[143];

---

[140] The Criminal Code of the Russian Federation, article 12.

[141] Ibid, article 205.

[142] Ibid, article 272.

[143] Ibid, article 273.

violation of the rules for operation of the facilities for computer information storage, processing and transmittance of information-telecommunication systems and of terminal equipment, as well as of the rules for access to information-telecommunication networks, that has entailed the destruction, blocking, modification or copying of computer information accompanied by causing a major damage[144].

The use of ICTs is not an independent element of committing criminal or terrorist acts. This, however, does not prevent socially dangerous act prohibited by Criminal law, which have been implemented with the use of ICTs, from qualifying it as a criminal act.

3. **The subject of regulation** of the commented rule are relations within international cooperation on provision of legal assistance to states in the fight against terrorist and criminal use of ICTs.

4. Cooperation of states in the fight against crime in the ICT sphere is caused, above all, by the states' need to coordinate efforts to prevent and combat criminal acts, identify perpetrators and to attribute the established legal responsibility to them, i.e. mutual assistance in criminal cases.

5. The Group believes that the need to strengthen international cooperation in this sphere is determined by: the terrorist and criminal use of ICTs that has spread to the ICT sphere; motives of criminal acts in this sphere are becoming more diverse - from a simple demonstration of technical skill and to the theft of money and information, or the commission of such activity as an additional form of conflict with a state; the main actors of considered criminal acts are criminal, including terrorist, organizations.

Terrorist organizations use ICTs to maintain contacts, gather information, recruit supporters, organization, planning and coordination of terrorist acts, promote their ideas and activities and fund-raising[145]. Despite the fact that the number of evidences of terrorists' attempts to jeopardize or destroy the ICT infrastructure or carry out operations with the use of ICTs was small, in the future such attempts can increase.

6. The existing international cooperation mechanisms do not fully contribute to full and rapid receiving of evidences from another state in the form of computer information[146].

Traditional forms of cooperation among states in the field of legal assistance in criminal cases provide forwarding of written petitions (requests) for legal assistance. This requires a relatively long time for their transfer, execution and receipt of written materials that

---

[144] Ibid, article 274.

[145] Ibid. article 205, 205.1, 205.2, 205.4.

[146] Volevodz A.G. Computer Crime Prevention: Legal Framework for International Cooperation. Moscow: Jurlitinform. 2002. (Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., Юрлитинформ. 2002.)

determines the loss of evidentiary information for investigation of crimes committed with the use of computer technologies.

Even measures taken quickly within mutual legal assistance, at best, can help to detect, remove and fix the "information trace" located on servers disposed in a certain state (e.g., a state of location of a victim or a host state of a person, who has committed a computer crime). When a computer message passes via telecommunication channels through the third (fourth, fifth) country, legal assistance can take considerably long time. The more countries through which the message is sent, the greater the likelihood that law enforcement authorities will not be able to trace the message until the end of the connection chain with the use of traditional forms of mutual legal assistance.

In most existing current international treaties on mutual legal assistance in criminal proceedings possibility of its provision in the forms of restricting the rights of citizens, determined by the principle of "double definition of crime", according to which, a state may not cooperate with the other one in investigation and prosecution of offenses that are not criminalized in the requested state.

7. **The purpose of regulation** in the commented rule resides in undertaking voluntary commitments by a state:

to consider the best ways of cooperation of states in exchange of information, mutual assistance, prosecution of those responsible for terrorist and criminal use of ICTs;

to carry out other joint measures, to counter threats of terrorism and crime in the ICT sphere.

8. The legal basis for increasing activity of states in the considered field lies in the resolution of the UN General Assembly (2001)[147], which noted the need to intensify efforts aimed at more effective fight against crimes related to the use of computers.

In particular, it recognized the importance of the following measures:

ensuring by states that their laws and practice eliminate safe havens for those who criminally misuse information technologies;

coordination of law enforcement cooperation in the investigation and prosecution of culpable actors of international cases of criminal misuse of information technologies by all concerned states;

exchange of information between states regarding the problems that they face in combating the criminal misuse of information technologies;

[147] UN GA Resolution "Combating the criminal misuse of information technologies". 22 January 2001. A/RES/55/63.

training and equipping of law enforcement personnel to address the criminal misuse of information technologies;

legal protection of the confidentiality, integrity and availability of data and computer systems from unauthorized impairment, and attribution of legal liability for persons culpable of abusing the use of ICTs for criminal acts;

legal protection of the safety of electronic data pertaining to particular criminal investigations and providing quick access to them;

improving mutual assistance regimes to ensure the timely investigation of the criminal misuse of information technologies and the timely gathering and exchange of evidence;

public notification of the need to prevent and combat the criminal use of information technologies;

improvement of the technological environment of information technologies development to help prevent and detect criminal misuse, trace criminals and collect evidence;

protection of personal liberties and private life of citizens in fighting against the criminal misuse of information technologies as well as the preservation of the capacity of governments to fight such socially dangerous phenomena.

7. Subparagraph e) "States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression"

Comments to subparagraph e) of paragraph 13

1. **The object of regulation** are the international relations in the field of human rights including the right to freedom of expression.

2. In accordance with the recommendations of the UN General Assembly[148]:

rights that people have offline must also be protected online, in particular, the right to freedom of expression, which is applicable regardless of frontiers and through any media of one's choice as well as the right to privacy, including the right to privacy in terms of digital communication, according to which no one shall be subjected to arbitrary or unlawful

[148] UN GA Resolutions A/RES/68/167 (2013), A/RES/69/166 (2014); Human Rights Council Resolutions of the UN General Assembly A/HRC/RES/20/8 (2012) and A/HRC/RES/26/13 (2014)

interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference.

Whereas states have pledged themselves:

to take measures to put an end to violations of those rights and to create the conditions to prevent such violations, by ensuring that relevant national legislation complies with their obligations under international human rights law;

to establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for state surveillance of communications, their interception and the collection of personal data;

to address security concerns on the Internet, in accordance with their international human rights obligations, to ensure protection of freedom of expression, freedom of association, privacy and other human rights online, including through national democratic, transparent institutions, based on the rule of law, in a way that ensures freedom and security on the Internet, so that it can continue to be a vibrant force that generates economic, social and cultural development;

combating advocacy of hatred that constitutes incitement to discrimination or violence on the Internet, including by promoting tolerance and dialogue.

3. **The subject of regulation** are relations regarding to ensure the comprehensive respect of human rights within implementation of measures as well as stability and security of the ICT sphere.

4. **The purpose of regulation** of the commented principle is to expand state's international obligations concerning respect of human rights on the activities related to ensure safe use of ICTs.

5. Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change religion or belief and freedom to exercise religion or belief, either alone or in community with others and in public or private practice, worship and performance of religious and ceremonial procedures, including with the use of ICTs.

Therewith, freedoms of thought and conscience imply freedom of independent formation of personal worldview, assessment of activity of other persons, non-governmental organizations and public authorities, taking into account views of non-governmental organizations, including political parties and state-run media.

Everyone has the right to freedom of opinion, to freely express themselves, regardless of frontiers and through any media of his choice, and to freely seek, receive and impart information and ideas, regardless of frontiers, either orally, in writing or in print, or any other forms of expression, or other media of his choice, including the media sphere.

The right to privacy means that no one shall be subjected to arbitrary interference in his or her privacy and family, arbitrary invasions on the sanctity of the home, the privacy of correspondence, nor to invasions on his honor and reputation, including with the help of the use of ICTs, cyber and media sphere. Everyone has the right to the protection of the law against such interference or attacks[149].

6. Compliance the state's commitments to respect human rights under countering security threats in the ICT sphere also takes into account the existence of certain obligations of the person to the community in which person can have free and full development of his personality[150]. In this regard, respect for human rights can be subject to certain restrictions, but these restrictions shall only be prescribed by law and be necessary: to respect the rights or reputation of others; to protect national security, public order, public health or morals[151]. These restrictions should be extended to the ICT sphere as an area of human rights and, above all, in the public relations related to cyberspace and the media sphere.

7. The obligations of a state to respect the human rights also include:

combating war propaganda[152], hatred that constitutes incitement to discrimination or violence on the Internet[153];

ban on:

direct or indirect interference in the decision on the formation, development and management of the ICT sphere relating to the domestic policy of any other state;

application and encouragement of usage of economic, political or any other type of measures to coerce another state, in order to obtain from it, the subordination of the exercise of its sovereign rights in the ICT sphere and to secure from it advantages of any kind; the use of the ICT sphere for the organization, foment, finance, incite subversive, terrorist or armed activities directed towards the violent overthrow of the régime of another state, or interference in civil strife in another state.

8. Subparagraph f) "A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public"

---

[149] The Universal Declaration of Human Rights. 10 December 1948. Article12.

[150] Ibid. Article 29.

[151] The Constitution of the Russian Federation. Article 55, paragraph 3.

[152] International Covenant on Civil and Political Rights. 16 December 1966. Article 20.

[153] Human Rights Council Resolution 26/13.

Comments to subparagraph f) of paragraph 13

1. **The subject of regulation** of the commented norm are social relations within international security related to damage to critical infrastructure.

2. In international law and the Russian legislation the concept of "critical infrastructure" is missing. The most extensive meaning seems to be captured by the concept of critical infrastructure used in the legislation of the USA and explained as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"[154].

3. **The subject of regulation** in the commented norm are international relations in the use of the ICT sphere by states aimed at damaging critical infrastructures.

4. The urgency of the problem, in the Group's view, determines, above all, by the fact that ICTs opening enormous opportunities for socio-economic development and getting more and more important for the international community create conditions for the malicious use of these technologies against critical infrastructures. This is indicated by the trend of increasing number of cases of ill-intentioned use of ICTs by public and non-state actors. At the same time, attacks using ICTs to critical infrastructure and related information systems constitute a real and serious danger.

States are justifiably concerned about the danger of destabilizing consequences of misconception of the intentions of the other side, the potential of international conflict occurrence in connection with this and the possibility of damage to their economies.

The Group noted that these trends pose a threat to all states and misuse of ICTs could harm international peace and security.

5. **The purpose of regulation** resides in undertaking voluntary commitments by a state on the prohibition of the deliberate and support activities in the ICT sphere, if such activities:

are contrary to the state's obligations under international law;

cause intentional damage to critical infrastructures;

otherwise prevent the use and operation of critical infrastructure to serve the population.

6. In accordance with the principle of prohibition of threat or use of force in international relations, each state is required not to carry out actions on organizing, instigating, assisting

[154] "Critical" infrastructure as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (Sec. 1016(e)). USA PATRIOT Act of 2001.

or participating in acts of civil war or terrorist acts in another state, and within its territory not to indulge organizational activity directed towards the commission of such acts, if they involve a threat or use of force.

7. Given that there is currently no universal international treaty governing relations in the field of combating terrorist activities, a state is governed by its national law when qualifying a socially dangerous act as a "terrorist act".

8. Activities of states in the ICT sphere directed against critical infrastructure of another independent state or to support such activities, acquiring features of a terrorist act[155], can be regarded as a violation of international obligations of the state arising, for example, from the principle concerning the obligations, in accordance with the UN Charter, not to intervene in issues within the domestic jurisdiction of any other state. Accordingly, it can be regarded as an internationally wrongful act.

9. The use of a state of the ICT sphere in order to impede the use or operation of critical infrastructures to serve the population, if it threatens the survival of the population[156], may be the content of an internationally wrongful act involving violation of the international principle of respect for human rights and fundamental freedoms (in particular the right to life) as well as the principle of non-intervention in domestic matters (in terms of encouragement or involvement of subversion by force[157]).

9. Subparagraph g) "States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions"

Comments to subparagraph g) of paragraph 13

1. **The object of regulation** of the commented norm are relationships regarding international cooperation on security of critical infrastructures. Issues of security of critical infrastructures relate to jurisdiction of states.

---

[155] Terrorist act is called the carrying out of an explosion, arson or other actions creating the threat of human death, of infliction of significant property damage or the onset of other grave consequences, for the purpose of violating the public security, intimidating the population or influencing the taking of a decision by authorities and also the threat of commission of the said actions for the same purposes. The Criminal Code of the Russian Federation. Article 205.

[156] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), article 54 paragraph 2.

[157] Declaration on Principles of International Law. UN GA Resolution 2625 of 24 October 1970.

2. **The subject of regulation** are actions against threats of the ICT sphere to ensure the safety of critical infrastructures.

3. Important areas of international cooperation regarding prevention of security threats of critical infrastructure arising in the ICT sphere are encouragement of safety culture formation in the society and provision of public safety facilities of critical information infrastructures used in their operation.

4. **The purpose of regulation** in the current context is the organization of international cooperation on actions against security threats of critical infrastructures.

5. According to the Group, the relevance of achieving this goal of international cooperation, in particular, is determined by the following:

states have the primary responsibility for providing security, including security of its citizens in the ICT sphere, and therefore - the security of critical infrastructures;

effective protection of critical infrastructures include, in particular, measures to detect threats and reduce vulnerability of critical information infrastructures, minimizing damage and recovery time in case of its damage or attempts of security breach, moreover, it includes measures to identify the causes of this damage or the source of such attempts, effectiveness of such measures can be enhanced, for example, through the exchange of information on best practices between states;

ensuring the effective protection requires cooperation at the national and international levels between all stakeholders that supports national efforts in this area.

6. The states have agreed within the framework of international cooperation[158] when developing the risk reduction strategies for critical information infrastructures in national legislations to take into account the following security elements:

existence of the communication networks for emergency warning of vulnerabilities, threats and incidents in cyberspace;

increasing level of awareness of states concerned about the nature and scope of their critical information infrastructures and about the role that states play in the protection of these infrastructures;

analysis of the structure of critical information infrastructures and identification of the factors that stipulate their interdependence and importance for strengthening the protection of such infrastructures;

---

[158] UN GA Resolution "Creation of a global culture of cybersecurity and the protection of critical information infrastructures" of 23 December 2003, 58\199.

assistance to development of partnerships between stakeholders from both public and private sectors to exchange information on critical information infrastructures and its analysis in order to prevent damage to these infrastructures or attempts to violate their protection, as well as to investigate cases of damage to objects of the most important information infrastructures;

development and support of operations of the communication systems in a crisis, and examination of them to ensure reliable and stable information exchange in emergency situations;

assistance in tracing attempts of attacks against critical information infrastructure facilities and, where appropriate, provision of information on the results of such tracing to other states;

provision of professional training and exercises to enhance response capabilities, examination of plans to ensure continuous operation and contingency plans in the event of attacks against critical information infrastructure facilities, and encouragement of stakeholders to take part in similar activities;

existence of an adequate substantive and procedural legal regulation, as well as trained personnel to investigate the attempts of violation of the security of critical information infrastructure facilities, detection and prosecution of persons involved in these attempts, as well as establishment of the procedure for coordination of such investigations together with other states;

participation, when it is necessary, in the international cooperation on protection of critical information infrastructure facilities, including through the development and coordination of the communication systems of urgent warning, information exchange on vulnerabilities, threats and incidents and analysis of such information, as well as coordination of investigations of attempts to attack such infrastructures in accordance with national legislation;

assistance to national and international academic researches and development activities and encouragement of the application of security technologies that meet international standards.

7. International cooperation in the field of protection of the objects of critical information infrastructures from malicious threats or hostile use of ICTs involves the formation of the relevant international information security systems using the foregoing elements of protection and aimes at preventing display of threats, identifying and fixing the facts of malicious or hostile use against the ICT security critical infrastructure, qualified investigation of the facts, identification of individuals responsible for such use of ICTs, and bringing them to responsibility imposed by law.

10. Subparagraph h) "states should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty"

Comments to subparagraph h) of paragraph 13

1. **The subject of regulation** in the commented norm are relationships regarding international cooperation between states on security of critical infrastructures.

2. In accordance with the principles of international law, states are obliged, regardless of differences in their political, economic and social systems, to cooperate with each other in various fields of international relations. One of the areas for such cooperation may be measures based on freedom from discrimination aimed at the maintenance of international peace and security, promotion of international economic stability and progress, the general welfare of the people, and in particular mitigation of the negative effects of infringements of critical infrastructures functioning as a result of malicious acts in the ICT sphere.

3. **The subject of regulation** in the commented norm are the international relations in the field of assistance to states, whose critical infrastructure suffered from the malicious acts against them in the ICT sphere, in order to reduce the negative consequences of such acts.

4. **The purpose of regulation** is the commented norm resides in undertaking voluntary commitments by a state on the provision of assistance to other countries, whose critical infrastructures suffered from the malicious acts against them in the ICT sphere in case such actions emanated from their territory.

5. In the commented norm, provision of assistance within international cooperation on a voluntary basis to other states stipulates a new kind of emergency - emergency arising in the ICT sphere as a result of malicious acts against critical infrastructures.

6. In accordance with the Russian legislation[159]:

the emergency situation is the situation in the certain territory which developed as a result of accident, the natural hazard, accident, natural or other disaster which can cause or caused, damage to human health or environment, considerable material losses and violation of conditions of life activity of people;

[159] Federal law of 21 December 1994 №68-FZ «On Protection of the Population and Territories from Emergency Situations of a Natural and Technogenic Character"

liquidation of emergency situations are the rescue and other urgent works which are carried out at appearance of emergency situations and directed on rescue of life and preserving of human health, decrease in the sizes of environmental damage and material losses, and also on localization of zones of emergency situations, cancellation of dangerous factors, characteristics of them.

7. In accordance with international law[160], every state is primarily responsible for assisting victims of natural disasters that occurred in its territory, and hence, the affected state should play the primary role "in the initiation, organization, coordination and implementation of humanitarian assistance within its territory".

8. In accordance with the principle of sovereign equality of states, international assistance is provided, above all, on the basis of existing international treaties and order and cases defined by these treaties.

9. By analogy with the procedure for international assistance in some other cases, enshrined in universal international treaties[161], it can be assumed that, if a state party to an international treaty needs assistance in the event of malicious act in the ICT sphere against its critical infrastructure, whether or not such accident or emergency originates within its territory, jurisdiction or control, it may call for such assistance from any other state party.

A state party requesting assistance shall specify the scope and type of assistance required and, where practicable, provide the assisting party with such information as may be necessary for that party to determine the extent to which it is able to meet the request. In the event that it is not practicable for the requesting state party to specify the scope and type of assistance required, the requesting state party and the assisting party shall, in consultation, decide upon the scope and type of assistance required.

Each state party, to which a request for such assistance is directed, shall promptly decide and notify the requesting state party, whether it is in a position to render the assistance requested, and the scope and terms of the assistance that might be rendered.

States parties shall, within the limits of their capabilities, identify experts, equipment and materials which could be made available for the provision of assistance to other states parties as well as the terms, especially financial, under which such assistance could be provided.

10. States affected by the malicious use of the ICT sphere against its critical infrastructure, may apply to the state, through the territory of which such actions emanated, on mitigating

---

[160] Strengthening the effectiveness and coordination of international urban search and rescue assistance. UN GA Resolution №57/150 of 16 December 2002

[161] The Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency. UN GA Resolution. 26 September 1986.

the effects of such actions in accordance with the Tampere Convention[162], if it is a party to the Convention.

11. In accordance with the Tampere Convention, states parties shall cooperate with each other and with non-state entities and intergovernmental organizations, in accordance with the provisions of the Convention in order to facilitate the use of telecommunication resources for disaster mitigation and relief operations.

Such use may include, but is not limited to:

the deployment of terrestrial and satellite telecommunication equipment to predict, monitor and provide information about natural hazards, health hazards and disasters;

the sharing of information about natural hazards, health hazards and disasters among the States Parties and with other States, non-State entities and intergovernmental organizations, and the dissemination of such information to the public, particularly to at risk communities;

the provision of prompt telecommunication assistance to mitigate the impact of a disaster;

the installation and operation of reliable, flexible telecommunication resources to be used by humanitarian relief and assistance organizations.

The states parties shall cooperate among themselves to improve the ability of governmental organizations, non-state entities and intergovernmental organizations to establish mechanisms for training in the handling and operation of equipment, and instruction courses in the development, design and construction of emergency telecommunication facilities for disaster prevention, monitoring and mitigation.

12. Currently, there is no universal treaty for assistance in emergency situations arising in the ICT sphere, as a result of malicious acts against critical infrastructure.

11. Subparagraph i) "states should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions"

[162] The Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations. 1998 // UN official website. URL: www.un.org/

Comments to subparagraph i) of paragraph 13

1. **The object of regulation** of the commented norm is relationships related to the delivery process of the ICT products to consumers in the world market.

As it is noted in the report of the Group of Governmental Experts (2010), states are concerned that the ICT supply chain may be subject to the attack or be broken in such a way that it will affect the normal, safe and secure use of ICTs. Installation in ICTs malicious hidden functions could undermine the trust in the goods and services, cause distrust to commerce and affect national security.

2. **The subject of regulation** of the commented norm is social relations concerning safety provision of ICT products supply chain to users during process of operation of the product, as well as preventing the spread of malicious software and hardware in the ICT sphere and the use of harmful hidden functions.

3. **The purpose of regulation** of the commented norm, in essence, resides in acceptance by states on a voluntary basis the responsibility for the safety of the use of ICT products that are received by end-users, regardless of where these products were produced.

In other words, the states, organizations of which produce ICT products, believe that is possible to attribute the responsibility for the safety of use of these products to the state in which end users are located. These states-consumers must take reasonable steps to ensure consumer trust in the security of ICT products available in the market.

4. Regulation of the relations concerning maintenance of the integrity of the ICT products supply chain, in accordance with the content of the commented norm, is related to issues of state sovereignty – the consumers of ICT products.

One of the possible means of performance of this state obligation is improvement of the system of technical regulation.

5. Technical regulation - legal regulation of relations in the sphere of establishment, application and meeting of the obligatory requirements for products or for processes of design (including survey works), production, construction, installation, adjustment, operation, storage, transportation, sale and reclamation connected with them, and also in the sphere of establishment and application on a voluntary basis of the requirements for products, processes of design (including survey works), production, construction, installation, adjustment, operation, storage, transportation, sale and reclamation, performance of works or rendering of services, and legal regulation of relations in the sphere of compliance evaluation[163].

[163] Federal law of 27 December 2002, № 184-FZ "On Technical Regulation".

6. Development of international cooperation on security of ICT products supply chain is not expected.

This is slightly discordant with the following threats to international security, highlighted by the Group (Report, 2013):

different levels of capacity for ICT security among different states can increase vulnerability in an interconnected world;

the possibility of the use of ICTs for both legitimate and malicious purposes;

the potential for the development and the spread of sophisticated malicious tools and techniques by states or non-state actors may further increase the risk of mistaken attribution and unintended escalation in the ICT sphere;

the potential for embedding harmful hidden functions in ICTs could be used in ways that would affect secure and reliable ICT use and the ICT supply chain for products and services, erode trust in commerce and damage national security.

7. Corporate rules of supply of ICT products to the world market, as well as the organization of support, these products at the stages of their exploitation do not contain mechanisms of national security controls of supplied and operated products. This fact further limits the possibility of the states-consumers of ICT products for provision of safety use of these products. At the same time, possibilities for implementation of some of the rules, norms and principles of responsible behavior of states in the ICT sphere (subparagraphs a), c), e), f), g) of recommendations on responsible behavior of states in the ICT sphere) are limited.

8. There are no international treaties that govern international cooperation on security of software usage released under free licenses and security of repositories with such a software that is widely used by many organizations producing ICT products.

9. The existing mechanism for ensuring the safe use of ICT products delivered to the world market does not stipulate international cooperation on countering threats to security breaches and sustainability in the ICT sphere. The Group named, in particular, such risks as:

development and widespread use of states or non-state actors sophisticated malware tools and means;

installation in ICTs hidden malicious functions that can be used to undermine the security and reliability of the use of ICT and the whole system of production and marketing of information system products and information technology services, to undermine trust between the parties of trade and cause damage to national security.

12. Subparagraph j) "states should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure"

Comments to subparagraph j) of paragraph 13

1. **The object of regulation** of the commented norm is the international relations regarding international cooperation on security issues in the ICT sphere.

2. **The subject of regulation** is the relationships on the exchange of information between states in order to limit and eliminate potential threats to ICTs and infrastructure dependent on ICTs.

3. **The purpose of regulation** of the commented norm resides in undertaking by states voluntary acceptance of international obligations on responsible provision of information about vulnerabilities in the ICT sphere and ways to combat with these vulnerabilities.

4. According to the Group, relevance of the issue of responsible provision of information is stipulated, in particular, by the inequality of states opportunities in terms of the ICT security, which is aggravated by differences in national legislation, regulations and practices to ensure security of ICTs.

5. Possible measures for international cooperation in this area can include the voluntary dissemination of national views and information about:

various aspects of national and transnational threats to ICTs and threats in the ICT use;

factors of vulnerabilities and installed hidden destructive functions in the ICT products;

leading methods of safety promotion of ICTs;

infrastructure categories, which are considered to be critical;

national efforts to protect critical infrastructures including ICT-dependent information on national laws and policies to ensure data security and infrastructure.

6. International cooperation on voluntary exchange of views and information about vulnerabilities in the ICT sphere and how to combat these vulnerabilities, international security threat assessment within the ICT sphere could be carried out with the assistance of specialized international organizations (e.g. the International Telecommunication Union), the interstate system monitoring threats to international information security.

13. Subparagraph k) "states should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of

another State. A State should not use authorized emergency response teams to engage in malicious international activity"

Comments to subparagraph k) of paragraph 13

1. **The object of regulation** in the commented norm are the international relations in the field of formation of the system of international information security, important elements of which should be authorized community emergency response teams (CERT)[164].

2. The commented norm proposes introduction of new objects of international relations in the international legal field – authorized CERTs and their information systems.

3. There are no universal international treaties on the matter.

4. Russian CERT is an autonomous non-profit organization "Center for Computer Emergency Response" (established in 1998), which is listed as Computer Security Incident Response Team (CSIRT) and is a member of associations CSIRT / CERT formed in various states (for example, such as Trusted Introducer), and within the framework of these organizations performs the functions of the contact of the Russian Federation[165].

The main objective of the "Center for Computer Emergency Response" is to reduce the level of information security threats for users of the Russian segment of the Internet (hereinafter referred as the Center).

The Centre carries out the collection, storage and processing of statistical data related to the spread of malware and network attacks on the territory of the Russian Federation, providing assistance to Russian and foreign legal entities and individuals in the implementation of functions of identification, prevention and cessation of illegal activity.

For implementation of tasks the Center cooperates with leading Russian IT companies, actors of operatively-search activity, public authorities, foreign computer incidents response centers and other organizations operating in the field of computer and information security.

Authorized CERT can be both state and non-governmental organization that operates on a commercial basis.

The competence of the authorized CERT is established by national legislation.

5. **The subject of regulation** is the international relations on authorized information systems of CERT security.

---

[164] Community Emergency Response Team – CERT.

[165] http://www.crime-research.ru/articles/sabodssh17.

In accordance with the Russian legislation, the information system is a collection of information contained in databases and information technologies and technical facilities providing its processing.

6. According to the Group, despite the fact that states have a primary responsibility to maintain a secure and peaceful ICT environment, identification of mechanisms of participation of the private sector, academia and civil society organizations would contribute to improving the effectiveness of international cooperation in ensuring security of the ICT sphere.

7. **The purpose of regulation** of the commented norm resides in undertaking voluntary commitments by a state on international obligations related to implementation of the ban and maintaining activities in the ICT sphere, which could cause damage to information systems of authorized CERT.

8. Identification and analysis of security incidents of information systems of CERT can be carried out within the framework of national jurisdiction, as well as within the competence of regional international security organizations. At the same time, the lack of coordinated universal international procedural norms regulating relations in the field of investigation of security breach of information systems of CERT will create difficulty in discussing results of the analysis with other states as well as non-party states to engaged regional security systems.

DRAFT – shared with the participants of the ICT4Peace Workshop on

Existing and future norms on international ICT infrastructure and data integrity

NATIONAL VIEWS ON THE APPLICATION OF INTERNATIONAL LAW TO CYBER SECURITY

By Dr. Elaine Korzak, LL.M.

INTRODUCTION

Every year the UN General Assembly asks member states to submit their views on a range of issues concerning cyber security under the official rubric of "developments in the field of information and telecommunications in the context of international security."[166] Since 1998 a growing number of states has informed the Secretary-General of their views and assessments with regard to a range of cyber security questions.[167] Taking together submissions of states, which are compiled into an annual report by the Secretary-General, offer an interesting and unique picture of evolving state practice in this field. They provide a snapshot of views of states over a period of almost two decades, while capturing the

[166] See for example UN General Assembly Resolution A/RES/70/237.

[167] UN General Assembly, Report of the Secretary-General A/54/213; UN General Assembly, Report of the Secretary-General A/55/140; UN General Assembly, Report of the Secretary-General A/56/164; UN General Assembly, Report of the Secretary-General A/56/164/Add.1; UN General Assembly, Report of the Secretary-General A/57/166; UN General Assembly, Report of the Secretary-General A/58/373; UN General Assembly, Report of the Secretary-General A/59/116; UN General Assembly, Report of the Secretary-General A/59/116/Add.1; UN General Assembly, Report of the Secretary-General A/60/95; UN General Assembly, Report of the Secretary-General A/60/202; UN General Assembly, Report of the Secretary-General A/61/161; UN General Assembly, Report of the Secretary-General A/62/98; UN General Assembly, Report of the Secretary-General A/64/129; UN General Assembly, Report of the Secretary-General A/65/154; UN General Assembly, Report by the Secretary-General A/65/201; UN General Assembly, Report of the Secretary-General A/66/152; UN General Assembly, Report of the Secretary-General A/66/152/Add.1; UN General Assembly, Report of the Secretary-General A/67/167; UN General Assembly, Report by the Secretary-General A/68/98; UN General Assembly, Report of the Secretary-General A/68/156; UN General Assembly, Report of the Secretary-General A/68/156/Add.1; UN General Assembly, Report of the Secretary-General A/69/112; UN General Assembly, Report of the Secretary-General A/69/112/Add.1; UN General Assembly, Report of the Secretary-General A/70/172;

opinions of states whose voices may not be heard as loudly as in other international processes.

Yet, the UN's annual reports in this field attract little attention and are not largely scrutinized. This is particularly the case in the context of the international norms debate. While the views of a few prominent nations are relatively well-known, the positions of the majority of states remain elusive. An analysis of states' submissions offers an obvious starting point to provide a more holistic picture of national views and their diversity in this debate. This paper seeks to do just that. It represents a study of the annual UN reports with regard to national views on the application of international law to cyber security. The analysis, whose aim it is to map a diverse set of emerging national views in this debate, is guided by the following questions: (1) What kind of guidance do states provide on the application of international law?, (2) How do national contributions inform the development of international law?, and (3) What similarities and differences flow from national positions?

In answering these questions, analysis is focused on areas of international law that regulate or guide the conduct of states. Thus, actions of non-state actors, unless attributable to a state, fall outside the preview of this paper. Accordingly, the criminal or terrorist use of information and communication technologies (ICTs) does not form the part of the analysis and emerging national views, with regard to the law governing these activities, are not examined.

National views with regard to international law applicable to state behavior are presented in two parts. The first part briefly recaps the question of applicability of international law to state actions in cyberspace. The second part then examines emerging states' views with regard to the application of substantive provisions of international law. A subpart presents and analyses areas of international law that appear to garner widespread acceptance from states. The second subpart subsequently examines areas where differing elements are advanced by a set of countries revealing emerging differences in national views with regard to the application of international law to cyber security. Three areas in particular are examined, human rights law, state sovereignty as well as international assistance or capacity-building. Finally, findings are summarized and presented in the conclusion providing insight into the areas of similarities and differences that will enlighten the potential for the future development of international law in this field.

METHODOLOGY

The following analysis seeks to distill national views with regard to international law from a textual analysis of national submissions. This is essential since contributions of states are not centered on international law but are embedded in the broader debate within the First

Committee.[168] The General Assembly's annual resolution asks for assessments on four issues in particular, none of them with an explicit focus on international law. The four issues are as follows:

(1) A general appreciation of the issues of information security,

(2) Efforts taken at the national level to strengthen information security and promote international cooperation,

(3) The content of relevant international concepts aimed at strengthening the security of global information and telecommunications systems, and

(4) Possible measures that could be taken by the international community to strengthen information security at the global level.[169]

A spectrum of questions related to cyber or information security is thus covered with no specific focus on international law.

In addition to annual submissions by states, the reports of Groups of Governmental Experts (GGEs) also inform the following analysis. GGEs are expert groups that are formed by the Secretary-General at the request of the General Assembly in order to inform the debate on a specific set of questions. Thus far, the First Committee created four GGEs, in 2004-2005, 2009-2010, 2012-2013, and in 2014-2015. A fifth Group of Experts is due to begin its work in August 2016.[170] While the mandate of past GGEs has been broad, studying "existing and potential threats in the sphere of information security and possible cooperative measures to address them,"[171] a number of GGEs have also been tasked to specifically look at legal questions, namely "how international law applies to the use of information and communications technologies by States, as well as norms, rules and principles of responsible behavior of States."[172] Both national submissions and reports of Groups of Governmental Experts form the basis of the following analysis.

While UN documentation offers new and important insights, a number of limitations flowing from this methodology need to be noted. First, the UN's annual report is compiled from voluntary submissions. Thus, the national views that can be detected come from a group that is self-selected. States that have not submitted their assessments to the Secretary-General are not included and their views on the application of international law to cyber security are not captured in this analysis. Second, even within the group of states that has

---

[168] Elaine Korzak, *Computer Network Attacks and International Law* (PhD diss., King's College London, 2015), p. 164.

[169] See for example UN General Assembly Resolution A/RES/70/237.

[170] Ibid.

[171] Ibid.

[172] UN General Assembly Resolution A/RES/70/237.

chosen to submit one or several reports over the years, the number of states with explicit or implicit opinions on international legal questions is relatively small. It is noticeable, however, that the overall number of state submissions has accelerated from 2010 onwards. National assessments have become both more numerous as well as detailed. Thus, an increasing number of countries are beginning to grapple with questions surrounding the application of international law to cyberspace. Yet, overall the number of states with opinions on international legal questions remains small even though more and more countries appear to be in the process of formulating their positions in this regard. Third, even the opinions of countries that carry discernible international law elements may not reveal the gamut of their legal thinking. States often chose to emphasize certain laws, frameworks or doctrines they hold to be applicable rather than pointing to legal areas they find problematic or inapplicable. It is thus more difficult to ascertain what legal views states (potentially) disagree with. The analysis of national views on the application of international law thus serves as an initial map of reference points that needs to be supplemented in the future. Lastly, the overall level of specificity or granularity with regard to views of states on international law and its applicability remains low. That is, pronouncements of states in this field remain general in nature rendering differences between very subtle views.

Nonetheless, an examination into the national submissions to the UN promises to be a worthwhile endeavor adding much-needed nuance and complexity to the international law in cyberspace debate.

NATIONAL VIEWS ON APPLICABILITY OF INTERNATIONAL LAW

With legal questions being embedded in the broader cyber security debate of the First Committee, the focus of international legal questions has shifted over the years of discussion. Whereas, the early period was characterized by an initiative for a new international convention in this field, discussions have subsequently broadened into a debate on "norms, rules and principles of responsible state behavior." In 1999, for instance, the Russian Federation advocated that "work should begin on the development of international principles" and that "these principles could take the form of a multilateral declaration; they would subsequently be incorporated into a *multilateral international legal instrument*."[173] Cuba similarly voiced that "*legally binding multilateral agreements* that prohibit aggression against information and telecommunications systems could be concluded within the framework of the United Nations."[174] Over the years, this treaty language has subsided,

[173] UN General Assembly, Report of the Secretary-General A/54/213, p. 9. Emphasis added.

[174] Ibid., p. 6. Emphasis added.

although it has not completely disappeared. As late as 2009, Kazakhstan proposed that "Member States of the United Nations should prepare and adopt an international convention on information security."[175]

More importantly, with the shift away from an international convention, the question of the applicability of international law appears to have been settled. In its 2013 report, the Group of Governmental Experts concluded that "[i]nternational 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."[176] The report further asserted that "the application of norms derived from existing international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability."[177] Herewith, the Group of Experts has in principle acknowledged the applicability of international law establishing a baseline in the international norms debate. However, the Group also acknowledged the difficulties of implementation by stating that "[c]ommon understandings on how such norms shall apply to State behavior and the use of ICTs by States requires further study" and that "[g]iven the unique attributes of ICTs, additional norms could be developed over time."[178] In many ways, this rationale represented a compromise to include countries that had been striving for a new international arrangement.

The consensus reached in the 2013 GGE report is mirrored in many national views although interesting nuances emerge. There are individual states from different regions that put forward more or less explicit acknowledgements of applicability. Mali, for instance, stated that "[i]nternational information security should be based on existing international law (*jus ad bellum*), which defines how to counter threats to international peace and security, and international humanitarian law (*jus in bello*), which relates to the means and methods of warfare."[179] Canada asserted that "[e]xisting treaty and customary international law is applicable to the use of information and communications technologies by States."[180] Similarly, Australia stated that "[e]xisting international law provides a framework for protection from information security threats arising from a variety of actors."[181] Lastly, the Islamic Republic of Iran is of the view that "[a]s a general principle, international law is

---

[175] UN General Assembly, Report of the Secretary-General A/64/129, p. 6.

[176] UN General Assembly, Report by the Secretary-General A/68/98, para. 19.

[177] Ibid., para. 16.

[178] Ibid.

[179] UN General Assembly, Report of the Secretary-General A/64/129/Add. 1, p. 7.

[180] UN General Assembly, Report of the Secretary-General A/68/156/Add. 1, p. 4.

[181] UN General Assembly, Report of the Secretary-General A/66/152, p. 6.

applicable and therefore should be applied to the use of information and telecommunications technologies and means by States."[182]

Other states acknowledged the applicability of international law, yet see the need for further discussion. Qatar argues that "[t]he United Nations should continue to lead the discussion and provide more clarification … whether existing principles of international law are sufficient to provide an appropriate framework to determine appropriate behavior online regarding aggressive acts."[183] In a somewhat similar manner Cuba argues for the need of new laws, while acknowledging the applicability of international law by stating that "[c]learly, there is a need to strengthen international law in the field of information and telecommunications."[184] But, "[i]t would not spring from a void; there are already existing related international principles, regulations and procedures which must be taken into account."[185]

An interesting dynamic springing out of these developments is the apparent split or distinction being made between international law on the one hand and norms on the other. Countries that otherwise acknowledge the application of international law also embrace and lobby for the development of non-binding norms. Germany poignantly expresses this: "Existing international law – both below and above the threshold of the law on armed conflicts -, supplemented by non-binding norms that define and shape expectations, should be the minimum baseline that guides responsible state behavior in cyberspace."[186] Similarly, Australia which has explicitly referred to existing international law and its principles to be applied to cyberspace supports "the development of international principles of responsible behavior in cyberspace, including agreeing a broad set of principles for normative behavior in cyberspace that will facilitate better international cooperation."[187] Although the language of international law as well as norms is used by a variety of states, it remains somewhat unclear whether these terms are being used with conceptual clarity. Perhaps they are used interchangeably by some states while others define norms more broadly and loosely as non-binding, political expectations in contrast to legally binding obligations of international law.

All in all, the question of applicability of international law has been answered in the affirmative. Yet, the difficulties anticipated in the application of substantive provisions have been acknowledged by the findings of the Group of Governmental Experts and similar concerns can also be found in national submissions. The need for the development of

---

[182] UN General Assembly, Report of the Secretary-General A/68/156/Add. 1, p. 12.

[183] UN General Assembly, Report of the Secretary-General A/65/154, p. 10.

[184] UN General Assembly, Report of the Secretary-General A/57/166/Add. 1, p. 5.

[185] Ibid.

[186] UN General Assembly, Report of the Secretary-General A/70/172, Submission of Germany, p. 1.

[187] UN General Assembly, Report of the Secretary-General A/66/152, p. 6.

additional norms has been recognized by numerous states. Perhaps the most interesting development in this context is the apparent split or differentiation being made between international law obligations and political, non-binding norms. Although the conceptual difference between both needs to be explored, the development of non-binding norms, rather than international legal provisions seems to be a more tenable proposition to some states.

NATIONAL VIEWS ON SUBSTANTIVE PROVISIONS OF INTERNATIONAL LAW

Following the emerging international consensus over the applicability of international law to cyber security, controversy centers on how states see the application or implementation of international law, and in particular the application of certain substantive provisions. Several trends can be detected from the submissions of states that inform the development of international law. First, there are some basic and critical provisions that seem to find widespread acceptance across states. Second, differing elements with regard to the application of provisions are being advanced in several areas of international law, namely human rights, state sovereignty, and international assistance or capacity-building. On this basis, both similarities and differences among national positions become visible which are explored in the following subsections.

Convergence on the UN Charter

A main reference point that emerges from the national submission of states is the UN Charter and the principles contained therein. This includes, among other things, the sovereign equality of states, the principles of non-interference in internal affairs and the non-use of force as well as the obligation to settle disputes with peaceful means. Support for the UN Charter as an anchor point is widespread across different regions. European states that acknowledge the application of the UN Charter and its main principles include France, Germany, Spain as well as Switzerland. The Netherlands, for instance, states "if cyber capabilities are used by States, they should be used in accordance with international law, including the UN Charter."[188] Other OECD member states, such as Australia, Canada, and South Korea also place an emphasis on the application of the UN Charter. Outside of this group of states, the Russian Federation, the People's Republic of China, Cuba, Georgia, Mali as well as Iran have submitted statements with similar effects. Qatar, for instance, "is

[188] UN General Assembly, Report of the Secretary-General A/70/172, Submission of the Netherlands, p. 4.

convinced that information and communication technology should be used in accordance with the Charter of the United Nations and the basic principles of international relations."[189]

Beyond this affirmation of the UN Charter and its principles, subtle differences emerge in the way states present their support. A number of states place a particular emphasis on the principle of non-interference and related elements, such as sovereignty. These include countries that have been traditionally mindful of this principle. Cuba, for instance, "underlined the importance of guaranteeing that the use of such [information and communication] technologies should be fully consistent with the purposes and principles of the Charter of the United Nations, international law, in particular sovereignty, non-interference in internal affairs and internationally recognized standards of coexistence between States."[190] Similarly, The Islamic Republic of Iran enumerates certain provisions stating that "States must observe the purposes and principles of the United Nations and their obligations under its Charter, in particular Article 2, paragraph 3, to settle international disputes by peaceful means, the prohibition in Article 2, paragraph 4, on the threat of use of force in any manner inconsistent with the purposes of the United Nations, as well as the prohibition set out in Article 2, paragraph 7, on intervention and interference in the internal affairs of States."[191]

Other states chose an alternative framing by categorizing areas of international law along the threshold of armed conflict or use of force. Several states provide explicit recognitions of two areas: international law on the use of force and international humanitarian law. This position is most poignantly expressed by the United Kingdom and the United States. Accordingly, the UK's view "is that the existing principles of international law, both on the use of force and the law of armed conflict, provide an appropriate framework."[192] The United States argues that "[d]espite the unique attributes of information and communications technologies, existing principles of international law serve as the appropriate framework … There are two distinct but related bodies of law to consider in this regard: *jus ad bellum* and *jus in bello*."[193]

In summary, national submissions show a clear trend, namely the convergence on the United Nations Charter as a main reference point in the application of international law to cyber security. Thus, several principles enshrined in the Charter are highlighted by different states. Whereas one group emphasizes the principle of non-interference in internal affairs, alongside fundamental provisions, such as sovereignty and peaceful dispute settlement,

---

[189] UN General Assembly, Report of the Secretary-General A/65/154, p. 9.

[190] UN General Assembly, Report of the Secretary-General A/69/112, p. 9.

[191] UN General Assembly, Report of the Secretary-Genearl A/68/156/Add. 1, p. 12.

[192] UN General Assembly, Report of the Secretary-General A/65/154, p. 15.

[193] UN General Assembly, Report of the Secretary-General A/66/152, p. 18.

others categorize applicable areas of international law along the threshold of armed conflict or use of force. The overlap of these two approaches is visible in the references to the principle of the non-use of force, or more broadly the area of international law on the use of force or *jus ad bellum*. In contrast, international humanitarian law or *jus in bello* and its application is highlighted only by predominantly Western states. However, overall, states' references to the UN Charter and its provisions remain fairly general in nature. No further guidance or elaboration is given as to how these provisions are seen to apply in certain circumstances. Perhaps a partial exception in this regard are the US views on the application of international law on the use of force and international humanitarian law.

With regard to the *jus ad bellum*, the US submissions highlight three provisions of the UN Charter, namely the prohibition on the use of force (Article 2(4)), individual and collective self-defense (Article 51) as well as collective measures authorized by the UN Security Council (Articles 39, 41 and 42).[194] In discussing the right to self-defense the US concludes that "under some circumstances, a disruptive activity in cyberspace could constitute an armed attack."[195] Similarly, the US asserts that the following principles of international humanitarian law would play an "important role in judging the legality of cyberattacks during an armed conflict", namely the principles of distinction and proportionality as well as the prohibition on indiscriminate attacks.[196] More importantly, "targeting analysis would have to be conducted for information technology attacks just as it traditionally has been conducted for attacks using kinetic (conventional and strategic) weapons."[197]

Even though these statements add detail to the acknowledgement that international law on the use of force and international humanitarian law apply to actions in cyberspace, their level of specificity in the context of cyber security remains low. The fundamental principles are enumerated, but no further guidance is given as to what concrete considerations would play a role in their application to cyber security other than those that presumably flow into assessments in the context of kinetic weapons. The US does recognize that "interpreting these bodies of law in the context of activities in cyberspace can present new and unique challenges."[198] However, it simply states that these challenges are "not unusual."[199] Any ambiguities or room for disagreement that arise in the context of cyber security "simply reflect the challenges in applying the Charter framework that already exists in many

[194] UN General Assembly, Report of the Secretary-General A/66/152, p. 18.

[195] Ibid.

[196] Ibid., p. 19.

[197] Ibid.

[198] Ibid.

[199] Ibid.

contexts."[200] In the end, "[w]hen new technologies are developed, they often present challenges for the application of existing bodies of law."[201] Thus, even though the US provides a more elaborate analysis than other countries, its considerations in applying international law on the use of force and international humanitarian law remain to be fleshed out beyond an acknowledgement of the ambiguities that emerge in this process in the context of cyber security.

Divergence in Areas of International Law: Human Rights, Sovereignty, Assistance

While there appears to be clear convergence on the United Nations Charter as an anchor point for the application of international law to cyber security, other areas of international law promise to be more contested in the emerging views of states. The following section examines three areas in particular where national submissions indicate that states advance different elements in the application of international law: human rights, sovereignty, and international assistance.

Human Rights

The application of international human rights law is mentioned by a vast majority of states in their national submissions. However, the language used in this context is characterized by different key words. The broadest language covers "individuals' rights and freedoms"[202] while some countries chose to focus on the concept of "ensuring a free flow of information."[203] Yet other states frame the area of international human rights law primarily in the language of "individual civil liberties, including the right to privacy."[204] Within the human rights framework, frequent reference is made to a particular right, namely the right to freedom of expression. As the US elaborates: "[t[he rights to freedom of expression and the free flow of information are embodied in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which generally provide, subject to certain limitations, that everyone has the right to freedom of expression, including the freedom to hold opinions without interference and to seek, receive and impart information through any media and regardless of frontiers."[205]

---

[200] Ibid., p. 18.

[201] UN General Assembly, Report of the Secretary-General A/66/152, p. 19.

[202] UN General Assembly, Report of the Secretary-General A/68/156, p. 5.

[203] UN General Assembly, Report of the Secretary-General A/64/129, p. 10.

[204] UN General Assembly, Report of the Secretary-General A/66/152, p. 3.

[205] Ibid., p. 19-20.

Beyond these references to the general application of international human rights law, and the right to freedom of expression in particular, different elements are advanced by states in their discussions. Most notably, Western states place an emphasis on the connection between the application of human rights law and an open and free Internet or cyberspace. Canada, for instance, states that it has "a strategic interest in preserving an open cyberspace."[206] The Netherlands similarly asserts its support for the "protection of an open, free Internet respecting human rights."[207] Concomitantly with this emphasis on a free and open Internet, many Western states express their concern that cyber security efforts may be used as a pretext to restrict the free flow of information. The United Kingdom expresses this clearly stating that it "does not recognize the validity of the term 'information security' … since it could be employed in attempts to legitimize controls on freedom of expression beyond those agreed in the Universal Declaration on Human Rights and the International Covenant on Civil and Political Rights."[208]

In contrast to this understanding, countries outside of the West emphasize that international human rights and freedoms apply in their national context. International human rights and freedoms are applicable but are to be implemented within the context of every individual state. The Islamic Republic of Iran holds that "[t]he right to freedom of expression should be fully respected."[209] Yet, "[a]t the same time, this right, in no case, should be exercised contrary to the purposes and principles of the United Nations, national laws and the principles of protection of national security, public order, public health or morals and decency."[210] In a very similar vein, Qatar asserts that the application of universal human rights needs to be balanced with the need to respect national differences. Accordingly, the "free flow of information must be guaranteed without prejudice to national sovereignty and while maintaining security and respect for cultural, political and moral differences among nations."[211] Preserving cultural and political differences is equally paramount for the People's Republic of China which argues that 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."[212]

The emphasis on cultural, political and historical differences in the application of international human rights may not be novel. The application of universal human rights

---

[206] UN General Assembly, Report of the Secretary-General A/68/156/Add. 1, p. 3.

[207] Ibid., p. 15.

[208] UN General Assembly, Report of the Secretary-General A/69/112, Submission of the United Kingdom, p. 1

[209] UN General Assembly, Report of the Secretary-General A/68/156/Add. 1, p. 13.

[210] Ibid.

[211] UN General Assembly, Report of the Secretary-General A/65/154, p. 9.

[212] UN General Assembly, Report of the Secretary-General A/61/161, p. 4.

across countries with markedly diverging political, economic, social and cultural systems has been a source of contention for decades. Yet, the changes brought about by the information revolution appear to have given renewed momentum to this debate. This is partly visible in the national views put forth by a select number of states that go even further in their concern over the free flow of information across borders.

The Islamic Republic of Iran argues that, among other things, states should refrain from the use of information and communication technologies for the "transboundary dissemination of information in contravention of international law, including the Constitution and regulations of the International Telecommunication Union, or national legislation of targeted countries."[213] Other countries, such as Syria, even call for an internationally enforced ban on disinformation. Accordingly, "[i]nternational standards and rules on the dissemination of information regarding the history, civilization and culture of peoples in databases and information networks (Internet) must be established, banning disinformation through the dissemination of erroneous information and calling for the adoption of appropriate measures, including the means to take action against parties who commit violations."[214]

In conclusion, the field of international human rights law is acknowledged across a broad swath of states in their national submissions. Beyond the basic reference to this body of law or the right to freedom of expression as a proxy, important differences emerge in views of states. Western states emphasize the connection between the application of human rights and the creation of an open and free Internet or cyberspace. In contrast to this Internet Freedom agenda, a sizeable number of states stresses the notion that human rights, although applicable, are to be implemented within the sovereign rights of a state thereby respecting the national, historical, political, and cultural circumstances. A rather small minority of states takes this limitation to constrain the transboundary information flows.

Sovereignty

The second area of international law with discernible differences in national submissions is the principle of sovereign equality or sovereignty. Similar to human rights law, it is widely recognized or acknowledged to apply in cyberspace by a vast majority of states. Greece, for instance, asserts that a "nation's sovereignty should be understood as the basic reference for every attempt of globalization."[215] In its 2013 report, the Group of Governmental Experts mirrored this sentiment by starting that "[s]tate sovereignty and international norms and

---

[213] UN General Assembly, Report of the Secretary-General A/68/156/Add. 1, p. 13.

[214] UN General Assembly, Report of the Secretary-General A/57/166/Add. 1, p. 6.

[215] UN General Assembly, Report of the Secretary-General AA/65/154, p. 6.

principles that flow from sovereignty apply to state conduct of ICT-related activities, and to the jurisdiction over ICT infrastructure within the territory."[216]

More importantly, the application of sovereignty in cyberspace is described as entailing both rights and responsibilities for states. Generally speaking, ensuring cyber security or the security of information and communication systems at the national level is seen as the primary responsibility of individual states. According to Sweden, "[i]t is first and foremost both the right and the responsibility of every country to protect its own information and information-based systems."[217] Brazil echoes this language and emphasizes that "all countries have equal rights regarding the protection of their homeland against cyberattacks."[218] The most significant consequence flowing from the recognition of sovereignty as a set of rights and responsibilities is the application of the law of state responsibility to cyber security. That is, states are equally responsible for internationally wrongful acts involving cyberspace, if the wrongful activity can be attributed to them. Thus, a number of states emphasize the law of state responsibility in their submissions.

Within this group several additional elements emerge. Some states are concerned with the use of proxies and underline the responsibilities of states with regard to the actions of non-state actors. South Korea argues that "[s]tates must meet their international obligations regarding internationally wrongful acts attributable to them."[219] To that end, "[s]tates must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-state actors for unlawful use of ICTs."[220] Likewise, the United States acknowledges the problem that "[a]cting through proxies significantly increases States' ability to engage in attacks with plausible deniability."[221] And "[w]hile existing international law has provisions governing the use of mercenaries, the use of proxies in cyberspace raises new and significant issues with wide-ranging implications."[222]

Another subset of states highlights the responsibility to combat terrorism asserting that existing legal obligations "apply fully when terrorists or terrorist facilitators use cyberspace to recruit, raise funds, move money, acquire weapons or plan attacks." Thus, "[a]ll States are obliged to share information about, and to take action against, online terrorist financing,

---

[216] UN General Assembly, Report by the Secretary-General A/68/98, para. 20.

[217] UN General Assembly, Report of the Secretary-General A/56/164, p. 5.

[218] UN General Assembly, Report of the Secretary-General A/64/129, p. 4.

[219] UN General Assembly, Report of the Secretary-General A/70/172, Submission by South Korea, p. 4.

[220] Ibid.

[221] UN General Assembly, Report of the Secretary-General A/66/152, p. 19.

[222] Ibid.

recruitment, planning and facilitation activities, while respecting the sovereignty of other States and their own responsibilities to allow the free flow of information."[223]

As these two concerns indicate, one of the main challenges in the application of international law of state responsibility to cyberspace lies in the level of due diligence required by the state for actions of non-state entities. This aspect remains unaddressed by national submissions although this does not diminish its significance. As the Netherlands eloquently summarizes this point, "[o]f particular importance is the examination of … the question of how the principle of State sovereignty applies to State activities in cyberspace, consistent with States' international obligations and the law of State responsibility. It also includes the question of the application of the principle of due diligence, i.e. not to knowingly allow a State's territory to be used for acts contrary to the rights of other States."[224]

With the application of state sovereignty seen as rather uncontroversial, the main contrast emerging among states' submissions concerns the contours of its reach. In other words, what is the regulatory reach of national jurisdictions in cyberspace and where are the limits to the exercise of sovereign rights? The emphasis of sovereign rights in the application of international human rights law is an already-discussed example of this controversy. In addition, some states stress the importance of sovereignty in limiting undue interference. The government of Venezuela for example considers "that any violation of information security is contrary to the legitimate right of States to full exercise of their sovereignty. Hence the use of information technologies and media for the purpose of political and economic destabilization is contrary to the fundamental rules of democracy."[225]

Assistance

The third area with diverging views in terms of applicable international law is a somewhat less prominent one. The question of international assistance or capacity-building in cyber security and any legal obligations involved in it has not been examined in any depth.

At first glance, relations in this field are structured along more or less advanced countries with regard to cyber security efforts. Several countries stress the need to ensure access of developing countries to assistance in the development of cyber security capacities and capabilities. Two states in particular point to their efforts in this area, namely the United Kingdom and the Netherlands. The UK asserts that it takes "a strong lead in developing and sharing best practice, experience and information with regard to cybersecurity" and that it

---

[223] Ibid., p. 20.

[224] UN General Assembly, Report of the Secretary-General A/70/172, Submission of The Netherlands, p. 4.

[225] UN General Assembly, Report of the Secretary-General A/59/116/Add. 1, p. 6.

is "committed to ensuring that the global community has access to assistance in developing their cybersecurity capabilities."[226] To that end, the UK has established an International Cybersecurity Capacity Building Fund within the Foreign and Commonwealth Office.[227] Additionally, the University of Oxford houses the Global Cybersecurity Capacity Building Centre which developed a Capability Maturing Model supposed to identify national and regional capacity building needs.[228]

The Netherlands, on the other hand, launched the Global Forum on Cyber Expertise in collaboration with 41 partners to improve exchange at the international level. Since "[t]here is a great need to step up efforts for capacity building. At both the technical and policy level the international community needs to learn from each other and exchange best practices in various fields in cyberspace."[229]

These and other initiatives resemble known dynamics between developed and developing countries in the area of development assistance. However, it is important to note in this context, that the initiatives supported by developed countries cover predominantly the exchange of best practices (albeit at both the technical and policy levels). Moreover, they are not formulated in terms of legal obligations.

In contrast, a more pressing concern for a variety of developing countries appears to be the question of access to technology. Several states stress that access to technology should be provided without restrictions or discrimination. The Islamic Republic of Iran notes that "[n]othing shall affect the sovereign right of States in the field of information and telecommunications, including the development, acquisition, use, import and export of, and access to, information and telecommunications know-how, technologies … without restriction or discrimination."[230] Similarly, Brazil argues that "discriminatory mechanisms that could prevent countries from accessing high technology in the field of telecommunications and information systems" should be avoided.[231] The Philippines go one step further in the question of technology access. Concerns extend beyond restrictions in the access to technology to scenarios of "information colonization."[232] These are defined as "[a]cts committed by a State or States against another State in order to dominate and control the information arena and prevent access to the latest information technologies and create a situation in which other States become technologically dependent in the information

---

[226] UN General Assembly, Report of the Secretary-General A/70/172, Submission by the United Kingdom, p. 5.

[227] Ibid.

[228] Ibid., p. 5-6.

[229] UN General Assembly, Report of the Secretary-General A/70/172, Submission by The Netherlands, p. 5.

[230] UN General Assembly, Report of the Secretary-General A/68/156/Add. 1, p. 12.

[231] UN General Assembly, Report of the Secretary-General A/64/129, p. 3.

[232] UN General Assembly, Report of the Secretary-General A/56/164, p. 4.

sphere."[233] Thus, situations of dependency and restricted access to non-indigenous technologies are drivers of developing states' views in this area.

Lastly, a minority of states advances the view that the provision of assistance is founded in a legal obligation. Further, assistance could potentially include the transfer of technology, not just the provision of unrestricted access. Accordingly, Panama asserts that "[f]or technologically advanced countries, however, that need implies a commitment and an obligation to provide, transfer and build the capacities of less advanced countries. Likewise, those countries must undertake not to use their technological advantage for commercial or industrial espionage against the rest of the less technologically advanced countries."[234]

CONCLUSION

Even though national submissions of views and assessments of cyber or information security do not focus on international legal questions, nevertheless, they inform the development of international law in important ways. Based on the foregoing analysis, a number of observations can be made that are visualized in the graph below.

On the most basic level, national submissions reveal areas of convergence and areas of divergence. Areas of convergence comprise international law fields that are acknowledged by an overwhelming majority of states. The second section of the foregoing analysis showed that the UN Charter and its basic principles have emerged as the main reference point in this regard. In addition, areas of overlap are also visible in the application of certain substantive provisions of international law. These areas of overlap are visualized in blue in the graph below. They are human rights law and state sovereignty, with the addition of international law of state responsibility, as a result of the recognition of sovereignty.

Within these areas of convergence, the controversy does not center on their application or recognition. Rather, questions arise with regard to the proper limits of these areas, for example, the limits of state sovereignty. This is where diverging state views emerge. Most visibly, the question of where to draw the balance between applicable legal areas arises in the boundary between state sovereignty and human rights. The question of transboundary information flows is a particularly controversial aspect advanced by a subset of individual states (highlighted in light blue in the graph below).

However, within these areas of convergence it is important to note that questions pertaining to proper limits between legal areas are not unique to their application to cyber security. Rather, the implementation of state sovereignty and human rights has attracted

---

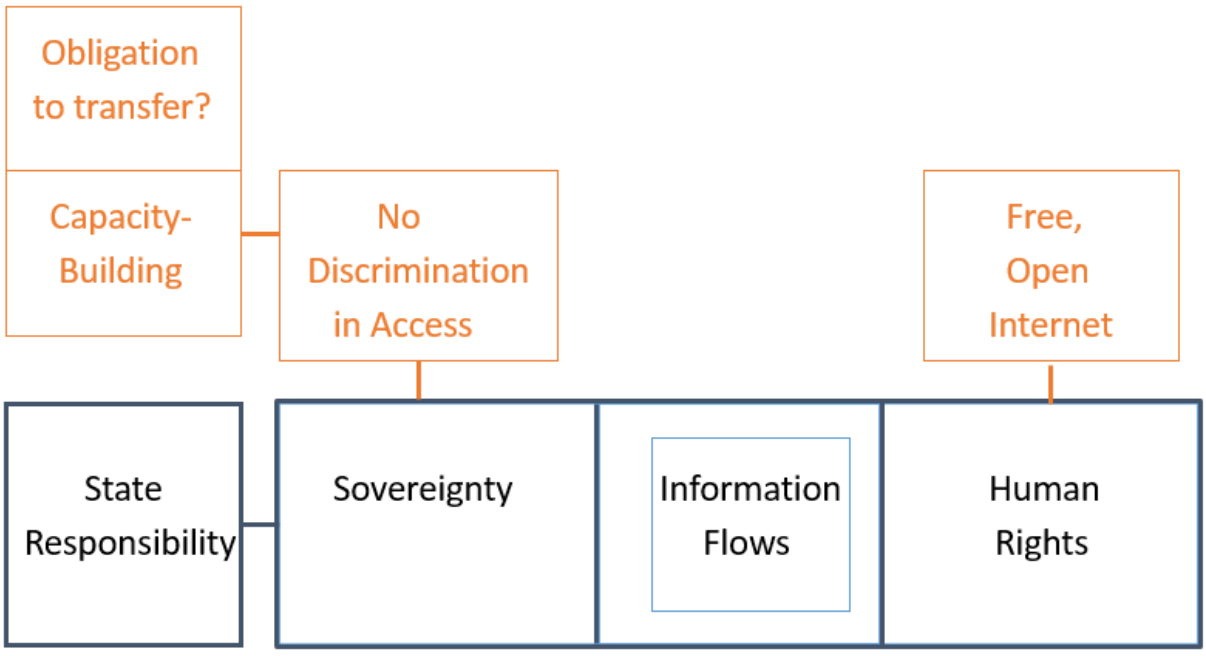
[233] Ibid.

[234] UN General Assembly, Report of the Secretary-General A/57/166/Add. 1, p. 5.

controversies before the emergence of cyberspace. In this sense, traditional legal disputes are simply transposed into cyberspace. Thus, the application of international legal provisions to cyber security does not prove to be dissimilar to other issues in international law. Ideological differences already apparent in international law are simply replicated in the context of cyber security.

Further areas of divergence, mostly those advocated by a subset of individual states, are marked in orange in the graph below. In the context of international human rights law this includes the emphasis on a free and open Internet or cyberspace advanced by Western states. Similarly, the analysis of views on international assistance or capacity-building shows an emphasis on unrestricted or non-discriminatory access to technology by certain states while a small number of countries assert a controversial transfer obligation. It is in these areas where the very real differences of states in terms of technological capabilities enter the international legal debate.

All in all, the elements advanced by states and visualized below provide an initial understanding of the breadth of national views on the application of international law to cyber security. They provide an outline to map the similarities and differences that flow from national positions and can inform the debate on the development of international law in this area. However, as mentioned in the beginning, this more complex understanding of states' views in this area is based on an examination of national submissions to the UN and should be supplemented by additional crucial research beyond these confines. A more inclusive and progressive debate on the application of international law to cyber security depends on it.



DRAFT – shared with the participants of the ICT4Peace Workshop on

Existing and future norms on international ICT infrastructure and data integrity

SUBVERSION: NORMATIVE CONSIDERATIONS

Liisi Adamson

After the Second World War, the international community has over several decades witnessed a significant change in the means for achieving the ends, which have traditionally been achieved by forcible measures. Instead, 'more subtle, veiled and indirect means calculated to achieve these ends have been used with greater frequency.[235] 'These acts […] take a variety of forms, assume different natures and can have serious consequences on the territorial integrity and political independence of the affected States. Their common characteristics are that they aim at definite political ends, usually in violation of the political independence of the State against which the acts have been directed, and that ostensibly the State which is responsible for the acts does not act directly but through third parties who are seemingly acting on their own initiative.'[236]

Subversion as a technique or method is old and well-established. However, besides the traditional notion of subversion, ICTs are increasingly used for subversive activities. The global and interconnected character of the cyberspace directly enable the modern features of subversion. Thus, the current work discusses how subversion materializes in cyber context and how the scope of subversive activity has expanded.

THE COLD WAR PERCEPTION

Merriam-Webster defines subversion as the act of subverting or the state of being subverted, but especially as a systematic attempt to overthrow or undermine a government or political system by persons working secretly from within.[237] Regardless of the proposed definitions, subversion has no universally accepted definition.[238] During the Cold War, the British Security Service (MI5) defined subversion as a generalized intention to 'overthrow or undermine

---

[235] Fu-shun Lin, 'Subversive intervention', University of Pitssburgh Law Review Vol 25 (1963-1964), at 35

[236] Ibid

[237] 'Subversion', *Merriam-Webster Dictionary*, http://www.merriam-webster.com/dictionary/subversion

[238] RJ Spjut, 'Definining Subversion', British Journal of Law and Society Vol. 6 (1979) at 254

parliamentary democracy by political, industrial or violent means'.[239] In 1978 the Home Secretary Rees followed the definition proposed by MI5 to great length, but added that '[s]ubversive activities are generally regarded as those which threaten the safety or well-being of the State'.[240] Similarly, among American officials, the term subversion was also imprecise, yet most often used when describing clandestine efforts to undermine the US and its allies (usually by communists).[241] Soviet Union, likewise, saw subversion as something only one's adversary employed.[242]

In 1971 Frank Kitson, the British counterinsurgency practitioner and theorist defined subversion as 'all illegal measures short of the use of armed force taken by one section of the people of a country to overthrow those governing the country at the time, or to force them to do things they do not want to do'.[243] Even though Kitson and Thompson claim that 'subversion is sometimes employed in the expectation that its nonviolent actions on their own suffice to lead to a government's downfall',[244] Rosenau contends that such 'examples of regime change by subversion alone are difficult if not impossible to find'.[245]

Though beneficial, none of the definitions offer a comprehensive account on the nature of subversion. Subversion is a broader concept than insurgency and revolution. It goes beyond violence but also has more limited goals than insurgency. When subversive activity aims at eroding and undermining authority, then insurgency and revolution are only the most extreme forms of subversive activity with the clear aim of overthrowing a government. Subversion can be limited to forcing those in power to do things they do not want to do, rather than to force them out and gain power, whereas insurgency aims always at overthrowing or challenging an existing order. Similarly, when subversion can be non-violent in nature, then in its most extreme form, insurgency uses violence to seize, nullify or challenge political control of a region.[246]

---

[239] William Rosenau, 'Subversion and Insurgency: RAND Counterinsurgency Study – Paper 2', *RAND Corporation* (2007), at 4, available at https://www.rand.org/content/dam/rand/pubs/occasional_papers/2007/RAND_OP172.pdf

[240] Spjut, Defining Subversion, at 254

[241] Rosenau, Subversion and Insurgency, at 4

[242] Ibid

[243] Frank Kitson, *Low Intensity Operations: Subversion, Insurgency, Peace-Keeping* (London: Faber and Faber 1971), at 3

[244] Ibid, at 83. Robert Thompson, *Defeating Communist Insurgency: Experiences from Malaya and Vietnam* (London: Chatto& Windus 1967), at 28

[245] Rosenau, Subversion and Insurgency, at 5

[246] US DoD, Dictionary of Military and Associated Terms, at 117

SUBVERSION IN THE MODERN CONTEXT

When comparing the notions of subversion that can be seen today in the traditional sense of subversion, some very significant features emerge. Firstly, ICTs are extensively used to influence States. ICTs and networks are also used for subversive purposes. When subversion would traditionally entail penetrating and manipulating political parties or infiltrating State institutions, then ICTs enable subverts to achieve the desired ends remotely without the human factor at site. For example, ICTs can be used to influence the target through shutting down or limiting access to certain services, e.g. by DDoS attack, or by retrieving information to use later to achieve the desired ends. At the same time, it is important to note that ICTs and computer networks are merely the means to achieve the ends. The primary targets are still decision-makers and those in power.

Secondly, ICTs have made it significantly easier to achieve the desired ends, whether used by States, non-State actors or private individuals. In the context of subversion, new technologies have enabled a proliferation of subversive causes and ideas. As a result, subversion, instead of having a narrow purpose of undermining a political order of States as recognized during the Cold War, has become more cause-driven on the part of subversive movement, uniting people and groups all over the world. Subversion offers also a useful tool for activists, when highly specific issues mobilize a critical mass of people, who may join a movement for their own individual reasons. It has been proposed that the more technologically sophisticated the subversive movement and its targets are, the more cause driven the subversive activity is likely to become.[247]

Thus, the aim of the subversion has been broadened. It is no longer solely about overthrowing a government, but rather influencing those in power to achieve the desired ends, i.e. change a course of action or inaction. That is recognized also within American and British military institutions, where the terms have as of today acquired different connotations than presented previously. US Department of Defense sees subversion as 'actions designed to undermine the military, economic, psychological, or political strength or moral of a governing authority'.[248] The British Army refined the term by identifying subversion as activities that fall 'short of the use of force' and are intended to erode the strength of the

---

[247] Rid Cyber War Will Not Take Place

[248] US DoD, 'Department of Defense Dictionary of Military and Associated Terms', Joint Publication 1-02 (8 November 2010, as amended through 15 October 2015), at 232, http://fas.org/irp/doddir/dod/jp1_02.pdf

State.[249] Thus, both definitions do not exclude the violent manifestations of subversion, yet are broader than the traditional view.

Thirdly, the Cold War perception of subversion clearly focused on State activity in undermining another States. However, the modern notions of subversion can be characterized by originating mostly from non-State actors. Nowadays, if considering that the aim of subversive activity is mostly influencing those in power to achieve certain cause-specific ends or influence the existing government into action or inaction, then examples of patriot hacking and the activities conducted by Anonymous can be considered subversive in character.

Furthermore, the subversive movements can be characterized by high membership mobility and low level of organizational control. Members can be located all over the world, to work towards subverting the same target. The interconnectedness of ICTs have not only made it easier to join a subversive cause, but the inherent insecurity of ICTs have made it easier to attack the systems and apply pressure to the authority many times with the added benefit of anonymity. At the same time, when detected, it has become easier to stop subversive activity, when the State has the appropriate means.

A modern example of high membership mobility and low level of organizational control is the Anonymous movement. It has no central leadership, no hierarchy or membership databases. Instead, there is a strict adherence to a set of basic guidelines to connect a loose and largely leaderless movement of activists all over the world. The activities have remained entirely non-violent and activists have concealed their identities while rallying around several self-defined causes, often promoting free speech, agitating against totalitarian States, censorship and government oppression.[250]

Of course one can still address the more traditional notion of subversion in the sense of the insurgent or revolutionary enterprise. A good example here is the Arab Spring and the uprisings in Egypt, which used social media eloquently for coordinating the subversive activity. Thus, social network offered a platform for planning as well as after-action deliberation.[251] Even though the uprisings grew to be violent to some extent, the early phases of subversively undermining established authority and collective trust require less violence than before. That is not to say that subversion today might not evolve into insurgency or revolution. The argument is rather that the prevalent form of subversive activity noticed today is not violent and rather aims at influencing the actions or inaction of a State. It is

---

[249] British Army, 'Army Field Manual, Vol. 1, "Combined Arms Operations," Part 10, "Counterinsurgency Operations" (Strategic and Operational Guidelines)', Issue 1.0, July 2001, at A-3-2. Rosenau, Subversion and Insurgency, at 4-5

[250] Rid, Cyber War Will Not Take Place

[251] Rid, Cyber War Will Not Take Place

easier to organize and establish subversive activity due to interconnectedness. However, when conducted through ICTs, the threshold of success is relatively higher, when the State has the appropriate means to curb the subversive activity.

SUBVERSION THROUGH ICTS

The typology discussed in the following paragraphs is not conclusive nor does it aim to suggest that each type of subversion follows a specific pattern using predetermined tools and practices. Especially taking into consideration the numerous possibilities ICTs offer, the subversive activity is more multi-faceted and –layered than before. Each subversive campaign is different and takes into account the social, political, economic, cultural and historical differences characteristic to the target State.

Even though subversion is most often categorized as internal or external, the notion pertains only to the source of subversive activity. Subversive actions can be taken by those within a country, mostly non-State actors, such as activists, or by someone external to the country,[252] i.e. another State, non-State actors etc. The target of the subversive activity is generally the authority of the State, e.g. government, political elites.[253]

William Rosenau offers an example of an earlier typology. He claims that subversive actions can generally be grouped into three interrelated categories. Firstly, establishing groups that penetrate and manipulate existing political parties. Secondly, infiltrating the institutions of the State and important non-government organizations. Thirdly, generating civil unrest through demonstrations, strikes and boycotts.[254] An approach of Rosenau, as the more traditional one, relies on the human element in subversion and does not fully take into account the use of ICTs. However, the activities described by Rosenau can be coordinated with the use of social networks and media.

Focusing more on the use of ICTs, subversive activity can be characterized by three phases of operation: the insertion of malware, such as the backdoors, Trojan horses etc., exercising them and thereby influencing the target or the retrieval of the unauthorized information and using it to influence the target. Insertion phase can occur over the entire life cycle of a system from its design phase to the production and working phase. Thus, taking into consideration the means through which subversive activity is conducted, another definition of subversion, offered by Myers, understands the activity as the covert and methodical

---

[252] Beilenson, Laurence, *Power Through Subversion* (Washington DC: Public Addairs Press 1971), at V-VII

[253] Paul W. Blackstock, *The Strategy of Subversion: Manipulating the Politics of Other Nations* (1st edition, Chicago: Quadrangle Books 1964), at 56

[254] Rosenau, Subversion and Insurgency, at 6

undermining of internal and external computer system controls to allow unauthorized and undetected access to the computer system resources and information.[255] The inherent insecurity of ICTs entails that the legitimate activities that are carried out during the various life cycle phases offer ample opportunities for subverter to undermine its components. Thus, subversive activity can occur at any time in the life cycle of the ICT system and is generally under the control of highly skilled individuals. Such activities utilize generally clandestine mechanisms deliberately constructed and inserted into a system to circumvent normal control or protection features.

Depending on the phase of the ICT lifecycle where the vulnerability is inserted, following types could be construed:

- Subversion by design
- Subversion by implementation
- Subversion by distribution
- Subversion by installation
- Subversion by production[256]

Thus, supply chain security plays a major role in curbing the subversive activities. As could be seen from the US decision to not allow Huawei and ZTE technology to its governmental systems, claiming that they pose a national security threat due to the influence of the companies of Chinese government,[257] curbing backdoors and other vulnerabilities inserted to the systems of States to enable subversive activity as well as, for example, espionage is considered a priority.

The above described focused more on the system subversion, where a clandestine functionality is added to the system that permits the adversary to bypass system security mechanisms. Subversive activity can be conducted also in the context of applications. As activist groups have rare access to the design, production or implementation phase of the ICTs or computer systems – so the same could not be said about States – but they often do have access to various forms of malicious software, e.g. Trojan horses, which enable to take control of the target system. Similarly, they can use botnets to conduct DoS or DDoS attacks to paralyze the government systems. With the widespread use of ICTs in the government

---

[255] Philip A. Myers, 'Subversion: The Neglected Aspect of Computer Security', Naval Postgraduate School (1980)

[256] Ibid

[257] US Congress House of Representatives, 'Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE' (8 October 2012) 1-7 <intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf> (visited 15 October 2015)

sector, it has become reasonably easy to subvert an information system by inserting software artifices that would enable a knowledgable attacker to obtain undetectable control of the system.[258] However, it is important to note that the techniques used in the application phase are not solely used for subversive activity, but can be used for other cybercrime purposes.

LEGAL REGULATION

As discussed, subversive activity is no longer used solely by States but instead non-State actors, e.g. activists, individuals, small groups to some extent have taken over the use of the method to influence those in power. Thus, legally speaking, one must distinguish between legitimate demonstration and dissent and subversive activity, which aims to change a certain course of action or decisions. Subversion to some degree in its mildest form is a natural part of society. Subversive activity and thought is not necessarily radical or militant, but mostly political, embracing progress or course of action different from those in power. Since democracies are political systems designed to accommodate a certain amount of subversive activity, balance must be found between legitimate dissent and subversive actions. It is a precondition of a free, open and critical polity, since the right to resistance is designed as a safeguard against abuse of power in liberal constitutional orders.[259] Then follows that for non-State actors legitimate expression and the articulation of dissent must be distinguished from subversion that constitutes a domestically punishable crime. When it comes to States, similarly legitimate dissent must be distinguished from illegal subversive intervention and violence.

Subversive activities of States

There have been opinions that subversion is not principally illegal and illegitimate and only the most extreme forms of subversion, i.e. those that use force, are illegal. Even though it is acknowledged that subversion may not remain entirely non-violent, the trend in using ICTs for subversive activity goes to show that the aim of the said activity is not to use violence, but rather find a more subtle way to achieve the desired ends. As of now, there is no explicit international prohibition of subversive activity, similarly to espionage.

However, subversion, if conducted by States, is considered a sub-category of intervention, breaching the non-intervention principle. Broadly, the non-intervention principle has a dual legal basis. On the one hand, it is grounded in relevant treaties and declarations and on the other hand, it is a principle of customary international law. Even though, the principle is not

---

[258] Emory A. Anderson, Cynthia E. Irvine, Roger R. Schell, 'Subversion as a Threat in Information Warfare', Naval Postgraduate School (2004)

[259] Rid, Cyber War Will Not Take Place

explicitly established in the UN Charter vis-à-vis State activities,[260] it is prominent in multilateral, regional and bilateral treaties. For example it is reflected in the Montevideo Convention,[261] in the Charter of the Organization of the Americas,[262] in the Treaty of Amity and Cooperation in Southeast Asia (ASEAN Treaty)[263] but also in the Constitutive Act of the African Union,[264] Charter of the Association of Southeast Asian Nations,[265] the Pact of the League of Arab States,[266] and the Charter of the Organization of the Islamic Conference.[267]

Additionally, the non-intervention principle is represented in numerous UN General Assembly resolutions.[268] The most significant of them, the Friendly Relations Declaration,[269] was adopted in 1970. The Declaration and respective ICJ case law in the *Nicaragua* case[270] have established the non-intervention principle as requiring coercion in the internal or external affairs of the State as preconditions of an unlawful intervention. Among other coercive activities, the Friendly Relations Declaration states also that 'no State shall organize, assist, foment, finance, incite or tolerate subversive […] activities directed towards the violent overthrow of the regime of another State, or interfere in civil strife in another State'.[271]

Commentators have identified subversive intervention as a form of intervention that clearly satisfies the requirement that prohibited intervention concerns a matter of internal

---

[260] UN Charter Article 2(7) establishes the non-intervention principle with regard to UN as an organization, yet it is not applicable to Member States.

[261] Montevideo Convention, Articles 3, 4 and 8

[262] OAS Charter, Articles 1 and 3e

[263] ASEAN Treaty, Articles 2a, b and c

[264] African Union, Constitutive Act of the African Union (11 July 2000), Articles 4a and 4g

[265] ASEAN, Charter of the Association of Southeast Asian Nations, 20 November 2007, in force 15 December 2008, Article 2(2)

[266] League of Arab States, Pact of the League of Arab States (22 March 1945) Article 8

[267] Organization of Islamic Cooperation, Charter of the Organization of the Islamic Conference (14 March 2008)

[268] Declaration on the Inadmissibility of Intervention (n 158) para 2; Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs (n 160) para 2, Principle I(b) and II(a). UNGA A/RES/42/22 '42/22. Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations' (18 November 1987), annex para 8

[269] UNGA A/RES/25/2625 '2625 (XXV). Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations' (24 October 1970), Principle 1

[270] ICJ, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States), Judgment, 27 June 1986, ICJ Reports (1986)

[271] Friendly Relations Declaration, Principle 3

affairs.[272] The aim of subversion is not just mere influence, but the goal is to bring about a change mostly in the political arena. When the subversive activity manages to bring about a change in the course of action that would have otherwise not be taken, the act is to be considered coercive. However, it is important to note that now more than ever, States use third parties to conduct the subversive activity through cyber means. State participation in subversion is unlawful only when the government furnishes subverts with the money, arms, supplies, logistics help or in any other significant way. Only when it constitutes significant support for coercion, equal to the level of logistical and financial support, as observed by ICJ in *Nicaragua*, the State can be considered indirectly part of the subversive activity. Additionally, in the context of using cyber means, the anonymity and attribution problems challenge the target State, since legal consequences can only follow, if the perpetrator has been identified.

As to the supply chain security and embedded hidden functions, which are directly related to system subversion, both have been recognised by the UN GGE as a threat pertaining to ICT systems.[273] Initiative in this field has been taken also by the US who has adopted series of laws and regulations that focus increased scrutiny on the security of supply chains for information technology procured for government use.[274] In the US, the threat posed to US national security interests by vulnerabilities in the telecommunications supply chain is an increasing priority given the country's reliance on interdependent critical infrastructure systems.[275] The 2010 Canada's Cyber Security Strategy emphasised that many of the risks and impacts are shared between the government and private sector, one of them being untrustworthy technology, which could be harmful to both Government and the industry.[276]

---

[272] Gerhard von Glahn, *Law Among Nations* (7th edition, Boston: Longman 1996); Phihil Kunig, 'Prohibited Intervention', Max Planck Encylopedia of Public International Law, online edition, para 25; Quincy Wright, 'Subversive Intervention', American Journal of International Law Vol. 54 (1960), at 521.

[273] UN GGE 2013 Report.

[274] See further Latham & Watkins. Government Procurement: Increased Security Scrutiny in IT Supply Chains. Commentary Numer 1645, 11 February 2014. Available at: http://www.lw.com/thoughtLeadership/lw-it-government-contracts-security.

[275] US Congress House of Representatives. Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE.

[276] Canada's Cyber Security Strategy. For a Stronger and more Prosperous Canada, 2010, page 12.

Efforts to curb the built-in vulnerabilities have been also made by Australia,[277] Russia,[278] India,[279] China[280] and the EU.[281]

Difference from other forms of intervention

Intervention is the most general notion used to signify the action of meddling into the affairs of another State. Use of force is only the most obvious form of intervention.[282] The fall of a government or the creation of a new government due to an external war is not subversion.[283] Other forms of intervention may be distinguished and based on the aim and nature of the intervention. As such espionage may carry an interventionist aspect, as well as subversion and sabotage. However, espionage is not to be equated with subversion.

	Espionage	**Subversion**	**Sabotage**	**Use of force**
Aim	Obtaining information clandestinely	Cause-driven change or influencing activity in a certain way or in most gravest form, aiming at overthrowing a government	Destruction, damage or obstruct something	Multiple purposes, including change

[277] BBC. China's Huawei barred from Australia broadband deal. 26 March 2012. Available at: http://www.bbc.com/news/business-17509201.

[278] Scott Charney, Eric T. Werner. Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust. Microsoft, 26 July 2011, page 6. Available at: http://www.microsoft.com/en-us/download/details.aspx?id=26826.

[279] Ministry of Communications and Information Technology. Department of Telecommunications. Policy for Preference to domestically manufactured telecom products in procurement due to security considerations and in Government procurement. Notification. 5 October 2012. Available at: http://www.dot.gov.in/sites/default/files/5-10-12.PDF

[280] Dieter Ernst. Indigenous Innovation and Globalization. The Challenge for China's Standardization Strategy. UC Institute on Global Conflict and Cooperation, East-West Center. June 2011, pages 36-37.

[281] Joint Communication to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (7 February 2013), page 12.

[282] ICJ, Nicaragua, para 205

[283] Beilenson, Laurence, *Power Through Subversion* (Washington DC: Public Affairs Press 1971), at VI

Nature	Non-violent	Non-violent/violent	Non-violent/violent	Violent
Legal regulation	*Non-intervention principle/Breach of sovereignty*	*Non-intervention principle*	*Non-intervention principle/Article 2(4)*	*Article 2(4), Article 51*

Table 1. State on State activities and their legal regulation

Non-State actors

The activities of non-State actors are regulated by domestic laws. Similarly, as there is no international prohibition of subversion, there are few States, who explicitly prohibit subversive activities. More prominently, the US[284] and the Philippines[285] have an explicit law pertaining to subversion. In 2002 Hong Kong tried to establish an anti-subversion law, but it was later withdrawn due to large-scale public protests. Mostly, the domestic laws pertaining to sedition or treason apply to the acts conducted with the aim of subversion. When it comes to subversion conducted through ICTs, then domestic cybercrime regulations and in Europe in cooperation with the Budapest Convention on Cybercrime,[286] regulate entering protected computer networks and retrieving information therefrom.

FOOD FOR THOUGHT

- Should the definition of subversion in the modern context focus on the means or the aim of the subversive activity?
- What counter-subversive capabilities ought to be deployed in the modern context?
- How do the rights of free speech, free association and other related liberties accommodate subversive and counter-subversive activities?
- Is propaganda activity subversive?
- Should we talk about subversion as a concept or just activities with a subversive nature? Is there subversion in the modern context?
- Where and how to draw a line between legitimate dissent and subversive activity in the context of using ICTs for subversive activities?

---

[284] 18 US Code Chapter 115, Treason, Sedition and Subversive Activities.

[285] Presidential Decree no 1835 – Anti-Subversion Law of 1981; Republic Act No 1700 – Anti-Subversion Act

[286] CoE, Convention on Cybercrime, Budapest (23.11.2001)

- Should subversion be explicitly regulated under international/domestic law?

CONCLUSION

The aim of subversive activity has been broadened since the Cold War. Deployed often by activists and other non-State actors, the subversive activities have become more cause-driven, uniting people all over the world. Since violence has been replaced with more subtle forms of influence, the most severe forms of subversion, such as insurgency and revolution are nowadays rare. The subversive activity aims mostly to influence the existing government into action or inaction using 21st century means. Subversion techniques are no longer reliant on the human factor on site, i.e. about infiltrating government institutions, but rather take use of ICTs and the interconnectedness of the networks. Thus, the security of supply chain and technology itself has become a priority, since the ICTs' inherent insecurity allows the system to be subverted throughout its life cycle. As there is no explicit prohibition of subversion, the international law offers only general solution through the non-intervention principle. The increasing use of subversive techniques by activists and other non-State actors is regulated in a fragmented way through different domestic regulations.

DRAFT – shared with the participants of the ICT4Peace Workshop on

Existing and future norms on international ICT infrastructure and data integrity

GREAT EXPECTATIONS: MULTI-STAKEHOLDER APPROACH AND INTERNATIONAL CYBERSECURITY

Mika Kerttunen

INTRODUCTION

Concepts cannot travel far. Removing notions from their time, place and settings changes their original meaning and force. Conceptual overstretching equals vague, amorphous, admittedly value-free, but useless, concepts. The more outlined concepts are the less applicable, they tend to become outside their home turf.[287]

This article inquires the transferability of the multi-stakeholder model from the context of (Internet) governance to that of international cybersecurity. It asks whether the approach itself or its particular mechanisms are applicable in the field of international cybersecurity and which particular areas within this grand theme permit or reject the applicability of multi-stakeholderism.

Addressing these questions takes a short visit to the concept of multi-stakeholder approach (or: model/cooperation) as well as the notion of international cyber security. The idea of multi-stakeholderism is then contextualized in global governance, and international cybersecurity with the view of geopolitics. These manoeuvres lead to the identification of three political moves that make a flat application of multi-stakeholder model problematic. The analysis results in concrete recommendations and mechanisms for accommodating the spirit of multi-stakeholder approach in diplomatic and normative processes of international cybersecurity.

THE ANATOMY OF MULTI-STAKEHOLDER APPROACH

Multi-stakeholder approach is a concept that implies everything and nothing at the same time. Its promise is a voice to voiceless and a statement to those who have something to

[287] Sartori, 1970; Macridis, 1968; Peters, 2013 on conceptual and operational travelling problems. Peters (among others) note the challenge of balancing between sufficiently general and sufficiently specific assumptions, concepts and criteria.

say. As a bottom-up policy development process it is said to "introduce new principles like openness, transparency and rough consensus into global negotiations."[288] The popularity of multi-stakeholder approach is a part of broader move to global governance where states, governments, delegate regulatory powers to private and international organizations.[289]

In the UN cyber politics, multi-stakeholder approach became endorsed in 2001, inviting the private sector and civil society to "actively participate in the intergovernmental preparatory process of the [World Summit on the Information Society, WSIS] Summit and the Summit itself." The WSIS 2003 Plan of Action asked Secretary General "to set up a working group on Internet governance in an open and inclusive process that ensures a mechanism for the full and active participation of governments, the private sector and civil society from both developing and developed countries."[290]

The 2005 WSIS *Tunis Agenda for the Information Society* concluded that "the management of the Internet" is to involve "all stakeholders and relevant intergovernmental and international organizations." The Agenda recognized the stakeholder and distinctive roles as follows:

- Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues.
- The private sector has had, and should continue to have, an important role in the development of the Internet, both in the technical and economic fields.
- Civil society has also played an important role on Internet matters, especially at community level, and should continue to play such a role.
- Intergovernmental organizations have had, and should continue to have, a facilitating role in the coordination of Internet-related public policy issues. International organizations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies.
- Academic and technical communities contributing within the stakeholders to the evolution, functioning and development of the Internet [291]

---

[288] Kleinwächter, 2005.

[289] Bevenisti, 2014.

[290] WSIS, 2003.

[291] WSIS, 2005.

The Tunis Summit agreed to establish the Internet Governance Forum (IGF). The IGF was to become a decentralized, multilateral, democratic, transparent, neutral, non-binding entity with a multi-stakeholder mechanism. As an open forum it was to discuss and give advice on Internet governance and capacity-building. Its role was thus to foster dialogue, give voice to a wide range of views and identify issues that need to be tackled through formal intergovernmental processes with decision-making mandates.[292]

The IGF has been criticized for failing to reconcile controversial views around underlying principles and norms in addressing global rules and procedures. It has said to have diluted the power of states arrayed against the status quo, while acknowledging and continuing to discuss problems without any commitment. For these countries, however, the IGF was acceptable as a mechanism for keeping the developmental and governance issues alive and binding the status quo camp to interaction with them on a new basis, while offering a public platform for mobilizing potential allies at the UN. [293]

Most often the issue of multi-stakeholder governance is of the development and management of the Internet: who decides, an expert organization such as the Internet Assigned Numbers Authority (IANA) and Internet Corporation for Assigned Names and Numbers (ICANN), multi-stakeholder entity such as the IGF or a multilateral organization such as the International Telecommunication Union (ITU), and how to incorporate the opinion of the private sector, civil society, and the individual users.[294]

DeNardis and Raymond remind that since different bodies exert authority over the Internet's technical architecture it is a misnomer to speak of the multi-stakeholder approach as a single thing. Internet governance tasks are divided between several often organically borne expert institutions[295] and mutual cooperation keeps the Internet operational even without a bilateral agreement or centralized governance.

The public Internet, however, is only one application, or an overlay, of cyberspace. Cyberspace consists of plethora of interdependent networks of information technology infrastructures and resident data within. This meta-system encompasses the Internet, telecommunications networks, computer systems, and embedded (often industrial)

---

[292] Desai, 2006. Major countries have lauched their series of international and multistakeholder conferences to discuss Internet and cyberspace development and governance and to advocate their views: the United Kingdom (and the like-minded) the Global Conference on Cyberspace, a.k.a. the London Process in 2012; Brazil hosted *NETMundia*l in 2014, and China *World Internet Conference*, a.k.a. Wuzhen Summit in 2014.

[293] Tikk-Ringas, 2015 referring to Mueller, Mathiason and Klein, 2007, and Mueller, 2010.

[294] For an account of the development of internet governance see for example Malcolm, 2008; Carr, 2015; and Tikk-Ringas (ed.), 2015.

[295] DeNardis and Raymond, 2013.

processors and controllers.[296] Offering or opposing multi-stakeholder approach should take a closer look at the differing demands and dynamics of, for example cybersecurity, Internet standards setting, and the role(s) of private ICT information intermediaries.[297]

Multi-stakeholder model is thus offered as a preferred form of governance maximizing global control, legitimacy and stakeholder profit.[298] The inaugural session of the IGF in 2006 widely accepted that "solving security issues is based on 'best practices' and multi-stakeholder co-operation in an international context."[299]

THE GOVERNMENTS STRIKE BACK

Multi-stakeholder approach finds wide rhetorical support from individual governments. The 2011 US International Strategy for Cyberspace values the representation of "the entire Internet community by integrating the private sector, civil society, academia, as well as governments in a multi-stakeholder environment."[300] Similarly the 2015 BRICS Ufa Summit Declaration repeats the official mantra of multi-stakeholder thinking: "We acknowledge the need to promote, among others, the principles of multilateralism, democracy, transparency and mutual trust, and stand for the development of universally agreed rules of conduct with regard to the network." The BRICS continue with their preferred venue: "It is necessary to ensure that UN plays a facilitating role in setting up international public policies pertaining to the Internet."[301] They have also forwarded a proposal to formalize and institutionalize the IGF.[302]

The US and her like-minded camp emphasize expertise and downplay political, governmental and bureaucratic functions in designing Internet architectures and defining technical rules and regulations. Centralized and political decision-making would not match the speed and

---

[296] Following the latest US policy and doctrinal documents. See also Tikk-Ringas (ed.), 2015.

[297] DeNardis and Raymond, 2013, cybersecurity governance having e.g. the tasks of securing network infrastructure, designing encryption standards, and responding to security problems.

[298] Koskenniemi, 2007.

[299] IGF, 2006.

[300] The White House, 2011.

[301] Ufa Declaration, 2015. Cf. Internet Governance Forum definition of multi-stakeholder cooperation "in the governance of the Internet generally" referring "to the inclusion of all stakeholders as equal participants in the Internet's continuing development" (IGF, 2013); and NETMundial demand that "Internet governance should be built on democratic, multi-stakeholder processes, ensuring the meaningful and accountable participation of all stakeholders" (NETMundial, 2014).

[302] Demidov 2014.

agility of technological advancement.[303] Russia and China, on the other hand, stress sovereignty, equality of the states and the inclusiveness of governance process.[304] As noted they would gladly see multi-stakeholder approach taken place within the UN structures and processes. They question the sustainability of expert-centric governance, regarding it unilateral, unequal and lacking political legitimacy and accountability. The sand in the oyster is the influence Washington has or is perceived to have on the expert institutions and communities and in overall technological development.[305]

Despite overall support to the model, it is unlikely that the governments who do not support domestic dialogue open-heartedly welcome such inclusiveness at the international level either. For some governments the main approach goal is multilateralism, the horizontal widening of the representation, and not the vertical one, taking on-board e.g. human right advocates, minority groups, state monopolies challenging private companies or peace-loving non-governmental organizations.

The underlying problem of the multi-stakeholder approach is not technical or procedural. Treating cyberspace governance as a technocratic management issue is a wrong diagnosis. Adjusting participatory mechanisms, developing new protocols and standards, or increasing the number of seats and tables without recognizing the fundamentally political nature of cyber affairs will not take us further. The expansion of cyber politics to non-governmental layers has made the political disappear.[306]

Moreover repairing the problem of representation by widening and deepening participation does not remove the problem of unassigned accountability. There is no private sector but thousands of companies, from micro small to mega size. There is no clear voice of civil society either but noise, tinnitus, cacophony. They are all stakeholders they are but respective interests at stake are not necessarily shared or openly communicated outside the corporations and 'the organic intellectuals' and their narrow agendas. No extra-national body is delegated or competent to solve the demands set by growingly self-aware and potent developing and aspiring nations.

---

[303] Kramer, 2012.

[304] See for example 'International code of conduct for information security', stating "'All States must play the same role in, and carry equal responsibility for, international governance of the Internet its security, continuity and stability of operation, and its development in a way which promotes the establishment of multilateral, transparent and democratic international Internet governance mechanisms which ensure an equitable distribution of resources, facilitate access for all and ensure the stable and secure functioning of the Internet." (Baodong, 2011).

[305] See for example Tarjanne, 1997; and Xi, 2015.

[306] Macridis, 1968; Sartori, 1970.

THE NUTS AND BOLTS OF INTERNATIONAL CYBER SECURITY

The Russian Federation was the first country to officially raise concerns of the development ICTs and information security in the context of international peace and security. In a letter of 1998 to UN Secretary-General Russia condemned the creation of information weapons and warned of the threat of information war and noted that developments in information systems might be used for purposes that ran counter to the objectives of maintaining international stability and security. The issues raised by Russia included the use of force, interference in internal affairs of states, arms race in creation of information weapons and the threat of information wars with the purpose to damage the information resources and systems of another country while at the same time protecting its own infrastructure. The need to review international law was also tabled.[307] Russia proposed that the topic of international information security be substantively discussed at the United Nations.

The Russian resolution initiated the international cyber security dialogue at the UN. The General Assembly 1998 resolution called all nations to inform the Secretary-General on the questions of the issues of information security, definition of basic notions related to information security, included unauthorized interference with or misuse of information and telecommunication systems and information resources, development of international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality.[308] The 2013 resolution mandating the latest Group of Governmental Experts had expanded but at the same time become more explicit. The resolution spoke of existing and potential threats in the sphere of information security, cooperative measures to address them, including norms, rules or principles of responsible behavior of States and confidence-building measures, the use of ICTs in conflicts and how international law applies to the use of ICTs as well as strategies aimed at strengthening the security of global information and telecommunications systems.[309]

The value of the GGE is the very political, inter-governmental and formalized nature of it. That the cyber troika of China, Russian Federation and the United States have a venue for deep talks, not only defending their positions but being forced to find ways forward and to make compromises is the effect and outcome of it, far more important than the interpretations of the existing international law or working out new norms or security building measures. Another outcome is the number of countries willing to contribute and join the GGE process, showing and taking responsibility to lead international debate and

---

[307] United Nations Disarmament Committee, 1998; Tikk-Ringas, 2015.

[308] United Nations General Assembly, 1998.

[309] United Nations General Assembly, 2013b.

progress. In this respect the process cultivates a global culture of cyber security and links national and international discourses. It is in the interest of governments to maintain this format diplomatic and for them without unnecessary media attention and populism.

The 2013 GGE report recognizes the private sector and civil society: "States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services."[310] The centrality given to the UN and other international organizations become clear in the 2015 report:

> "The United Nations should play a leading role in promoting dialogue on the security of ICTs in their use by States and developing common understandings on the application of international law and norms, rules and principles for responsible State behavior. Further work could consider initiatives for international dialogue and exchange on ICT security issues. These efforts should not duplicate ongoing work by other international organizations and forums addressing issues such as criminal and terrorist use of ICTs, human rights and Internet governance."[311]

International cyber security cannot be separated from any other international security concerns, modes, methods or modalities. For governments, cyberspace has offered a new area of competition, marketplace of ideologies as well as a battlefield to project power, the fifth domain alongside land, maritime, air and outer space environments. The novelty of cyber affairs underlines the perceived insecurity of many have nots.

Three transformative developments in the cyber security discourse speak against effective applicability of multi-stakeholder approach. Alongside technical development and management the political and ideological nature of the cyberspace has become imminent. Standards, protocols and security measures have turned into issues of who gets, what, when and how.[312] Governments will be the first and, for the foreseeable future, the only ones who will have an authoritative say on that. Secondly, the discourse has widened from the management of the Internet to the availability, stability, and peacefulness of cyberspace. The Internet is not the issue but power. Geopolitical great game is signified by the extension of state sovereignty and power projection into cyberspace. States increasingly seek to

---

[310] United Nations General Assembly, 2013a.

[311] United Nations General Assembly, 2015.

[312] Carl Schmitt's notion of the political is here an useful handle. 'The political' notices the contested and conflicted nature of politics as given. A moderate interpretation of competing and justifiable views and claims is found in Lasswell's well-known "who gets, what, when and how" maxim. Similarly Sartori's 'expansion of politics' and Macridis' everything "potentially political" underline politics rather as a discourse than fight of incommensurable views. Perhaps the most powerful antidote to Schmitt's poisonous and abused pessimism is Sen's understanding of democracy as decision-making by debate.

protect and expand their political, ideological and cultural boundaries and spheres of influence in the virtual and informational realm, too. All countries regard ICTs and cyberspace highly useful but many at the same time are fearful of potential foreign influence and interference, both on national information infrastructure and the content of information. Finally, what started as voluntary, organic and good-willing governance, but without explicit delegation of such a mandate, has turned into governmental political and calculative contestation. The governments are back.

CONCLUSION: SQUARING THE CIRCLE

States are sovereign but governments are not omnipotent. As outlined in the 2005 Tunis agenda various stakeholders do have a meaningful role to play and a role that is the most competent to them.

Stakeholders forward multiple of interests: technical functionality, human rights and individual freedoms, information security as well as national security and international stability. All these interests are legitimate. How to effectively accommodate the diverging interest and meaningfully allocate values and resources obliges statesmanship.

As cyber affairs are capillary, it is functionally justifiable to cautiously extend principles and mechanisms of multi-stakeholder approach into the international level of cyber security. Not listening the private sector, civil societies and countries and governments of various size, shape and colour would turn international cyber diplomacy into elitist *Glasperlenspiel* where ultimately its participants would also be left unhappy and unsecure.

Following the *raison d'être* of multi-stakeholder approach four admittedly dissident ways forward are outlined below. The recommendations seek to increase the quality, representativeness and accountability of international cyber security discourse but without diluting the state-centricity of international peace, security and stability.[313]

Firstly, appointing *international ombudsman for civil society* with a duty and mandate to promote the interests of the individual and the civil societies. The tasks of the ombudsman would *inter alia* entail sense, collect and represent the concerns of individuals, minority groups, societal interest groups and non-governmental organizations. The ombudsman would participate in national and international workshops, report publicly her findings and participate in the UN GGE or another such formal mechanism.

Secondly, establishing a *UN ICT Advisor* function working within and in conjunction the UN Scientific Advisor Board with a similar duty and mandate to follow technological

[313] This line-drawing implicitly acknowledges, but without further elaboration here, expert organizations as *primus inter pares* in the development and management of the Internet.

development, initiative and concerns of the industry, developers and service providers. The advisor would report publicly her findings and participate in the UN GGE process or in another formal mechanism.[314]

Thirdly, *rotating participation* in the GGE or the next similar forum. Rotation would bring a formalized promise of participation, limited continuity and performance pressure to give your best to the process or to get into the Group. The P5 countries are obviously the permanent members but for others two consecutive terms could be sufficient tours of duty.

Fourthly, *establishing regional groups of governmental experts* to deal with regional ICT and cyber-specific agendas. This explicit regional mechanism should take place within the existing organizational and administrative boundaries and practises of the major regional organizations, the AU, the ASEAN (and ARF), the OAS and the OSCE. This mechanism would entail close coordination with the UN process but would be mutually supportive.

All four proposed steps would also effectively sensitise international cyber security agenda of peace, security and stability with their perceived concerns and potential measures to nations, societies and private companies. Such travel of issues and ideas is most welcome. It would help to build inter-national, inter-agency and inter-disciplinary understanding often missing in cyber dialogues.

This exchange of views and travelling of interests help the diplomats and the mightiest of powers to acknowledge the nexus between cyber security and national development. The inputs from civil societies and the private sector can make the governments appreciate that cyber security is as much about sustainable livelihood, health and well being, economic prosperity, governance and justice as it is about stability and peace.[315]

---

[314] Private companies as well as academia can participate in a formalized way for example within national cyber and information policy and strategy development and implementation or by providing timely advice to various ministries and agencies on subject-matter issues. Such cooperation entails mutual trust, confidence and courage to flourish. Private companies also exercise influence through lobbying governments and international governmental organizations as well as indirectly by developing architectures, infrastructures, systems and services.

[315] Following the development impact areas of The Global Initiative Against Transnational Organized Crime 2015 report "Results-Based Approaches to Organized Crime and Development." The report is in its methodological rigour and insightfulness is most applicable to the cyber realm, too.

STABILITY FOR CYBERSPACE

Mika Kerttunen and Eneken Tikk

INTRODUCTION

This paper explores whether and how the concepts of 'stability' and 'strategic stability' can be applied to international information and cyber security. The first part opens with examination of the theoretical foundations as well as with the use of the concepts in international relations. It takes the assumptions that emerge from that particular use of the concepts and explores their utility in the context of contemporary ideas about cyberspace. The authors discuss the limits of this conceptual evolution and go on to develop a heuristic model of strategic cyber stability that can strengthen international peace and security in the context of international information and cyber security. Such modelling and specificity is much needed for two reasons. First, the general understanding of 'stability' is too broad. It is frequently applied to diverse elements like social stability and continuity of regimes. Conversely, 'strategic stability' is too narrow with its persistent focus on nuclear weapons and the credibility of deterrence.

The paper applies to three parallel perspectives of cyberspace: a systematic perspective referring to it as interdependent network of information technology infrastructures; an effect-based perspective that observes the impact of information and communication technologies on societal and technical processes; and a political perspective that acknowledges the wider political and security implications of developing, deploying and employing these technologies.[316]

THE CONCEPT OF STABILITY

The notion of stability or international stability in International Relations literature, is not explicitly defined: stability rather refers to a desired outcome of international order and

[316] For definitions of cyberspace see for example ITU, *Measuring Information Society Report 2015* and U.S. Joint Chiefs of Staff, Joint Publication 6-0 *Joint Communications* (10 June, 2015).

stable and peaceful international life.[317] Given this contingent and political use of the notion the mechanism that is considered to lead to or maintain that stability is seen as more important than any specific outcome. These may include balance of power, hegemony, nuclear weapons (and deterrence), collective security, world government, peacekeeping and peace-making, war, international institutions, international law and diplomacy. Finally, they look at the *nature* of international actors and their interactions, typically regarding democracy and trade as stabilizing factors and the basis for the internal strength of states.[318]

According to Deutsch and Singer systematic stability increases the probability of the (international) system retaining its essential characteristics. Stability also prevents any single nation becoming dominant but ensures the survival of the most of members (states) and the avoidance of large-scale war. Accordingly stability for a single state represents the probability of the "continued political independence and territorial integrity without any significant probability of becoming engaged in a war for survival".[319] Hurwitz's five propositions: absence of violence; governmental endurance; existence of legitimate constitutional order, absence of structural change; and multifaceted societal attributes, help to operationalize stability in the spirit of Deutsch and Singer.[320] Dowding and Kimber criticize views that regard stability as *regularity* of behaviour and *normality* of it. They note that the capacity of a political actor is to prevent of incidents that could force its non-survival, and relate stability to threatening contingencies.[321] Drawing on biology and physics Boyd stresses that closed systems inevitably develop entropy that will cause a systematic change, destroying the old one and creating a new one.[322]

Despite that, in an abstract, ideal systematic location stability either exists or not, stability in real world is contextual and raises the question: what about stability and to whom? In the context of information and communication technologies, the stability/instability covers objects and subjects, such as single devices, like a computer operating system, industrial

---

[317] The notions of Pax Romanum, Pax Britannica, Pax Americana as well as the doctrines of *Monroe*, *Brezhnev*, and? *Indira Gandhi* all testify to the desirability ofstable world orders.

[318] Milner, Helen V., "International Political Economy: Beyond Hegemonic Stability", *Foreign Policy*, No. 110, Special Edition: Frontiers of Knowledge (1998), pp. 112-123 at 112-113; Hasani, Enver, "Reflections on weak states and other sources of international (in)stability."

[319] Deutsch, Karl W. and J. David Singer, "Multipolar Power Systems and International Stability". *World Politics*, vol. 16: no. 3 (1964), pp. 390-406 at pp. 390-391.

[320] Hurwitz, L , "An Index of Political Stabiltiy: A Methodological Note". *Comparative Political Studies*, vol. 4 (1973), pp. 41-68.

[321] Dowding, Keith M. And Richard Kimber,"The Meaning and Use of 'Political Stability'". *European Journal of Political Research*, vol. 11 (1983), pp. 229-243.

[322] Boyd, John R., "Destruction and Creation (1976).

processes, global military communications, regional adversary or global superpower relations and the fundamental equation between haves and have-nots.

The capacity of stability is to resist threats and accommodate required and unanticipated changes. This conceptual understanding acknowledges the continuity of the system and its functionality as the most important objective. In this view, stability does not equate to *status quo* despite the prevalence of this discourse - especially in political speech focussing on a cemented political or world order. Although stability can align with the status quo in some circumstances, given the inherent systemic dynamics and specific cyber-technological developments, it is also important to recognize the likelihood and imperative of fairly constant change.

Where security is predominate over an actor-centric perception with relative truth-value, stability refers to a systemic quality that conceptually either exists or does not. As stability focuses on the continuity of operations (e.g. of a political or technical nature), stability as such may or may not bring a sense of security to a particular actor. Here lies a major difference in the political and technical approaches: while political thinking more often than less regards no-change in security (particularly for those actors in secure positions), a technical perspective is able to recognize the need for resilience but also the necessity of change as a guarantee of security.

Similarly, no single issue or measure is by default stabilizing or destabilizing. For example, while the escalation of a confrontation might be considered destabilizing, the risk of escalation in the nuclear deterrence literature, is seen to promote stability in a system because the threat of escalation can often result in the continuation of (or retreat to) the expected and peaceful (more or less) behaviour. The fact that an increasing number of countries are issuing and implementing national cyber security strategies, as well as the development of national and military cyber capabilities, can be seen as alarming in the sense that they exacerbate the gaps between haves and have-nots. But these developments can also be seen as measures that strengthen national systemic resilience, the ability to accommodate technical and behavioural changes, and responsible, predictable state behaviour.

STABILITY AS A POLITICAL CLAIM

Parallel to the conceptual and academic use and understanding of the concept of stability subsists the political use and meaning of the term. What is common in the following non-exhaustive collection of international and national examples, is the obviously contingent, i.e. historical and (even) ideological tune and content. Despite and because of their colour

or consensual flavour the samples signify the political that no past or current report, statement or resolution can escape and which needs to be identified.[323]

The United Nations Security Council welcomed in 1992 (on-going political) changes but recognized their propensity to bring new risks for stability and security of which the most acute arose from changes to state structures. The UNSC noticed that "non-military sources of instability in the economic, social, humanitarian and ecological fields" had become threats to peace and security. It still maintained its established approach of arms control and disarmament: the non-proliferation of weapons of mass destruction, limiting the accumulation and transfer of arms, and to resolve peacefully any problems "threatening or disrupting the maintenance of regional and global stability."[324]

The United Nations General Assembly has adopted several resolutions on information security in the 2000s and 2010s.[325] For example, Resolution 57/239 (2003) spoke of the creation of a global culture of cybersecurity, and Resolution 64/211 (2009) developed a voluntary self-assessment tool for national efforts to protect critical information infrastructures. Successive resolutions on "Developments in the field of information and telecommunications in the context of international security" have both mandated the UN Group of Governmental Experts to study these developments and inform the Group's reports. The 2015 resolution (70/237) expressed concerns that information technologies and means "can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields". Moreover the General Assembly welcomed the GGE 2013 conclusion "that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment, that voluntary and non-binding norms, rules and principles of responsible behaviour of States, in use of information and communication technologies can reduce risks to international peace, security and stability". The Resolution called for the consideration of existing and potential threats as well as possible strategies to address emerging threats. The UNGA took a functional stand when considering that "the

---

[323] On the notion of the political see Schmitt, Carl, *The Concept of the Political* (Chicago: University of Chicago Press, 1996). In short the political is an arena of authority rather than general law and which requires decisions which are singular, absolute and final. Schmitt criticized modern bourgeois (democratic) politics of focusing on compromises that lead to temporary and occasional solutions; not being able to solve the claims of equality; and substituting procedure for struggle.

[324] United Nations Security Council, "Note by the president of the Security Council". S/23500 (1992).

[325] Resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007, 63/37 of 2 December 2008, 64/25 of 2 December 2009, 65/41 of 8 December 2010, 66/24 of 2 December 2011, 67/27 of 3 December 2012, 68/243 of 27 December 2013, 69/28 of 2 December 2014, and 70/237 of 30 December 2015.

purpose of such measures could be served through further examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems".[326]

Between 2014 and 2015 the United Nations Institute for Disarmament Research (UNIDIR) organized a series of Cyber Security Seminars. The seminars did not define or take a position on stability and the reports present the key claims of the seminar speakers. The presentations focussed on threats as well as normative (political and legal) measures to promote security and/or stability, especially confidence-building measures (CBMs) and norms. Here again, the conflation of notions of stability and security was evident as the terms were often used interchangeably. Some speakers emphasized the difference between stability (as a more operational and technical quality) and security (as a wider concept). For example, the Russian representative noted that bilateral agreements (on transparency and confidence-building measures) "cannot by themselves eliminate all threats to international security".[327]

UNIDIR has also published a 'Cyber Stability Tool'. It defines cyber stability as "a geostrategic condition whereby users of the cyber domain enjoy the greatest possible benefits to political, civic, social, and economic life, while preventing and managing conduct that may undermine those benefits at the national, regional, and international levels". The concept paper presents a model that is to "contribute towards the achievement of international cyber stability by improving the capacity of diplomats and policymakers to participate in a more informed and effective manner in dialogue and decision-making processes pertaining to stability in the cyber sphere". The proposed tool is envisaged as a UNIDIR webpage that would guide and assist policymakers to address stability issues with framework documents, recent event briefs and databases such as country profiles and index ("The Cyber Index Tool"). [328]

The United States 2011 "International Strategy for Cyberspace" operationalized network stability (as a condition/state in which states)

- Respect the free flow of information in national network configurations,
- Ensure that they do not arbitrarily interfere with internationally interconnected infrastructure"; and

---

[326] UNGA, Resolution 70/237 (30 December 2015).

[327] UNIDIR, "UNIDIR Cyber Stability Seminar 2014: Preventing Cyber Conflict"; and UNIDIR, "UNIDIR Cyber Stability Seminar 2015: Regime Coherence".

[328] Rudnick, Lisa and Derek B. Miller with Leeor Levy, "Towards Cyber Stability A User-Centred Tool for Policymakers", UNIDIR 2014.

- Continue to recognize? Acknowledge? Respect? the domain name system as a key technology that needs to remain secure and stable.

At the same time, the Strategy regards stability as continuity of expected and accepted norm-guided behaviour. It implicitly refers to the nuclear realm by noting, that "In other spheres of international relations, shared understandings about acceptable behaviour have enhanced stability and provided a basis for international action when corrective measures are required. Adherence to such norms brings predictability to state conduct, helping prevent the misunderstandings that could lead to conflict". The Strategy's call to build "a system of cyberspace stability" where the full range of stakeholders, "particularly those organizations and technical experts vital to the technical operation of the Internet" are recognized and allowed to work explicitly anchoring stability to the model of governance.[329]

The International Security Advisory Board of the U.S. Department of State working under the chairmanship of Congressman Hart was asked in 2013 to examine *inter alia*

- The pros and cons of different strategies for pursuing international cyber stability: particularly global, like-minded coalition, and regional organization approaches;
- How groups of countries could be organized, and how they could operate to promote cyber stability goals; and
- What principles, norms and commitments should guide states that work together to promote cyber stability.

The Board's 2014 report "A Framework for International Cyber Stability" recognized cyber stability as enhancing "continuity of relations between nations in the face of attack or exploitation through cyber means". The report defined cyber security in functional terms consisting of "organizational actions that provide assurance of legal and reliable use of cyberspace, from hardware and software systems to operations and information (data), so that it is protected and usable in the manner expected by its originators and recipients". Accordingly, cyber stability was defined as:

An environment where all participants, including nation-states, non-governmental organizations, commercial enterprises, and individuals, can positively and dependably enjoy the benefits of cyberspace; where there are benefits of cooperation and avoidance of conflict, and disincentives for these actors to be engaged in malicious cyber activity.[330]

---

[329] The White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World* (May, 2011).

[330] Department of State, International Security Advisory Board, *Report on A Framework for International Cyber Stability* (2014), Appendix B.

The report emphasized cyber stability as fundamentally depending on transparency and the knowledge on both sides of their opponent's trigger points - those actions leading to escalatory decisions and to deployment of more powerful capabilities that may result in full spectrum conflict. Fostering transparency, attribution, and the political will to act were regarded, as the critical underpinnings of cyber stability as well as the geopolitical, economic, technological, and legal elements of the cyber stability framework. To avoid unintended escalation, the Board advocated by setting rigorous rules of engagement for US military and civilian organizations in responding to significant attacks using cyber means. Ultimately, the goal "would be to establish a multinational cooperative response mechanism, which would promote confidence in the ability to sustain cyber stability".[331]

The Department of State International Security Advisory Board concluded with nine functional and understandably U.S. centric recommendations:

- Cooperate on crime as a first step;
- Seek international consensus on rules of the road;
- Enhance governments' situational awareness through information sharing;
- Combat theft of intellectual property;
- Expand education and capacity-building;
- Promote attribution and prosecution;
- Lead by example;
- Adopt a two-tier approach for building consensus toward future norms: continued multilateral negotiations along with ongoing efforts to engage bilateral discussions that can, in principle, lead to or at least be compatible with multinational commitments;
- The Department of State should engage the business community in updating, and as needed, forming public-private partnerships that can leverage the diverse expertise of the information and communication technology industries to provide policy and operational and technical expertise to inform, shape, and participate in Department of State efforts.[332]

It should be noted that while the Russian Federation had bilaterally and globally expressed serious concerns about the stability of the international system and relations its 2001 (and

---

[331] Department of State, International Security Advisory Board, *Report on A Framework for International Cyber Stability* (2014).

[332] Ibid, Appendix A.

2008) "Information Security Doctrine" explicitly refers to the importance of political, economic and social stability as well as the stability of state authority. The doctrine took a national-administrative perspective with "a totality of official views on the goals, objectives, principles and basic guidelines for ensuring information security in the Russian Federation".[333]

A 2015 statement by the U.S. Director of National Intelligence on Worldwide Cyber Threats" did not explicitly address stability but testified, that "the likelihood of a catastrophic attack from any particular actor is remote at this time". Rather than foreseeing a "Cyber Armageddon" scenario that would "debilitate", and by definition destabilize, "the entire US infrastructure, the Office foresaw an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security".[334] The 2016 statement "Worldwide Threat Assessment" elaborated further on instability and saw its sources mainly in a nation state and regime context. Stability then, was regarded here as the continuation of any regime or established mechanism, for example international trade and the financial system.[335]

THE CONCEPT OF STRATEGIC STABILITY: BACKGROUND AND HISTORICAL ORIGINS

Stability either looking at *status quo* or recognizing the need of constant change did not alone serve the security purposes of the superpowers. The development of nuclear devices and their delivery platforms in the 1950s created fear of a devastating surprise attack paving way to the concept of strategic stability.[336] The concept became to centre on vulnerabilities

---

[333] The President of Russian Federation, *Information Security Doctrine of the Russian Federation* (2000 and 2008). In Soviet and Russian political language change and continuity have been present. On one hand the Bolshevik and *Komintern* advocated for world proletarian revolution and supported many liberation movements in the colonies and the developing world, on the other Soviet leaders defended the post-World War II regional order in Europe. See for example Brezhnev, Leonid, "Sovereignty and the Internationalist Obligation of Socialist Countries" (Originally published in *Pravda, September 25, 1968*, reprinted in Tuathail, Gearóid Ó, Simon Dalby and Paul Routledge, *The Geopolitics Reader* (London: Routledge, 1998, pp. 90-93) as well as President Putin's views that the collapse of the Soviet Union being on the greatest tragedy of the 20th century.

[334] Clapper, James R., "Statement for the Record. Worldwide Cyber Threats", House Permanent Select Committee on Intelligence (10 September, 2015).

[335] Clapper, James R., "Statement for the Record. Worldwide Threat Assessment of the US Intelligence Community", Senate Armed Service Committee (9 February, 2016).

[336] For example two international conferences on "measures to safeguard against surprise attack" were arranged in 1958; one in Washington, D.C. among the five leading western nations and another in Geneva that included also five socialist/communist countries.

and mutual capabilities to retaliate. In very twisted way certain instability especially by accepting the risk of escalation became to ensure security.[337]

The concept and theory of strategic stability was developed in the writings of Albert Wolhstetter, and Thomas S. Schelling. Wohlstetter's seminal 1958 RAND article (and the January 1959 *Foreign Affairs* paper) "The Delicate Balance of Terror" argued that the key issue in deterrence is the ability to survive a nuclear attack and then to strike back: "*to deter an attack means being able to strike back in spite of it*". Because the vulnerability of nuclear forces to a surprise attack could not be removed, high-alert status of forces and pre-emptive strategy, and later submarine launched ballistic missiles, became the solutions to guarantee such a strike-back capability.[338] Accordingly, the 1958 U.S. Interagency Working Group on Surprise Attack aligned strategic stability with freedom from surprise attack that depended "not only on an inspection of one's potential enemy and limitations on his forces, but also very heavily on the vulnerability of one's own retaliatory forces". In these unavoidable circumstances it became essential to reduce the vulnerability of such forces "to acceptable levels in order to safeguard their effectiveness as retaliatory forces".[339]

Wohlstetter and Brodie both regarded the mutual (U.S. – Soviet) vulnerability as a stabilizing factor. Schelling turned the necessity to a virtue. The vulnerability of one party would ensure the other of its capacity to retaliate. Such an assurance would help to prevent nuclear war, and thus increase stability in the nuclear equation.[340] The survivability of command and control and weapons systems denied ultimate victory and the vulnerability to attack ensured the likelihood of retaliation. Gerson credits Schelling not just with making stability an essential metric for evaluating nuclear forces but with ensuring that the concept of stability became the new rationale for U.S.-Soviet nuclear arms control. Arms control took distance from disarmament and started to focus on risk-reduction by enacting restrictions on nuclear arsenals of both sides to minimize the fear of surprise attack and ensure that both sides possessed a second strike capability.[341]

---

[337] See espeacially Ogilvy-White, Tanja (ed.), *"On Nuclear Deterrence. The Correspondence of Sir Michael Quinlan"* (London: International Institute for Strategic Studies, 2011).

[338] Schelling , Thomas, "Foreword", in Colby, Elbridge A. and Michael S. Gerson (eds.), *Strategic Stability* (Carlisle PA: Strategic Studies Institute, 2013), p. v-vi; Gerson, Michael S., "The Origins of Strategic Stability: The United States and the Fear of Surprise Attack", in Colby & Gerson, pp. 3-12; Albert Wohlstetter, *RAND P-1472* (1958); http://www.rand.org/publications/classics/wohlstetter/P1472/P1472.htm; also Wohlstetter (1959), "The Delicate Balance of Terror," *Foreign Affairs*, vol. 37, no. 2

[339] "Report of the Interagency Working Group on Surprise Attack," August 15, 1958, p. 1, quoted in Gerson (2013), p. 30.

[340] Schelling, Thomas C., *Surprise Attack and Disarmament* (Santa Monica, CA: RAND, (1958), and Schelling, Thomas C., *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960).

[341] Gerson, p. 35.

The demise of Soviet Union and the dissolution of the Warsaw Pact did not change how strategic stability is understood in international politics. The political, economic and military rise of the People's Republic of China has only solidified the nuclear and strategic weapon system centric setting. The U.S.-Russia and the U.S.-China relationships and an attitude of arms control continue to function as the main conditioning framework for both the established nuclear and the emerging security-stability questions.

In "Soviet-U.S. Joint Statement on the Treaty on Strategic Offensive Arms", issued in June 1990 when one signatory was already crumbling, the parties agreed upon their mutual responsibility to enhance strategic stability. In particular the reductions in several nuclear weapons systems were designed to make a first strike less plausible, which in turn was said to result in "greater stability and a lower risk of war".[342] Similarly the "U.S.-Russia Joint Statement: Cooperation on Strategic Stability" underscored in July 2000 "that continued strengthening of global stability and international security is one of the most important tasks today" and established a basis to (further) reduce nuclear weapons arsenals and preserve and strengthen the Anti-Ballistic Missile Treaty. Furthermore, the Statement noticed the need to confront "new challenges to international security" and called the other nation to unite Russo-American efforts to strengthen strategic stability.[343]

STRATEGIC STABILITY IN CYBERSPACE

Global debates about stability and cyberspace replicated the political discourse described above; they also conflated security and stability. Depending on the political discourse stability in cyberspace oscillated, and still does, between either preventing political change or ensuring the functionality of information and communication systems.

Despite the fact that the Russians had expressed their concerns about the creation and employment of "information weapons" in September 1998 the July 2000 Joint Statement did not elaborate on this new security challenge. Russia had explicitly referred to the potential use of information technologies and weapons (i) "for purposes incompatible with the objectives of ensuring international security and stability", (ii) to "actions taken by one country to damage the information resources and systems of another country while at the same time protecting its own infrastructure", as well as (iii) to "the destructive 'effect' which may be comparable to that of weapons of mass destruction" - all observations that speak of alarm at strategic stability being eroded by rapidly advancing technology and a hegemonic possession on the part of one nation. To mitigate this perceived threat Moscow forwarded in the same letter a draft resolution that invited discussions on this and the

---

[342] "Soviet-United States Joint Statement on the Treaty on Strategic Offensive Arms" (1 June, 1990).

[343] "Joint Statement: Cooperation on Strategic Stability" (21 July, 2000).

development of "international legal regimes to prohibit the development, production or use of particularly dangerous forms of information weapons."[344]

Similar concerns and wordings were expressed in the "International code of conduct for information security" proposal China, Russia, Tajikistan and Uzbekistan forwarded in 2011. These countries recognized the threat to international stability and security as well as to national political and societal security that the use of information and communication technologies could potentially bring about. The "Code of Conduct" linked the rights and responsibilities of states, the responsible behaviour of states, and the use of information and communication technologies for social and economic development, to the objective of maintaining international stability and security.[345]

More recently, although the language of strategic stability remains largely absent, we can see the same logic and rationale beginning to emerge in policy documents. Echoing the understanding of the danger of unpredictability and surprise in international relations that guided Schelling's thinking on strategic stability, the 2013 "U.S.-Russia Cooperation on Information and Communications Technology Security" speaks of the need to "reduce the possibility that a misunderstood cyber incident could create instability or a crisis in our bilateral relationship".[346]

Strategic stability functions as a pattern of thought fundamental to the theory and policy of deterrence. It has become one cornerstone in superpower relations. The concept of strategic stability is dualistic, dynamic and contextual. It operates with the desire of survival and the knowledge of vulnerability as well as change it can also have utility beyond them. For example the U.S. Nuclear Posture Review (NPR) lists the maintenance of strategic deterrence and stability at reduced nuclear force levels as one of its goals. The NPR notes that bilateral dialogues with Russia and China on missile defence, space-related issues, conventional precision strike capabilities, and nuclear weapons issues promote more stable and transparent strategic relationships.[347] Another example of this thinking is President Putin's rhetoric justifying the suspension of an agreement with the U.S. on the disposal of

---

[344] United Nations General Assembly, "Letter dated 23 September 1998 from the Minister for Foreign Affairs of the Russian Federation addressed to the Secretary-General", United Nations General Assembly, A/C.1/53/3 (30 September, 1998).

[345] United Nations General Assembly, "Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General", A/66/359 (14 September, 2011). In January 2015, six members of the Shanghai Cooperation Organization (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan) proposed an updated version of the International Code of Conduct for Information Security to the United Nations with an among others an up-date noticing the risk of the use of ICTs interfering "in the internal affairs of other States or with the aim of undermining their political, economic and social stability".

[346] The White House, "U.S.-Russian Cooperation on Information and Communications Technology Security", 17 June, 2013.

[347] Rose, Frank A., "Strategic Stability in East Asia", remarks at The Johns Hopkins-Nanjing Center for Chinese and American Studies, Nanjing, China (8 December, 2014).

plutonium from decommissioned warheads. For him the radical change in the environment, i.e. the U.S. "hostile actions" and "inability to deliver on the obligation", constituted a threat to strategic stability-a stand echoing the sentiments of becoming vulnerable."[348]

It is important to acknowledge that while some existing concepts can help us to make sense of new circumstances, the lessons and concepts of the nuclear era cannot be 'copy-pasted' into the cyber age and space. Any definition or operationalization of strategic stability in cyber affairs or space must take account of the key principles of the concept. Similarly the notion of 'strategic' pays attention to issues of war and peace, international peace and security, and national survival. Significantly, not all cyber problems are strategic. Consequently, any attempt to apply the concept of strategic stability to cyberspace requires a full comprehension of the idiosyncrasies of cyber/information and communication technologies, systems and services.

Both nuclear and ICT systems are obviously vulnerable, thus underlining the necessity of survivability of systems and the continuity of critical operations. These realms also differ quite fundamentally. Firstly, while mutual vulnerability is regarded as a stabilizing factor in nuclear relations, vulnerability in cyberspace is a destabilizing factor. Secondly, in nuclear affairs zero tolerance of error (i.e. nuclear strike or technical error) is a realistic goal in cyber affairs and every actor needs to tolerate errors including continuous attacks and technical failures. Finally, while some have reworked the concept of deterrence in cyberspace by focusing on 'deterrence by denial', however limited, deterrence by punishment remains questionable for a number of reasons.

On the basis of the perspectives and parameters elaborated above, a tentative definition of strategic stability in cyberspace can be set out as follows (a):

> *Conditions in which serious political-military conflict can be averted and the continuity of political relations and the functionality of global techno-strategic systems, networks and processes is secured.*

Such techno-strategic systems encompass global command and communication infrastructure, information and telecommunication systems, and financial and logistic systems as well as strategic weapons systems. These *inter alia* include superpower military command, control and communication, intelligence and reconnaissance, global positioning, energy production and air and maritime transportation systems as well as the public Internet without which nations could not operate the manner they wish and are accustomed to.

---

[348] Russia Today, "Putin signs decree suspending Russia-US deal on plutonium disposal over hostile US actions" (3 October, 2016).

In this context it should be remembered that the Internet does not constitute the whole of cyberspace but is one part of it.[349] Thus cyber stability/instability concerns with going beyond the public Internet to the ability to conduct and continue national, governmental, societal and military operations. Therefore, as such essential Internet focused measures can be necessary but remain insufficient.

CONCLUDING REMARKS

Examining the notions and the applicability of stability in cyberspace perhaps raises more questions and provides answers. If and when accepting stability dualistically consisting of continuity and change, we have to ask of the factors and conditions of both permanence and alteration. We can rather easily end up with similar accounts of factors as did the IR scholars with the notion of stability: the *nature* of the international system, the *means* or *institutions* designed for the management of power relations (and governance) within the international system and the *nature* of international actors and their interactions. The role of these-or other-factors is yet not given. For example, technological development seldom creates a paradigmatic change. On the contrary, the added value of devices and service aggregates incrementally. Yet over time separate innovations, devices and services can create a mutually amplifying effect. Within the defence sector several innovations from machine guns through bomber planes to the atom bomb and the deployment of information and communication technologies were believed to cause a revolution in military or strategic affairs. Not even the latest 'buzzword' of 'hybrid war' can change the nature of war, only some characters appear new to those who have not properly studied war.[350] Most importantly the value the States give to any factor is a determinant of their political ideology and ambitions: stability is what States make of it.[351]

What States can make of it is to take stability in cyberspace seriously. Applying a systemic understanding of stability that emphasizes the continuity of operations and stability-as-controlled-change technical and political measures that can promote national and international cyber stability necessitates:

---

[349] U.S. Joint Chiefs of Staff, JP 6-0 *Joint Communications*, 10 June 2015; Tikk-Ringas, Eneken (ed.), *The Evolution of the Cyber Domain* (London: IISS/Routledge, 2016).

[350] Tikk-Ringas, Eneken (ed.), *The Evolution of the Cyber Domain* (London: IISS/Routledge, 2016). On the permanence of the nature of war see Clausewitz, Carl von, *On War* (translated by Michael Howard and Peter Paret) (Princeton: Princeton University Press, 1984), Book 1, Chapter 1:28.

[351] To paraphrase Alexander Wendt's groud-braking article "Anarchy is what States Make of it: The Social Construction of Power Politics" (*International Organization,*, Vol.. 46, No. 2 (Spring, 1992), pp. 391-425).

- National cyber capability development to establish frameworks and mechanisms to ensure the continuity of technical and political operations, i.e. handle threats and incorporate technical and societal development;
- International capacity-building that by applying known standards and criteria but recognizing contingent needs supports national cyber/ICT endeavours;
- Based on its established track record of maintaining and developing the Internet that continue the expert and multi-stakeholder-centric Internet governance model;
- Establish institutionalized mechanisms that regionally and/or globally address issues of political or technical instability, the former include the continuation of global or bilateral cyber consultations, and the latter not only transparency but increasingly cooperative confidence-building measures, and enhancing in a controlled manner ITU's capacity to work with States and groups of States (as this has taken place anyway, staunch resistance would only promote the other camp argument and keep the like-minded one passive or reactive at best).

NATIONAL CYBER SECURITY STRATEGIES: COMMITMENT FOR DEVELOPMENT

Mika Kerttunen, Eneken Tikk

INTRODUCTION

Cyber is not a technology but an agenda encompassing various goals and ambitions centered on the development and proliferation of ICTs. National values, ambitions and goals determine the directions of the development of security policies and strategies. National priorities and resources condition the depth and scope of activities. There is no pre-determined way or model or strategy to embracing ICTs in national development: countries and governments need to prioritize among competing but legitimate objectives, allocate scarce resources, and take calculated risks based on their own assessments and realities.

In the aftermath of the 2007 cyber attacks against Estonia technologically and economically advanced countries have driven a security-centric approach to national cyber strategies. Cyber security strategies became measures of political and technical crisis management. The first wave of strategies led some analysts to observe *inter alia* difference in understanding what cyber security is supposed to cover, the unclear relationship of the strategies with existing national and international policies as well as the lack of dynamic approach to cyberspace (technological) threats and challenges. National approaches also lacked explicit methodology and criteria as to tactical and operational plans [action plans].[352]

Some more advanced countries have recently updated their late 2000s strategies by increasing/furthering their political, operational and technical ambitions, expanding their focus, for example to include offensive military capacity, and developing measures and

[352] Eric Luiijf, Kim Besseling, Maartje Spoelstra & Patrick de Graaf, "Ten National Cyber Security Strategies: a Comparison", *CRITIS 2011 – 6th International Conference on Critical information infrastructures Security*, September 2011, also Eric Luiijf, Kim Besseling and Patrick de Graaf, 'Nineteen national cyber security strategies', *International Journal of Critical Infrastructure Protection*, Vol. 9, No. 1/2 (2013), p. 3–31.

mechanisms of implementation. The European Union, the North Atlantic Treaty Organization, the Organization for Security and Cooperation in Europe, the Organization for American States, the African Union, and the ASEAN Regional Forum all have taken determined and nuanced approaches to cyber security. Moreover, the United Nations Group of Governmental Experts on "Developments in the Field of Information and Telecommunications in the Context of International Security" has addressed issues to promote peace and stability in State use of ICTs. By discussing issues such as the applicability of International Law, norms, and confidence-building measures the GGE reports politico-normative standpoints, for national cyber security strategy development.

This positive statistics offers also important evidence of absence: the majority of states (governments) have not formulated or published cyber security strategies.[353] The on-going and unfinished strategy and capability development underlines the need to continuously attend global, regional and national policy, strategy and capability development trends and patterns. It also frames the proliferation of capacity-building initiatives as well as national, international and commercial models and methods to support the development of national cyber security strategies.

This policy brief advocates attention to the ambition, direction and content of national cyber security strategies, focus on reliable methodologies to evaluate the impact of policies, and, most importantly, and emphasis on sustainable and development-oriented capacity building. With the development and proliferation of ICTs and other high technologies, national strategies in the field require continuous review both as a process and as products. This paper forwards an engaging and strategic approach that recognizes and respects the contingent and political national cyber security strategy processes.

NATIONAL CYBER SECURITY STRATEGY

Strategy can be understood as a pattern or method of thinking, an administrative process or a manifestation of policy that is in form of an issued instrumental document. Strategic thinking is a balanced calculation between ends, ways and means, or in other words between objectives and resources. Moreover, strategy and strategic decision-making by choosing between contesting but legitimate alternatives takes and needs to take deliberate risks.[354]

---

[353] Depending on criteria 50-60 countries have by the beginning of 2016 have a policy or strategy on cyber or information security, well over hundred states are at least imlicitly working on cyber policies or strategies.

[354] Colin S. Gray, *The Future of Strategy* (Cambrigde: Polity, 2015), p. 23-42. See also Lawrence Freedman, *Strategy* (Oxford: Oxford University Press, 2014), especially page xii on strategy as "the central political art" and "the art of creating power."

Strategy as an administrative process constitutes of organized work to define objectives and design overarching and long-term policies and action plans as well as implement, steer, and improve such policies and plans. To be effectively implemented, strategies as manifestation of policies and plans need to be communicated.[355]

The purpose of an issued strategy is to inform and educate domestic and foreign audiences of providing political guidance by articulating objectives, choosing priorities and allocating resources as well as legitimizing the direction and content of taken policy. By forwarding intentions, direction and capabilities security and defence strategies, there are also possible to create deterring effects on the potential or known adversaries. In fact, a lack of explicit strategy or policy can lead to question of the efficacy and legitimacy of governmental and official activities. On the other hand national, political and administrative cultures differ, and instruments, such as issued legislation, adopted proposals, government decisions, and development plans can fulfil the purpose of a strategy document.[356] More important than the purity of the process and structure of documents is the determined and successful implementation of the chosen policy: issuing a strategy does not end but starts real work.

Strategies need to be tailored to match the political, operational, financial and technological realities and stages of development of the actor and its environment. Thus, there is no uniform ambition, direction or content to be followed or be evaluated by. A functional national security strategy:

- Defines and prioritizes national, strategic objectives;
- Remains focused on the clearly identified core issues;
- Maintains a long, rather than short-term perspective;
- Aligns and is harmonized with other policies and strategies;
- Clearly allocates resources and responsibilities;
- Implements international best practices and lessons learned;
- Considers international cyber security trends and currencies; and
- Frequently reviews the process as well as the objectives, methods and means chosen.

---

[355] Often the notions of *strategy* and *doctrine* can be used interchangeably or in hierarchical order: strategy – doctrine or doctrine - strategy. Strategies can accordingly be characterized as doctrinal policy papers.

[356] Of countries not having issued explicit cyber or information *strategies* Israel is the most notable example. Hardly anyone can nevertheless question the cyber or information and communication technological prowess of this nation. The Israeli Government nine pages long Resolution 3611 "Advancing National Cyberspace Capabilities" (2011) outlines Israeli cyber policy
(http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf.)

To sum up, strategy asks and answers to three fundamental questions: where are we; where do we want to go; and how do we get there?

To locate the starting point and the 'ground-zero' state of performance, it requires analysis of the current state of cyber prowess and cyber security as well as 'real' and anticipated threats and risks in question. The difficulty is not only of cognitive nature but also of political correctness: national planners and decision-makers need to admit shortcomings and acknowledge domestically sensitive issues, e.g. incompetent administration or agencies, state or private telecom and internet service provider monopolies, money laundering, or the surveillance of political dissidents and insurgents.

Defining the direction, it requires strategic vision. The importance of IT and ICTs are generally recognized but perhaps too often from a narrow, single sector or tactical perspective. The strategic choices before any government require considering national values, societal development, national security, and geopolitical gaming. Deciding on the ways and means seems easy – at least in the sense that there are both guidance and lucrative services and products available promising to fill the gaps between the present and the future.

By developing national cyber security strategies and respective capabilities, governments commit to responsible, comprehensive, forward-looking policies that increase their developmental capacity and help achieve national ambitions. Effective implementation of strategies will narrow capability and performance gaps, reduce perceived insecurity and foster international cooperation. In sum, strategies help determine and analyze shared expectations to responsible State behavior and guide international cyber policy-making.

As long as there is no wider sufficient systemic understanding and technical competence cyber policy is by necessity driven by technical considerations. Without holistic understanding and vision of the potential and consequences of the use of ICTs national and intergovernmental policies easily become or remain incremental. Comprehensive and detailed analysis and planning, therefore in itself indicates maturity and high level of strategic preparedness. The majority of countries do not have the culture, confidence or competence of coordinated cyber policy planning and implementation.

FRAMEWORKS, MEASURES, AND INDEXES

In the wake of national information technology, information and communication technologies, and cyber or information security strategies, a number of national, international and commercial assessment tools and maturity models have emerged. Nations are ranked by various ICT, *e-*, cyber and cyber security postures and profiles. The simplest of assessments pay attention to technical and other rather easily measurable indicators, such as telephone connections, Internet penetration, financial expenditure, and manpower.

More sophisticated analyses pay attention to a wider range of capability factors or elements such as legal and political frameworks, organizational measures, technical measures and levels, and national and international cooperation. Measures and rankings pledge tangible benchmarks to promote development of national ICT and cyber policies and strategies as well as advanced culture of cyber security.

These models depart from defining factors, dimensions or key performance indicators which existence and level of implementation are assessed. The most metrical of assessments break findings into weighed factors to produce individual scores and international rankings. Some frameworks remain principal and take distance from rather prescriptive checklist typologies.

The objectives and methodologies (typologies, methods, and criteria) of the recently developed and employed assessment models are summarized in the annexed table. The table includes the [UN] International Telecommunication Union (ITU) *Global Cybersecurity Index and Cyberwellness Profile* (GCI)*;* the Commonwealth Telecommunication Organization (CTO) *Commonwealth Approach for Developing National Cybersecurity Strategies*; European Union Agency for Network and Information Security (ENISA) [An] *evaluation framework for National Cyber Security Strategies*; University of Oxford, *Cyber Security Capability Maturity Model* (CMM); Melissa Hathaway and Potomac Institute for Policy Studies, *Cyber Readiness Index* (CRI)*;* and Australian Strategic Policy Institute (ASPI) International Cyber Policy Centre *Cyber Maturity in Asia-Pacific Region*.[357]

The benefits of evaluation as summarized by the ENISA *Evaluation framework* are:

- Evaluation can inform about policy changes and the framing of issues in the long term; allow learning from past experience;
- Evidence of effectiveness or learning can support the accountability of political action;

---

[357] The [UN] International Telecommunication Union, Global Cybersecurity Index and Cyberwellness Profile (https://www.itu.int/pub/D-STR-SECU-2015); the Commonwealth Telecommunication Organization, Commonwealth Approach for Developing National Cybersecurity Strategies (2015) (http://www.cto.int/media/foth/cybsec/Commonwealth%20Approach%20for%20National%20Cybersecurity%20Strategies.pdf); University of Oxford, Cyber Security Capability Maturity Model, v. 1.2 (15 December 2014); European Union Agency for Network and Information Security, An evaluation framework for cyber security strategies (https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1); Melissa Hathaway, *Cyber Readiness Index 2.0.* Potomac Institute for Policy Studies (November 2015), see also Hathaway, *Cyber Readiness Index 1.0.* Hathaway Global Strategies LLC (November 2013); Australian Strategic Policy Institute International Cyber Policy Centre (ASPI), *Cyber Maturity in Asia-Pacific Region 2015,* https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2015/Cyber-Maturity-2015.pdf. In addition the ITU as well as NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) have published handbooks that discuss in detail strategy development as a process (Frederick Wamala, *ITU National Cybersecurity Strategy Guide* (Geneva: ITU, 2011); Alexander Klimburg (ed.), *National Cyber Security Framework* (Tallinn: CCDCOE, 2012)). The latest of cyber indexes, the Estonian one and for example the World Economic Forum *Network Readiness Index* are excluded from this analyses.

- Evidence base can give credibility towards general public and international partners;
- Evaluation can support outreach and enhance public image as transparent organization;
- Having facts on what works can help gain traction in policy process;
- Evaluation makes it necessary to compile data sources on policy and its implications for long-term planning; and
- Catalysis discussion with stakeholders.

Accordingly ENISA lists the challenges of:

- Evaluation needs investment of resources;
- Exposing flaws in policy can undermine political priorities even when the priorities themselves are supported;
- Good practices can be of limited use due to differences in national evaluation cultures;
- Outcomes are often challenging to define and measure; and
- Attributing changes to the strategy itself can be difficult.[358]

Indeed for the purposes of useful advice of strategy, one either has to cautiously select the dimensions and factors that need to be assessed or apply a more holistic approach that tries to accommodate all relevant aspects. For example, military cyber capability development, a fact deductible from empirical analysis of national security strategies, is absent in the most assessment tools promoting economic growth; or some emphasize critical infrastructure protection and its modalities. As such, the dimensions, elements and factors that the models deploy are correct, but they can remain blind to other theoretically as 'real' or nationally preferred aspects of cyber or information security.

However, ranking nations for the purposes of strategy development is unnecessary and potentially counterproductive. Indexing and ranking implicitly promote relative country positions and reward political and administrative attention over implementation and performance. Most importantly indexing and ranking does not pay attention to the impacts, outcome of policy. Invalid measurement taxonomies and uncritical selection of criteria and evidence produce results that many cyber policy and security professionals find at best amusing. This impotence of assessment is dangerous if politicians and public truly start to believe in these propagated national strengths or weaknesses. One can also critically ask how many international rankings and measures are enough?

---

[358] European Union Agency for Network and Information Security, *An evaluation framework for cyber security strategies*, p. 7, drawing from the research of Furobo, Knill, and Weiss, yet with a slightly more positive view of the impact of evaluations.

The debility of the indexes and measurement tools does not lie in their taxonomies or specific methods, which can be fine-tuned *ad infinitum,* but on the very reductionist logic of the models. Firstly measuring models are built on a number of implicit and questionable assumptions on their validity, and secondly they are at one and the same time ahistorical, apolitical and astrategic.

In general the assessment models assume that

- The total fulfilment of the measured [selected] criteria equals perfection and certainty of cyber prowess;
- The total fulfilment of the criteria is in the best interest of all nations;
- All nations need, want and are able to fulfil these criteria.

Thus, the existing models expect uniform, maximalist and pre-determined behaviour in admittedly interlinked but still diversified field of national policy-making where national priorities differ, authoritative allocation of values is challenging and where intellectual, financial and material resources are scarce. By promoting paradigmatic views of cyber security strategy any indexing and measurement model contradicts the very notion of strategy and strategic thought.

Many models explicitly promote western and technologically advanced countries' values such as market economy and growth, democracy and transparency, and technological solutions to social and political issues. One does not need to contest the inherently good of these values to observe that many nations and in particular governments do not wholeheartedly share these values. Models can be fully correct but without being accepted would still remain irrelevant. For example, the notion of harm is not universally shared: for some regimes the spread of ICT services represents harmful development. While recognizing the traps of overgeneralization, patronizing or colonial attitude or balkanization of the cyberspace regional emphasis need to be acknowledged in the well-meaning capacity enhancing initiatives.

Strategy, on the other hand, is by definition contingent and calculative. As a practise strategy, it can be understood as the use of tactical engagements for broader purposes,[359] but strategic thinking and strategic decision-making cannot be reduced to prefixed lists of tactical and technical activities. Improving the models and tools by adding, removing or fine-tuning the dimensions, elements or factors or changing their metrics will not remove the fundamental problem of reductionism.

By not explicitly recognizing and discussing alternative directions and solutions the employed tools and imported models are prone to neglect the contingent, predominately political

[359] Following Clausewitz's known logic of strategy as "the use of engagement for the purposes of war."

nature of strategy-making, the uncertain balancing between contesting but justifiable views that compete in democracies as well as in totalitarian regimes. Policy making stems from national political, societal, cultural and organizational realities.[360]

JETZT WOHIN?

The critique above does not deny the value of indexes or maturity models. Empirical research points out that evaluations and assessment have less impact to strategy and policy formulation but can have more impact to the implementation of the on-going policies. Whereas the former is explained by the dominant role of values and ideology in fundamental policy questions as well as the influence of competing pressures and objectives, the latter builds on the instrumental match between implementation as problem and evaluation as answer.[361] Surveys, interviews and workshops with baseline analysis can promote self-awareness, and with the help of implicit or explicit carrots and sticks the measuring models get national authorities to meet, talk and work together.

A guidance that better regards national ambitions and political and material realities, answers to the essential and difficult questions of strategy, and supports governments to build endogenous capacity for becoming strategic is nevertheless needed. Without abandoning technical and political security requirements national cyber security strategies can become positive tools of societal development and instruments of international peace and regional stability.

An approach, *Commitment for Development*, consisting of the interlinked aspects of Direction; Strategic Capacity; and Policy Analysis is shortly presented below.

Direction

The commonly prioritized capability areas of the contemporary national cyber and information security strategies can be grouped into six, partially interlinked and generally progressive, categories: Information assurance and basic network protection; Critical Infrastructure Protection; Internal (national) security; Military cyber defence; Integrated cyber policy; and International Capacity building. Within these categories, countries have very diverse political and technical ambitions, challenges and opportunities.

---

[360] Strategy-making is by default decision-making of who gets, what, when and how to paraphrase Harold Lasswell's maxim (and the name of his 1936 book on politics). See also ITU *Guide*, p. 5 and 35-39.

[361] Jan-Eric Furubo, "The Role of Evaluations in Political and Administrative Learning and the Role of Learning in Evaluation Praxis" *OECD Journal on Budgeting*, 3(3) (2003), p. 67-86; Furobo concludes that "[T]he information acquired from evaluations does not seem to be a major explanation for significant policy changes" (p. 72); Carol Hirschon Weiss, "The interface between evaluation and public policy", *Evaluation*, 5(4) (1999), p. 468-486.

Accordingly, the CCDCOE *National Cyber Strategy Framework Manual* discusses of five opposing choices (named as "The Five Dilemmas of National Cyber Security") that represent competing directions of cyber security strategies:

- Stimulation of the economy vs. improving national security;
- Modernizing infrastructure vs. protection of critical infrastructure;
- Private sector vs. public sector;
- Data protection vs. information sharing;
- Freedom of expression vs. political stability.[362]

The *Manual* pays attention to the contingent national conditions developing over long period of time "determine the current placement of functions and the course of existing institutions".[363]

The CTO *Approach* emphasizes the need of cyber security strategy to align to the country's development goals and plans as well as relate to other relevant national strategies and initiatives such as for broader national security, telecommunications, education, energy, trade and industry, tourism, law enforcement and defence. The CTO also pays attention to national and Commonwealth principles as "the guidance in the development of national strategic goals."[364]

Contemporary national cyber security strategies have various ambitions. Many seek to set, develop and maintain necessary technical and organizational capacities within data and information security and network protection as well as subsequent supportive capabilities such as legislation, organization and workforce development; some seek to develop processes and performance across the public sector with an increasing emphasis on e-services and commerce; an increasing number of countries seek qualitatively improvement by all-societal multi-stakeholder approach with an increasing emphasis to international cooperation and to the role of armed forces; and few pursue to integrate national and international cyber security policy and considerations as an omnipresent aspect and ambition in support of all major national policies, predominately national security strategy, foreign policy, defence policy, and economic and development policy, as well as a way of societal and private life.

---

[362] Melissa Hathaway & Alexander Klimburg, "Preliminary Considerations: On National Cyber Security" in Klimburg (ed.), *National Cyber Strategy Framework Manual*, p. 34-43.

[363] Eric Luiijf & Jason Healey, "Organizational structures and considerations" Klimburg (ed.), *National Cyber Strategy Framework Manual*, p. 120.

[364] Commonwealth Telecommunication Organization, *Commonwealth Approach for Developing National Cybersecurity Strategies* (2015), p. 9. On value-based approach see also Wamala, *ITU National Cybersecurity Strategy Guide*, p. 42-45.

The mastery of strategy does not lie in maximal pursuance of any or every relevant objectives but being able to allocate and use resources optimally: doing less is as good an option than doing more. As the CTO *Approach* explains "it is unlikely that a country will want to devote the necessary resources towards achieving the highest levels of maturity in all aspects of cyber security" and that "every country will have to consider the stages of maturity that can be attained and must prioritize this against competing demands for resources to meet other national strategic goals."[365]

In fact defining its direction, a national cyber security strategy have to look backwards to the fundamental base values and forward to desired end-state(s): know yourself and know your destiny. The end-ways-means maxim of strategy, in the case of cyber security strategy development is translated to:

Accepted direction - Relevant elements - Sufficient effect-ambitions.

Breaking apart, operationalizing, the key capability areas into more detailed lists of specific factors and keeping in mind the desired levels of ambitions, a comprehensive view of potential directions and alternative activities can be outlined. The intention of this empirical accounting and typology is not to offer any exhaustive to-do list, but to provide an encompassing overview of the alternative ambitions and action. Contextualizing and grouping the detected elements, factors and criteria, as optional lines of policy/strategy direction constitutes, the crucial and unique element of the ICT4P approach. Without direction any action would be blind.

Strategic capacity

The ICT4Peace Foundation approach enables nations to identify needs and capabilities, threats and risks as well as areas of potential domestic and cross-border cooperation. The approach supports experts, policy planners and decision-makers in understanding and explaining the field and its respective ambitions, opportunities, requirements and consequences in a broader governmental, national and international context. By doing this the ICT4P approach promotes interagency/cross-disciplinary dialogue and attention to the interrelationship of priorities, ambitions and resources. Most importantly such horizontal and vertical dialogue helps to grasp and consider 2nd and 3rd order consequences and requirements that otherwise could be missing in action; these may include legal and resource requirements, interagency coordination, international normative restrictions and cooperative opportunities. This also enables to conduct more fruitful discussion with private sector and civil society as governments are empowered to communicate their visions and cyber security profiles. Such societal actors can support the government to identify 2nd and

[365] Ibid, p. 9.

3rd order consequences, for example industrial and business opportunities as well as private or corporate issues of concern.

Building durable cyber capacity takes time. The foundations of human skills and competences are created at basic and advanced education; some basic capabilities can be purchased. It is advisable for governments to ask for external, domestic or international support. To effectively enhance visionary, political and strategic capacity, yet requires rather than indexing or ranking countries long-term and progressive engagement between national authorities and their advisors and potential sponsors.

Initial steps of such engagement should include strategy-formulation and issue-specific courses for national authorities: legislators, diplomats, administrators and regulators as well as intelligence, law enforcement and military officers. The most generic of courses and workshop dealing with strategy alternatives and requirements, the nexus of ICTs and development as well as respective administrative, technical and financial methodologies can be, if needed, organized regionally. Such preparatory engagements also teach which policy directions are acceptable. In addition to general knowledge, specific skills and competences on targeted and tailored courses and workshops can be built. If desired national sessions and consultations can follow to e.g. discuss and develop policy options, alternative strategies and draft legislation or to conduct table top exercises. Many nations would appreciate assistance in developing national cyber security strategy, countering cyber crime and terrorism and protecting critical infrastructure.

It is essential to emphasize national responsibility and domestic considerations over theoretical knowledge. The more detailed the process becomes, the more necessary it is to bring on-board subject-matter experts. However, the national authorities in question and the external experts ought to maintain strategic mindset and the desired ambitions and directions.

Reliable and valid policy analysis and assessment

National policies and strategies need to be assessed. Assessing cyber security strategy is by default policy analysis where its distinct methodologies can be employed. A proper assessment able to support and develop organizational or national programs entails analysis of not only the content and direction or implementation of governmental policies and programmes, but in particular the impact of these policies that is the achieved level and status of actual ICT developmental prowess and cyber security. Conceptual and

methodological support for such analysis can be found, for example, in health, education, and energy sectors.[366]

The analysis feeding forward into the strategy process, both reviewing mechanisms and the implementation (of action plans), strengthens national ownership and responsibility, the primacy of national decision-making. Thorough policy analysis also helps to satisfy the supervision criteria national parliaments and international financing institutes have on governmental policies and programs.

CONCLUSION

Technological development and dependency are not slowing down. The benefits of 5G networks, artificial intelligence, nanotechnology or quantum computing will not be automatically employed or equally distributed. The functionality and stability of national ICT environments and infrastructure is a question of technical and political security but increasingly an essential element and dimension of development. Ineffective and unstable cyber infrastructure leads to the inefficient use of national resources and discourages international investments and other positive engagements.[367] Security first advocates to find it hard to approve the acceptance of some risks and threats, an inevitable condition of strategy-making. Furthermore, security-heavy cyber and information security strategies being incompatible to anticipate and deal with the upgrades of services, software and infrastructure as well as emerging threats soon become obsolete. The instability and the economic and societal progressive technological development is projecting the need to be constructively balanced to create of the desired and necessary national and international effects.

National cyber security strategies are building blocks for international peace and security. Strategies allow countries to address issues of perceived insecurity and promote issues of stability. Of the latter, national commitment to confidence building measures are of particular and practical importance. Strategies being politically approved, documents can mandate and task agencies and organizations to implement, for example transparency measures, participate in regional cooperative initiatives, and exercise restraint in their otherwise more offensive activities. Similarly, strategies can communicate government ambitions to develop international regulatory instruments for the cause of peaceful use of

---

[366] Cyber affairs in general are plagued by ill-researched and uncritical literature of cyber pulp fiction and politically, commercially motivated agitation and even undergraduate papers. ICTs as tools of peace and development deserve more serious and professional attention.

[367] International Institute for Strategic Studies, *The Evolution of Cyber Domain* (Ed. Eneken Tikk-Ringas), (London: IISS, 2015).

ICTs and cyberspace. In fact issuing cyber or information strategies can be regarded as a norm: expected and constructive conduct by a government that takes an active stand on the nations future and development and for the stability of international relations. The proliferation of national strategies is not inflating or inflammatory but progressive behavior, a sign of emerging global cyber culture.

In conclusion, some models take that no country is cyber ready, undermines the international capacity building agenda by logically suggesting that even those who seek to teach other how to do it may not be up to the task. This, in turn, can be used by opponents of ICT proliferation to resist promoting of freedom of information and pluralist information society. On the other hand, all indexes assume that 'more' is better, setting ICT penetration, information society and other maximalist criteria as the ultimate goals of development. Doing so, they miss potential target countries with lesser ambitions, or, more importantly, countries that are not yet convinced of benefits brought by ICTs. As a result, the existing indexes and rankings fail to point the targets as well as priority areas of engagement when it comes to national strategy development assistance. By focusing security as a goal indexes miss out on important developmental aspirations, which are more likely to indicate opportunities of exporting the values and experience of their political patrons.

Consequently, relying or directly linking the international cyber policy and national strategy development initiatives on the existing indexes and rankings is not recommended. Existing rankings and indexes can be used as part of country assessments-provided that they enhance or deepen the questions or inquiries that are needed to facilitate national strategy development from the strategic point-of-departure. Indexes and rankings can also serve as basis of training and education programs to open relevant themes for discussion and hopefully critical self-assessments.

States' approaches to cyber affairs are shaped by their distinct national and political culture, particularly in the development, use and oversight of ICT capabilities. Capacities of nations to grasp 'cyber' differ. Countries, although facing similar-appearing problems and utilizing same foundational technologies, have very different political, operational, financial and cultural premises to build to and from. Strategic thinking can arguably be regarded universal and even ahistorical, but strategies cannot be not pre-ordered, exported or imported. A more ambitious and advanced strategy would not function in an operating environment where baseline technical and administrative requirements are not met. Accepting the claim of one index that no country is cyber ready, undermines also the potential of capacity-building as no one logically would be competent to offer appropriate guidance. A heuristic and strategically attuned engagement can support governments to design national vision, provide political direction and develop sustainable long-term policies, strategies and action plans. Without vision national cyber security strategies can be rich in detail but yet remain misdirected.

Annex to the Policy Paper "National Cyber Security Strategies: Commitment for Development"

Summary of selected frameworks for and assessment models of national cyber security strategies

	OBJECTIVES	TYPOLOGY[368]	METHODS	MEASUREMENTS
ITU	Providing the right motivation to countries intensify their efforts in cyber security; help foster a global culture of cyber security and its integration at the core of information and communication technologies.	Legal; Organizational; Capacity-building; Technical		Index (0.000 – 1.000); Global and regional ranking
CTO	Serve as a guide for countries to develop their individual national cyber security strategies. The guide provides practical advice and proposes actions that can be adapted by countries to suit their individual circumstances; indicate where a country lacks intrinsic capacity in aspects of cyber security and potentially needed to reduce risks to national goals or to create opportunities for the country.	Strategy [document] components of: Introduction; Guiding principles; Strategic goals and vision; Objectives and priorities; Stakeholders; Governance and management structure; Implementation (covering Legal and regulatory framework; Awareness; Local technical capability; Incident response); Monitoring and evaluation	Forwarding, monitoring and evaluation method: Key Performance Indicators by which progress will be measured based on reporting required from stakeholders, collating the data to achieve transparency in reporting progress against the strategy's objectives either as measurements of about delivery activity or measure the outcome or end state by posing questions to those stakeholders who are intended to benefit.	n/a
ENISA	Perform a stocktaking exercise on the approaches currently used to perform evaluation of national cyber security strategies; present recommendations and identify good practices on the implementation and evaluation of cyber strategies; design and develop an evaluation framework to adapt to the varying needs of countries at different levels of maturity in their strategic planning.	Cyber defence policies and capabilities; Cyber resilience; Counter-cybercrime; Cyber security support to industry; Critical information infrastructures protection.	Literary review; Documentation review of national cyber security strategies; Logic modeling where Key Performance Indicators illustrating the underlying logic of recurring components of cyber security strategies are mapped to the objectives of the evaluation model.	n/a

[368] *Inter alia* notions such as dimensions, components, elements, key performance indicators, or topics. Eric Luiijf and Jason Healey identify "the five mandates of national cyber security" as military cyber operations, counter cyber, intelligence/counter-intelligence, cyber security crisis management and critical infrastructure protection and CIP, and internet governance and cyber diplomacy. The authors notice the "optimal, clean sheet positioning of the cyber security functions" as "a theoretical best practice." (Luiijf & Healey, "Organizational structures and considerations" in Klimburg (ed.), *National Cyber Strategy Framework Manual*, p. 120-128.)

CMM	Increase the scale and effectiveness of cyber security capacity building, both within the UK and internationally"; making this knowledge available to governments, communities and organisations to strengthen their cyber capacity.	Cyber policy and strategy; Cyber culture; Workforce and leadership; Legal and regulatory framework; Risk management thorough organization, standards and technology.	Structured 3-5 day workshops and self-assessment focusing on the five dimension and their sub-dimensions, factors and categories. A report with recommendations for courses of action.	Start-up; Formative; Established; Strategic; Dynamic.
CRI	Inform national leaders on the steps they should consider to protect their increasingly connected countries and potential GDP growth by objectively evaluating each country's maturity and commitment to cyber security and resilience.	National strategy; Incident response; E-crime and law enforcement; Information sharing; Investment in research and development; Diplomacy and trade; Defense and crisis response	Evaluating each country's maturity and commitment to cyber security and resilience with a focus on economic growth; Defining what it means for a country to be "cyber ready" and document the core components of cyber readiness into an actionable blueprint for countries to follow. The fact-based assessments for each country rely on primary sources, and each unique data point is grounded on empirical research and documentation.	Insufficient evidence; partially operational; fully operational.
ASPI	Make considered, evidence-based cyber policy assessments; identify opportunities for the sharing of best practice, capacity building and development, plus commercial opportunities. With this additional layer of analysis, governments and the private sector can tailor engagement strategies to best fit existing levels of maturity in each policy area in each country.	Governance; Financial cybercrime enforcement; Military application; Digital economy and business; Social engagement	Weighed indicators, the importance ratings, and averaged weighting factors that are used in the calculation of an overall score. Each country is rated against the 10 factors. The overall score is the sum of the scores against each factor weighted by the average importance. The overall scores are converted to a percentage of the highest possible score [100].	Weighed score (0.0-100) Engagement opportunities indicators

Sources:

- The International Telecommunication Union *Global Cybersecurity Index and Cyber wellness Profile* (https://www.itu.int/pub/D-STR-SECU-2015);
- The Commonwealth Telecommunication Organization *Commonwealth Approach for Developing National Cybersecurity Strategies* (2015) (http://www.cto.int/media/foth/cybsec/Commonwealth%20Approach%20for%20National%20Cybersecurity%20Strategies.pdf);
- European Union Agency for Network and Information Security, *An evaluation framework for cyber security strategies*

(https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1);

- University of Oxford, *Cyber Security Capability Maturity Model*, v. 1.2 (15 December 2014);
- Melissa Hathaway, *Cyber Readiness Index 2.0*. Potomac Institute for Policy Studies (November 2015), see also Hathaway, *Cyber Readiness Index 1.0*. Hathaway Global Strategies LLC (November 2013);
- Australian Strategic Policy Institute International Cyber Policy Centre (ASPI), *Cyber Maturity in Asia-Pacific Region 2015*, https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2015/Cyber-Maturity-2015.pdf.

DRAFT – shared with the participants of the ICT4Peace Workshop on

Existing and future norms on international ICT infrastructure and data integrity

STATEMENT BY H.E. MARINA KALJURAND FOREIGN MINISTER OF ESTONIA AT THE CONFERENCE ON STATE PRACTICE AND DEVELOPMENT OF INTERNATIONAL LAW

Dear Friends and Colleagues,

I cannot tell you how much I appreciate you gathering here in Tallinn today. I know that many of you have participated in several events on the issue of norms, rules and principles for the responsible behaviour of State in cyberspace during the past months. I also hope that the following two days will allow lively and prolific exchanges of views in an open, inclusive and forward-looking way.

As a lawyer and a diplomat, I appreciate the interplay of law and politics in the dialogue of international cybersecurity. I have personal experience of complicated diplomatic efforts to mitigate cyberattacks against my country. Today, my Ministry is in charge of developing Estonian views on international law as it applies to the behaviour of State in cyberspace.

Estonia has been a member of three consecutive UN Groups of Governmental Experts (UN GGE) in the United Nations First Committee.

The upcoming GGE is faced with the expectation of taking us beyond already agreed positions. Whether or not each of us will be part of the next GGE, it is our privilege and duty to inform of those discussions and to support an outcome that respects and responds to our common concern.

International law is highly relevant for Estonia. Therefore, we strive for clarity and certainty of norms, it not only reduces the risk of intolerable practices, but also provides transparency and predictability of behavior that allows us to focus on peace rather than on conflict.

I want to take this opportunity to elaborate on the question of peace and conflict. Seen through the Estonian lens, while we have witnessed the disruptiveness of malicious cyber activities, our focus has always been on using ICTs in support of State and societal functions; peace, growth and prosperity. We have never invested overly into military cyber capability development, although we have taken the question of cyber defence very seriously. We have

promoted an atmosphere of trust and cooperation between government and industry, including critical infrastructure providers. We have always taken into account the preferences and requests of the community of users. For Estonia ICTs are technologies of peace and development, not of conflict. I am sure this is the case for the majority of countries in the world.

However, I can understand how these technologies can be seen as a potential source of conflict by some of us. We have heard of development of offensive military cyber capabilities and doctrines. We can see the growing statistics of cybercrime, economic espionage and other malicious uses of ICTs. Estimates of cyber crime diminishing GDP vary between 0.1 and 1.6 per cent, thus depriving us from the full benefits that ICTs can offer. Terrorists exploit ICTs and social media deliver their sermon full of hatred, violence and intolerance, to recruit followers and lead their mislead troops.

It is essential to acknowledge that we perceive cyber threats and opportunities differently. Regardless of how clearly we can see and understand perspectives of each other, it is essential that we remain mindful of the views of each other. This open and permissive attitude allows us to achieve stability and security, while taking full advantage of technological development and advances.

Therefore, it is essential that we need to go further than we already have.

We need to broaden our understanding of international law. We have concluded that international law, in particular the UN Charter, is applicable to international cyber security. There are other international legally binding instruments that are applicable. We need to identify and register these instruments.

I have noted that for some commentators the applicability of international humanitarian law is not settled. Let me share the Estonian position on that. While we acknowledge, and in fact hope, that cyber hostilities will never mount to the levels of use of force or armed attack, we also consider it very essential that it should not ever happen, protections of international humanitarian law are to be afforded to their fullest. Once we have affirmed these guarantees AND clearly condemned any threat to peace and security in cyberspace, we can start working on details that, no doubt, need to be clarified with the view to application of particular norms.

We need to broaden our discussion on how international law applies to State activities in cyberspace. In this regard we have witnessed both uncertainty and differences. In the absence of easily observable State practice, and given the challenges of attribution, we must make extra efforts to apply the concepts and principles of sovereignty, non-intervention and state responsibility to activities in the cyber domain. And we need to be mindful of our different interpretations of some of these concepts, both due to our different traditions of

international law, but also due to the fact that we are only starting to apply the well-established legal norms and principles to a new reality – cyberspace.

Almost over two decades that the UN First Committee has dealt with the issue of international cyber security, individual States have grown their expertise and experience in addressing these fundamental questions and specific threats. **We need to look at what States actually do when facing cyber threats**, because their actions speak of proposed standards of responsible behavior. We need to carefully look at all the proposals, verbal and material, that States are making about how to deal with these threats.

In this regard, I also want to emphasize how important it is that we have different experiences. Our differences inform the margins of actions that each of us, or all of us together, can take in case of an incident.

But we should not stop at that – while we have clearly condemned any malicious and hostile acts in cyberspace and focused on the remedies that international law offers in case of breaches, **we need to start preventing incidents from happening and escalating**.

Here, it is important to find the incentives and common interests of all stakeholders, including governments, industry and the civil society.

It is equally important to acknowledge that international law is not the only regime that we need to adjust to our needs. When it comes to prevention, it is essential to create national policies, procedures and standards that support cooperation and exchange of information.

This is why this conference looks at the future of international law in a broader sense, by not only looking at international law. As the GGE has structured the conversation, when discussing how international law applies, we also identify potential gaps and inconsistencies that merit new norms, rules and principles. State behavior is equally conditioned by legally non-binding norms. The GGE could be further informed by practices and norms that both States and industry have come to follow in their activities in cyberspace.

I would therefore propose a few additional approaches that the international community could consider.

States have the responsibility to lead a global culture of cybersecurity. The GGE has made reference to expectations that governments have towards industry and critical infrastructure operators. It is now essential to **hear how governments should lead.** Few corporate actors have tabled their views on this. In my point of view, we need to listen more. I would therefore invite the industry to consolidate and share their views on norms, rules and principles of responsible State behavior, as well as the application of international law.

I also invite different schools of international law and international relations to discuss the urgent and practical issues of international cyber security and help us chart the political-normative surface that we need to operate on. Let us not just suggest, but demonstrate that

international law is alive, is relevant, and is useful. Let us demonstrate that we can use some of its core principles, such as good faith, and our pledge to remain bound by treaties, to modernize it to the age of smart and connected technologies.

My last point is something I hope you all consider when thinking and making decisions about international cyber security and international law. I would like to introduce you to a scholar of Estonian origin who spent most of his career at the service of the Russian empire at the end of the 19th century.

Professor **Friedrich Frommhold Martens**, a distinguished legal scholar and an assigned diplomat to the Hague Peace Conference, helped governments overcome a similar legal puzzle we are facing today. He suggested that while norms on (at that time) land warfare are still to be clarified by high contracting parties, states should afford maximum protections to anyone under the rule of law. The Martens Clause reads as follows:

> *Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity, and the requirements of the public conscience.*[369]

I very much hope that in our thinking and discussion of the future of international law, we follow the example and spirit of Professor Martens and that we build the future of international law by not changing the law, but changing our thinking and behavior to support the existing legal order to the fullest.

[369]Preamble, Convention No. II with Respect to the Laws and Customs of War on Land, with annex of Regulations, 29 July 1899, 32 Stat. 1803, 1 Bevans. 247