UNIVERSITY OF TARTU

SCHOOL OF LAW

Department of public law

Liisi Adamson

SOVEREIGNTY IN CYBERSPACE: ORGANISED HYPOCRISY?

Master's Thesis

Supervisor

Prof. Lauri Mälksoo

Tartu

2016

Table of Contents

List of abbreviations

ASEAN	Association of Southeast Asian Nations
CNA	Computer Network Attack
CNE	Computer Network Exploitation
CUP	Cambridge University Press
DDoS	Distributed Denial-of-Service Attack
DoD	Department of Defence
DoS	Denial of Service Attack
FBI	Federal Bureau of Investigation
IISS	International Institute for Strategic Studies
ICJ	International Court of Justice
ICJ Statute	Statute of the International Court of Justice
ICT	Information and communication technology
IEC	International Electrotechnical Commission
ILC	International Law Commission
ISO	International Organization for Standardization
IT	Information Technology
KGB	Committee for State Security (in Russian *Komitet gosudarstvennoy bezopasnosti*)
LOAC	Law of Armed Conflict
NIST	National Institute of Standards and Technology
OAS	Organization of American States
OUP	Oxford University Press
PCA	Permanent Court of Arbitration
PCIJ	Permanent Court of International Justice
Saudi Aramco	Saudi Arabian Oil Company
SCO	Shanghai Cooperation Organisation
UN	United Nations
UN GGE	United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
UNGA	United Nations General Assembly
UNSC	United Nations Security Council

Introduction

The fast development of computers and communication networks[1] as well as the beginning of the so-called Information Age[2] has caused a reliance on information and communication technologies in an exponentially increasing number of States.[3] Networked systems and fast developing technology are now considered not only characteristics of the modern society but also important aspects of national security.[4] Correspondingly, it has been claimed that "[l]ongstanding notions of sovereignty fall apart when it comes to cyber operations."[5]

Increased dependency on information and communication technologies (hereinafter ICT) and inherently dual-use networks[6] offer hostile actors the opportunity to exploit the advantages that cyberspace offers, irrespective of the aim of the exploitation, e.g. achieving financial gain or military advantage, gathering information or influencing State behaviour.[7] As a result, interconnected and interdependent information infrastructure and architecture represent new strategic targets[8] as well as mediums through which offensive operations can be conducted.[9] Thus, during the last decade "cyber" has become one of the most frequently used prefixes in the international security discourse.[10]

As expected, a broad academic and political discussion has followed the evolution of cyber domain, gearing into full force after the cyber attacks in Estonia in 2007. Especially after the

---

[1] The rapid development started from the 1960s. See International Institute for Strategic Studies. Strategic Dossier. The Evolution of the Cyber Domain: the Implications for National and Global Security. Abington: Routledge 2015, p 7 ff.

[2] The term was used by Alvin Toffler to describe the "Third Wave" society, which represented the transition of the developed States' societies from Industrial Age to Information Age. A. Toffler. The Third Wave. New York: Bantam books 1981.

[3] "The information age society is highly dependent on computer and internet connections to accomplish tasks both mundane and critical." V.M. Antolin-Jenkins. Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places? – Naval Law Review 2005, Vol. 51, p 132.

[4] K. Geers. Pandemonium: Nation States, National Security, and the Internet. – L. Vihul (ed.). The Tallinn Papers: Numbers 1-9 (2014-2015). Tallinn: NATO CCD COE Publications 2015, p 1.

[5] D. Perera. Schmidle: Cyber Ops Might Require New Combatant Command Structure. – FierceGovernmentIT, 15.05.2011, www.fiercegovernmentit.com/story/schmidle-cyber-ops-might-require-new-combatant-command-structure/2011-05-15 (visited 15.04.2016).

[6] Dual use indicates that networks are being used for military as well as civilian purposes.

[7] Among others, C. C. Joyner and C. Lotrionte note that, "the technology-intensive Information Age brings with it the opportunities for 'cyber-crime', 'cyber-war' or, as more aptly put, the prosecution of 'Information Warfare'". C.C. Joyner, C. Lotrionte. Information Warfare as International Coercion: Elements of a Legal Framework. – European Journal of International Law 2001, Vol. 12, p 826. See also R. Buchan. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? – Journal of Conflict & Security Law 2012, Vol. 17, No. 2, p 211. P.W. Franzese. Sovereignty in Cyberspace: Can it Exist? – Air Force Law Review 2009, Vol. 64, pp 2–3.

[8] R.A. Miller, D.T. Kuehl. Cyberspace and the "First Battle" in 21st-century War. – Defense Horizons 2009, Vol. 68, p 2.

[9] M. Roscini. Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press (hereinafter OUP) 2014, p 12. R. Geiss, H. Lahmann. Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space – Israeli Law Review 2012, Vol. 45, p 384.

[10] M.E. O'Connell. Cyber Security Without Cyber War. – Journal of Conflict & Security Law 2012, Vol. 17, No. 2, p 187.

2010 Stuxnet attack in Iran, the feared hostility of cyber operations and their possible destructive effects shifted the focus of the discourse rapidly to hypothetical cyber operations with so severe consequences as to fulfil the criteria of the use of force under United Nations (hereinafter UN) Charter[11] Article 2(4) or even of an armed attack. Even though no known cyber operation thus far has crossed the threshold of an armed attack,[12] alarming statements have been made[13] and publications written[14] about cyber war looming in our future as well as destructive cyberwarfare capabilities being developed by States, which would eventually lead to a cyber "Pearl Harbor".[15] Thus, resulting in most of the discourse revolving around the application of the law of the armed conflict (hereinafter LOAC), law of the use of force and the law of self-defence as reflected in UN Charter Article 51.[16]

---

[11] Charter of the United Nations. 26 June 1945. – www.un.org/en/charter-united-nations/ (visited 15.04.2016).

[12] M.N. Schmitt (ed.). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press (hereinafter CUP) 2013, p 57.

[13] The US General Keith B. Alexander has stated, "Catastrophic cyberattacks loom in the nation's future." Similarly, an open letter to George W. Bush warned already in 2002 the world of a cyber attack that would "devastate the national psyche and economy more broadly than did the 9/11 attacks". General Keith B. Alexander's keynote address to senior government security officials and industry executives attending a cybersecurity conference. – 30.10.2013, archive.defense.gov/news/newsarticle.aspx?id=121030 (visited 25 March 2016); Various authors. Open Letter to President George W. Bush. – 2002, www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/letter.html (visited 20.03.2016).

[14] For works of proponents of cyberwar see for example, R.A. Clarke, R.K. Knake. Cyber War: The Next Threat to National Security and What to Do About It. New York: HarperCollins Publishers 2010; J.P. Farwell, R. Rohozinski. Stuxnet and the Future of Cyber War. – Survival 2011, Vol. 53; R. Buchan, N. Tsagourias. Cyber War and International Law. – Journal of Conflict & Security Law 2012, Vol. 17, No. 2; Y. Dinstein. The Principle of Distinction and Cyber War in International Armed Conflict. – Journal of Conflict & Security Law 2012, Vol. 17, No. 2; J. Stone. Cyber War Will Take Place! – Journal of Strategic Studies 2013, Vol. 36, No. 1; G. McGraw. Cyber war is Inevitable (Unless We Build Security In). – Journal of Strategic Studies 2013, Vol. 36, No. 1; P.W. Singer, A. Friedman. Cybersecurity and Cyberwar. Oxford: OUP 2014; J.D. Ohlin, K. Govern, C. Finkelstein (eds.). Cyber War: Law and Ethics for Virtual Conflicts. Oxford: OUP 2015. For the opposing opinion see T. Rid. Cyber War Will Not Take Place. Oxford: OUP 2013; J. A. Lewis. The Cyber War Has Not Begun. – Center for Strategic and International Studies 2010.

[15] Leon E. Panetta stated that "[t]he collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life". L.E. Panetta. Remarks by Secretary Panetta on Cybersecurity to the Business Execturives for National Security. – 11.10.2013, www.cfr.org/cybersecurity/secretary-panettas-speech-cybersecurity/p29262 (visited 01.04.2016).

[16] Some consider the Tallinn Manual as the epitome of the discourse on the application of LOAC. M.N. Schmitt, Tallinn Manual. Cf. M. Roscini. Referenced work; T.A. Morth. Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter. – Case Western Reserve Journal of International Law 1998, Vol. 10; Y. Dinstein. Computer Network Attacks and Self-Defense. – International Law Studies 2001, Vol. 76; E.T. Jensen. Computer Attacks on Critical National Infrastructure: A Use of Force Revoking the Right to Self-Defense. – Stanford Journal of International Law 2002, Vol. 38; E. Kodar. Computer Network Attacks in the Grey Areas of Jus ad Bellum and Jus in Bello. – Baltic Yearbook of International Law 2009, Vol. 9; M. Hoisington. Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense. – Boston College International and Comparative Law Review 2009, Vol 32, No. 2; P. Palojärvi. A Battle of Bits and Bytes: Computer Network Attacks and the Law of Armed Conflict. Helsinki: Publications of the Erik Castrén Institute of International Law and Human Rights, University of Helsinki 2009; M.C. Waxman. Cyber Attacks and the Use of Force: Back to the Future of Article 2(4). – Yale Journal of International Law 2011, Vol. 36; N. Tsagourias. Cyber Attacks, Self-Defence and the Problem of Attribution. – Journal of Conflict & Security Law 2012, Vol. 17. No. 2; S.J. Shackelford. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. – Berkley Journal of International Law 2013, Vol. 27, No. 1.

Undoubtedly, the debate around the application of LOAC is of great importance in the context of cyber operations with debilitating and destructive consequences. Whilst they could be feasible, the realisation of such cataclysms in the current state of affairs seems unlikely.[17] The reality is that even though the empirical trend shows a steady rise in the amount of cyber operations over the past dozen years,[18] all of those operations can be considered low-intensity, meaning that they do not manifest in physical damage and are thus not captured by Article 2(4) of the UN Charter or the damage caused by the operation can be considered insignificant.[19] This will most likely be also the trend in the future. As such, the focus of the discourse has been, if not displaced then skipping certain fundamental topics for the past decade. Operations that do not cross the threshold of use of force still affect State sovereignty. Moreover, besides the question of offensive cyber operations, the fundamental characterisation of sovereignty in mostly intangible cyberspace requires attention, which it has not received thus far.

Therefore, understanding the concept of sovereignty and the exercise thereof by States is in the current state of affairs of outmost importance. By asking "wrong" questions about cyberspace,[20] States and academics alike are going around in circles, failing to consider the wider implications of cyber operations and cyberspace itself to international law. During the Cold War the space race was largely conducted between two States – the USA and the Soviet Union. These States were also the biggest actors deciding over the framework regulating the use of such technology. However, when it comes to "cyber-race", the circle of decision-makers with different interests in mind is continually increasing. Whilst there is a rich literature covering the application of LOAC to cyber operations, such interpretations are grounded in the hypotheticals that they have been built on. Whereas the basic questions concerning the foundation of international law have been left aside, pulling thus away from the reality that States' are facing: breaches of sovereignty through low-intensity cyber operations in an organised hypocrisy. The latter phrase has been borrowed from Stephen D. Krasner, who in his book Sovereignty: Organized Hypocrisy contends that States as

[17] S. Watts. Low-Intensity Cyber Operations and the Principle of Non-Intervention. – J.D. Ohlin, K. Govern, C. Finkelstein (eds.). Cyber War: Law and Ethics for Virtual Conflicts. Oxford: OUP 2015, p 250.
[18] T. Rid. Cyber War Will Not Take Place. – Journal of Strategic Studies 2013, Vol. 35, No. 1, p 15.
[19] Even though some scholars consider the Stuxnet cyber attack in Iran in 2010 as crossing the threshold of at least use of force, this thesis makes the claim that even in the case of Stuxnet, the damage can be considered insignificant, therefore, not crossing the threshold of Article 2(4) of the UN Charter. Yet, the Stuxnet attack can still be interpreted as coercive in the meaning of the non-intervention principle.
[20] G.D. Brown. The Wrong Questions About Cyberspace. – Military Law Review 2014, Vol. 217, p 214.

sovereigns often violate long-standing norms, if it benefits them or is otherwise important in order to achieve their aspirations and goals.[21]

This thesis focuses on the (un)changed concept of sovereignty and exercise thereof vis-à-vis cyberspace, exploring the "organised hypocrisy" that surrounds the regulation of offensive cyber operations, corresponding State practice and relevant international law. Thus, the main research questions of the present work are: *How does sovereignty apply and how do States assert and exercise their sovereign rights in cyberspace?*

The hypotheses of the thesis are two-fold: firstly, the concept of sovereignty remains to a large extent unchanged in relation to cyberspace. States exercise sovereignty differently in different spheres,[22] however, the concept of sovereignty remains the cornerstone of the international legal system. Besides territorial sovereignty, normative decisions made on the international plane reflect exercises of State sovereignty regarding to the development and interpretation of existing international law in the context of cyberspace. Secondly, States make the conscious decision of non-compliance with international law when it comes to low-intensity cyber operations, using operations that are effective, below the threshold of Article 2(4) of the UN Charter to further their own strategic goals. Cyberspace allows States to use the anonymity and ambiguity offered by low-intensity cyber operations to further their strategic ambition and at the same time avoid responsibility under international law.

Thus, the aim of the thesis is not to give a comprehensive overview of the concept and history of sovereignty, as that would be outside of the scope and ambition of the thesis. Plenty of authors have offered an excellent contribution as to that regard.[23] Instead, the thesis aims to construe its case about sovereignty narrowly in the confines of the central topics of cybersecurity and cyberspace and thereby offer a novel view on how States exercise sovereignty in cyberspace. The thesis uses mainly comparative and historical methods. In order to do so, the thesis looks at relevant international treaties, case law, State practice and academic works pertaining to the concept of sovereignty and exercise thereof.

The fundamental question in any discourse regarding cyber operations has been how to apply *lex lata* to "new" circumstances, yet stay "faithful to enduring principles, while accounting for

---

[21] S.D. Krasner. Sovereignty: Organized Hypocrisy.
[22] ICJ. 09.04.1949. Corfu Channel Case (*United Kingdom of Great Britain and Northern Ireland v. Albania)*. ICJ Reports 1949. Separate opinion of Judge Alvarez, p 43.
[23] See for example, N.G. Onuf. Sovereignty: Outline of a Conceptual History. – Alternatives: Global, Local, Political Fall 1991, Vol. 16, No. 4; M.P. Ferreira-Snyman. The Evolution of State Sovereignty: A Historical Overview. – 2006, uir.unisa.ac.za/bitstream/handle/10500/3689/Fundamina%20Snyman.finaal.pdf?sequence=1 (visited 15.04.2016).

changing times and technologies?"[24] International law, which usually is more than a few steps behind the development of technology, has found itself struggling during the past decade to provide affirmative interpretations of existing rules applicable to cyber operations or cyberspace in general. For quite some time, cyberspace and actions conducted therein were considered as the "Wild West": no State would be able to exercise territorial control and no laws would apply.[25] The metaphor of a "Wild West" lost its ground when the 2013 United Nations Group of Governmental Experts (hereinafter UN GGE) Report affirmed the applicability of international law to cyber security.[26] Yet doubts about the sufficiency of the current international law regulation to provide an effective legal framework for cyber operations have remained.

It must be kept in mind that it is not the first time that technology has taken a significant leap forward and international law has been tasked with dealing with the accompanying changes. New technologies raise new issues,[27] but core questions, such as sovereignty, remain the same and therefore, the existing international law should provide a solution or an interpretation for new technologies also in the future.

The literature on the applicability of international law to cyber operations continues to proliferate at a fast pace. However, there is surprisingly little literature dedicated to the question of exercises of sovereignty in a cyber-specific context. Most of the existing literature ponders about the application of sovereignty *in abstracto* to cyberspace, i.e. whether it applies at all. Thus, the existing literature does not answer the research question *per se*, allowing the present thesis to contribute to the existing discourse by exploring the theoretical framework and exercises of sovereignty within existing State practice. By inquiring into the exercise of sovereignty *in concreto*, the thesis takes a rather practical approach by incorporating as much State practice as appropriate to illustrate the issue.

---

[24] H.H. Koh. International Law in Cyberspace. – Harvard International Law Journal 2012, Vol. 54, p 2.
[25] For examples of academic discussion surrounding the Wild West metaphor, see, L.J. Gibbons. No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace. – Cornell Journal of Law and Public Policy 1997, Vol. 6, No. 3; R. Ku. Foreword: A Brave New Cyberworld? – Thomas Jefferson Law Review 2000, Vol. 22, pp 125-126; S. Shipchandler. Note, The Wild Wild Web: Nonregulation as the Answer to the Regulatory Question. – Cornell International Law Journal 2000, Vol. 33; D. Yan. Virtual Reality: Can We ride Trademark Law to Surf Cyberspace? – Fordham Intellectual Property, Media & Entertainment Law Journal 2000, Vol. 10; S. Biegel. Beyond our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace. Cambridge: MIT Press 2001, pp 13–18.
[26] UNGA. A/68/98. 24.06.2013. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by Secretary-General, para 19.
[27] H.H. Koh. Referenced work, p 3.

One of the main characteristics of many cyber-related scholarly works is the inquiry into what law *ought* to be in order to address the challenges of cyberspace wholly and efficiently.[28] The present thesis will focus on *lex lata*, i.e. what the law *is*, not what it *ought* to be.[29] It is not the task of this thesis to fill in the gaps in the existing regulation; however, they will be brought into the reader's attention through the discussion on whether the existing framework that is being applies is adequate or antiquated. As the state practice surrounding the questions of sovereignty and intervention as well as cyber operations is far from settled, it is better to leave the "question open than to answer it incorrectly".[30]

Since the literature surrounding cyber operations is fairly extensive and rich there are some delimitations that must be set in order to focus the present work properly. Firstly, the question of sovereignty operates exclusively with respect to States. Thus, even though non-State actors play a significant role in the cyber discourse, the present thesis will focus on State-on-State interactions, taking into account only State activities in cyberspace. Secondly, as pertaining to State practice, cyber operations can take several forms depending on their characterisation but for the purpose of this thesis, cyber operations are understood as entailing either cyber attacks or cyber operations, which can involve exploitations. Since cyber incidents mostly do not have intent to harm and are considered accidental, they cannot be considered to have a coercive nature. On the other hand, extensive cyber campaigns, even though feasible in the future, are not likely to realise in the nearest future. Thirdly, only cyber operations that fall below the threshold of use of force according to Article 2(4) of the UN Charter will be discussed. Thus, the thesis limits itself to peacetime operations and conflict situations as such will be excluded from the scope. Last, but not least, the present thesis will not dive into the problem of attribution. The problematic and difficulties of attribution are well documented and need only a brief comment in the thesis.[31] The thesis lies on the premise that all cyber operations discussed in the thesis are considered State-organised or at least State-sponsored.

---

[28] See C.C. Joyner, C. Lotrionte. Referenced work. D. Brown. A Proposal for an International Convention; S.J. Shackelford. From Nuclear War to Net War; J. Barkham. Information Warfare and International Law on the Use of Force. – NYU Journal of International Law and Policy 2001, Vol. 34, No. 56, p 57.

[29] John Austin has stated "The existence of a law is one thing: its merits or demerits are another. Whether law *be*, is one inquiry: whether it *ought* to be, or whether it agree with a given or assumed test, is another and a distinct inquiry." J. Austin. The Province of Jurisprudence Determined. London: John Murray 1832, p 278.

[30] L. Oppenheim. The Science of International Law: Its Task and Method. – The American Journal of International Law 1908, Vol. 2, No. 2, p 318, p 335.

[31] See, D.B. Hollis. An e-SOS for Cyberspace. – Harvard International Law Journal 2011, Vol. 52, pp 397–401. E.M. Mudrinich. Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem. – Air Force Law Review 2012, Vol. 68; M.N. Schmitt. "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law. – Virginia Journal of International Law 2014, Vol. 54; E.T. Jensen. Cyber Sovereignty: The Way Ahead. – Texas International Law Journal 2015, Vol. 50, No. 2, p 277.

Admittedly, none of the target States has been able to fully attribute the attacks on a particular States. There are suspects in each case, but full attribution has not been achieved. Yet, if the thesis would not accept as a premise that the operations were indeed State offensive activities, due to the fact that they were never fully attributed, discussing breaches of sovereignty and the application of the non-intervention framework would be increasingly difficult. Thus, while recognising that in reality such offensive State operations require full attribution,[32] the existence thereof is taken in this thesis as given.

This thesis is divided into five main chapters. The first chapter offers an overview of the vocabulary used in the cybersecurity discourse. The second chapter focuses on the general concept on sovereignty, while the third chapter explains how sovereignty is applied in cyberspace. The fourth chapter elaborates on the exercise of State sovereignty vis-à-vis cyberspace and explores different modes of State action. The fifth chapter presents an analysis of international law and cyberspace juxtaposed.

[32] Since violations of the non-intervention principle are considered internationally wrongful acts, it is apt to remind that the UN GGE 2015 report emphasised that "States must meet their international obligations regarding internationally wronful act attributable to them under international law", yet the mere indication that an ICT activity was launched or otherwise originated from a State's territory, from its infrastructure may be insufficient for State-attribution. Furthermore, the accusations of organising and implementing wrongful acts that are brought against a State must be substantiated. UNGA. A/70/174. 22.07.2015. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General, p 12.

1. The vocabulary of cybersecurity

Cybersecurity discourse pertaining to international law is inevitably legal as well as political.[33] Not only does international law serve the political and strategic interests of different States but the vocabulary they use within international law highlights the emphasis one wishes to set. Thus, it is important to note the terminological differences among different actors and explain the main terms and concepts of this thesis.

International law offers today a wide variety of specialist vocabularies.[34] Cybersecurity is one of them, as the field has created in the matter of the past two decades its own vocabulary that unless explained caters only for special audiences with special interest and carries a special ethos.[35] Characterised by the notions of malleability and fluidness, the vocabulary used depends on the perspective of the actors involved. Different participants in the discourse, all equipped with a specific bias towards the expert vocabulary, aim at affecting the outcomes that later manifest in the inter-State relations and international law discussions.[36]

It is important to note that whilst considering any term with the prefix "cyber",[37] it is safe to say that none of them has an agreed upon definition. It is a political notion anchored to the convergence of different technologies[38] and thus, there are as many definitions as there are actors in this discourse. Some of the terms have been defined by individual States in their cyber strategies.[39] Some have acquired a definition through the works of scholars and standardisation bodies.[40] Either way, it is useful to give a short overview of some of the specific terms used in this thesis, since they are not part of the everyday public international law discourse. One must also keep in mind that it is highly likely that no matter what definition we give to any of the cyber-related terms, it is either too narrow or too wide as well

---

[33] Generally about the inevitablity of politics in international law, see M. Koskenniemi. The Politics of International Law. Oxford: Hart Publishing Ltd 2011 and for his updated view on the matter, M. Koskenniemi. The Politics of International Law – 20 Years Later. – European Journal of International Law 2009, Vol. 20, No. 1.

[34] See M. Koskenniemi. Politics of International Law – 20 Years Later, p 12.

[35] *Ibid*, p 9.

[36] *Ibid*.

[37] According to the Oxford English Dictionary, "cyber" means "relating to information technology, the Internet, and virtual reality". The Oxford Compact English Dictionary. Oxford: OUP 2003, p 268.

[38] IISS. Dossier, p 15.

[39] For example NATO CCD COE has collected some of the definitions from States' cyber strategies in their Cyber Definitions database. However, this list is by no means comprehensive and definitive. NATO CCD COE. Cyber Definitions Database. – ccdcoe.org/cyber-definitions.html (visited 15.03.2016). Alternative list of definitions is provided by IISS. Dossier, pp 5-11.

[40] For example of scholarly work see M.N. Schmitt. Tallinn Manual, p 15. Katharina Ziolkowski proposes her own definition of cyber espionage in K. Ziolkowski. Peacetime Cyber Espionage – New Tendencies in Public International Law. – K. Ziolkowski (ed.). Peacetime Regime for State Activities in Cyberspace. Tallinn: NATO CCD COE Publications 2013, p 429.

as led by a bias of the writer and therefore, the definitions chosen are used only for the purposes of this thesis.

One of the widest terms used is "cybersecurity". When it comes to providing a definition for it, there are two different strands of interpretations. First strand, as for example proposed by the US National Institute of Standards and Technology (hereinafter NIST), focuses on the security of cyberspace itself, defining cybersecurity as the "ability to protect or defend the use of cyberspace from cyber attacks."[41] The other strand of interpretation, offered by International Organization for Standardization (hereinafter ISO) and International Electrotechnical Commission (hereinafter IEC), however centres on the confidentiality, integrity and accessibility of the information processed in cyberspace.[42] When Western countries often combine the two strands,[43] the Sino-Russo approach focuses mainly on the security of information, leading them to use a different set of terms altogether. For example, Russia and China use the term "international information security", which is not to be equated with the Western term "cybersecurity", since it insists that international peace and security concerns go beyond mere information infrastructure concerns.[44] Focusing the discussion not on information infrastructure but on the information therein, highlights different solutions, different actors and different interests as will be explained in Chapter 4.1. Both views – the Western as well as the Sino-Russian one – render some aspect of the discourse visible, with pushing other aspects consciously to the background.[45] Choosing and using knowingly a different vocabulary is also a manifestation of a focus point that the State as a sovereign has decided to set in the discourse.

---

[41] R. Kissel. Glossary of Key Information Security Terms. – Cybersecurity, www.nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (visited 10.03.2016).

[42] ISO, IEC. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity. – www.iso27001security.com/html/27032.html (visited 10.03.2016). The same interpretation is also used by some States, see Australian Government's definitions of cyber security. Australian Government. Cyber Security. – www.ag.gov.au/RightsAndProtections/CyberSecurity/Pages/default.aspx (visited 10.03.2016).

[43] For example see France's Strategy. Information systems defence and security. – 2011, www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf (visited 10.03.2016). Similarly, the US approach combines the protection of information infrastructure with the protection of information contained therein. US Department of Defense. Dictionary of Military and Associated Terms. – Joint Publication 1-02, 08.11.2010 (as amended through 15.02.2016), www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (visited 15.04.2016), p 57.

[44] See for example Institute of Information Security Issues of Moscow State University and Conflict Studies Research Centre. Russia's "Draft Convention on International Information Security", A Commentary. – 2012, www.academia.edu/1611951/Russia_s_Draft_Convention_on_International_Information_Security_-_A_Commentary (visited 10.03.2016).

[45] M. Koskenniemi. Politics of International Law – 20 Years Later, p. 11. Koskenniemi also states, "What is being put forward as significant and what gets pushed into darkness is determined by the choice of the language through which the matter is looked at, and which provides the basis for the application of a particular kind of law and legal expertise. That this choice is not usually seen as such – that is as a *choice* – by the vocabularies, but instead something natural, renders them ideological."

International bodies, such as the UN GGE have often used a compromise wording using the phrase "security in the development and use of ICTs"[46] in their deliberations regarding cybersecurity. For the purpose of this thesis, the term "cybersecurity" is used combining the security of the information infrastructure and architecture with the confidentiality, integrity and accessibility of information processed therein.

Secondly, the definition of "cyberspace" has had over time different focuses. Some have defined it through its characteristically man-made nature,[47] some have focused on the use of electromagnetic spectrum.[48] The understanding of "cyberspace"[49] for the purposes of this thesis follows the definition provided by NIST, that is: "A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[50] Again, in the Sino-Russo approach a parallel term of "information space" is used in international discourse, which is defined as the sphere of activity connected with the formation, creation, conversion, transfer, use and storage of information and which has an effect on individual and social consciousness, the information infrastructure and information itself.[51] Even though the focus of both of the definitions is at opposite directions, what transpires for the present thesis from both of them is that even though to a large extent cyberspace is considered an intangible space, it is nevertheless supported by physical infrastructure, which connects it to the physical world.[52]

Lastly, and most importantly, it is of essence to define what is understood under the term "cyber operations". As the literature on "cyber" continues to proliferate, scholarly works offer numerous definitions to cyber operations, cyber attacks,[53] cyber exploitations and information

---

[46] UNGA. A/65/201. 30.07.2010. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General; UNGA. UN GGE 2013 Report; UNGA. UN GGE 2015 Report.

[47] G.H. Todd. Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition. – Air Force Law Review 2009, Vol. 64, p 68.

[48] See D.J. Ryan, M. Dion, E. Tikk, J.J.C.H. Ryan. International Cyberlaw: A Normative Approach. – Georgetown Journal of International Law Summer 2011, Vol. 42, No. 4, p 1167.

[49] The word "cyberspace" was first used by William Gibson in his book Neuromancer. W. Gibson. Neuromancer. New York: Berkley Publishing Group 1989, p 128.

[50] R. Kissel. Referenced work, p 58. The definition is identical to US DoD definition in US DoD. Dictionary of Military and Associated Terms, p 58.

[51] Institute of Information Security Issues of Moscow State University. Referenced work, p 32.

[52] R. Bryant. What kind of space is cyberspace? – Minerva – An Internet Journal of Philosophy 2001, Vol. 5, p 138; N. Tsagourias. The Legal Status of Cyberspace. – N. Tsagourias, R. Buchan (eds.). Research Handbook on International Law and Cyberspace. Cheltenham: Edward Elgar Publishing 2015, p 15.

[53] For example Shackelford defines computer network attack as "hostile attack hostile attack by one nation or hostile party against the important information technology /…/ systems and networks of another". Waxman characterises cyber attack as an "effort to alter, disrupt, or destroy computer systems or networks or the information or programs on them". Palojärvi adds to prior definitions that the aim of the attack is to "manipulate,

operations[54] etc. One way of distinguishing different activities in cyberspace is by assessing their intent and severity. From that follows a spectrum, which starts from the least severe activity: "cyber incident". It stands for a possibly unintentional activity resulting in actual or potentially adverse effect on an information system and/or the information therein.[55] "Cyber attack" (often also computer network attack or CNA), however, presumes intent and targets an "enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information".[56] Tallinn Manual offers an alternative definition stating that "cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects".[57] "Cyber exploitation" (often also computer network exploitation or CNE) combines the enabling operations and intelligence collection capabilities conducted through the use of computer networks in order to gather data from target or adversary's information systems or networks.[58] When turning back to the original question of a definition for cyber operations, then for the purpose of this thesis, cyber operations are understood as comprising of cyber attacks and cyber exploitations which stay below the use of force threshold, but can be characterised by intent, specific target, coordination, strategy and motivation. Hence, they are more severe and sophisticated than cyber incidents and must possess the element of intent.

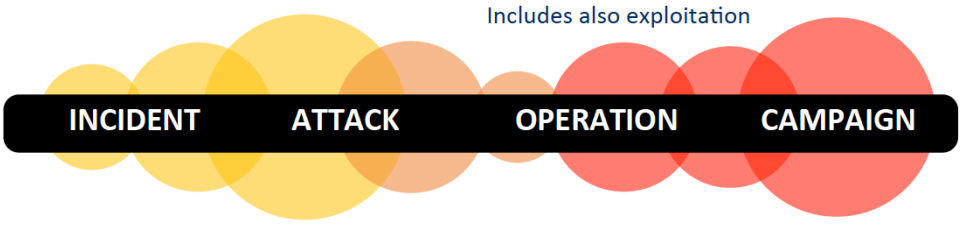

Figure 1. Spectrum of cyber activities

---

corrupt or hide the information that the systems rely on to function properly". S. Shackelford. From Nuclear War to Net War, p 199; M.C. Waxman. Referenced work, p 422; P. Palojärvi. Referenced work, p 27.

[54] See for example NIST's definition: "The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making process, information, and information systems while protecting our own." R. Kissel. Referenced work, p 94.

[55] *Ibid*, p 57.

[56] R. Kissel. Referenced work, p 57.

[57] M.N. Schmitt. Tallinn Manual, p 106.

[58] R. Kissel. Referenced work, p 41.

Additionally, throughout the thesis the concept of "information infrastructure and architecture" will be used. For the purposes of clarity, infrastructure describes the set of components that make up a system (e.g. submarine cables, satellites, fibre optic cables, computers, servers), while architecture describes the design of the components and the relationships between them.[59] Hence, cyberspace is built on an information infrastructure and has a particular information architecture. Lastly, the fourth chapter makes use of the technical term distributed denial-of-service attack. Distributed denial-of-service (hereinafter DDoS) is an attack, where multitude of compromised systems, i.e. botnets, attack a single target. That causes a denial of service for the users of the targeted systems and the target system shuts down.[60]

[59] E. Tikk-Ringas, C. Spirito. Lecture series on Information Infrastructure and Architecture at University of Tartu. – Autumn 2014/2015, www.uttv.ee/naita?id=20298&sessioon=4191174049486303024 9 (visited 10.03.2016).

[60] TechTarget. Distributed Denial-of-Service Attack Definition. – searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack (visited 20.03.2016).

2. Sovereignty as a concept

The concept of sovereignty, albeit more often than not interdisciplinary contested, has proven to be highly adaptable over time.[61] It has survived many eras – de-colonisation, globalisation, the rise of supra-national organisations – and thus, some would say it has over time acquired a borderline mythical quality.[62] Deploring the ambiguity of the concept has according to Hent Kalmo and Quentin Skinner become itself a recurring motif in the rich literature on sovereignty.[63] Even though dubbed by some as the "bad word",[64] sovereignty as a concept is still at the heart of the international legal system and the sovereign State is still the ultimate member of international community as well as the most important actor in the international legal system.[65]

Sovereignty is resolutely also surviving the digital age, thus before turning to the concept of sovereignty vis-à-vis cyberspace, one has to inquire into the general meaning of sovereignty. The following chapter elaborates on sovereignty as the cornerstone of international law and on the questionable death of sovereignty.

2.1. Sovereignty as a cornerstone of international law

The Peace of Westphalia (1648) is often seen as the point of inauguration for modern international law and for the modern State. It represents a moment, when the core concept of sovereignty became part of international law.[66] Over time, sovereignty has become not only the core notion of statehood but also the axiomatic principle on which "the whole international law rests".[67] Most, if not to say all principles of international law rely directly or indirectly on State sovereignty.[68] Sovereignty, even though, some doubt its necessity in

[61] B. Fassbender. Sovereignty and Constitutionalism in International Law. – N. Walker (ed.). Sovereignty in Transition. Oxford: Hart Publishing 2003, p 115.
[62] L. Henkin. The Mythology of Sovereignty. – R.St.J. Macdonald (ed.). Essays in Honour of Wang Tieya. The Hague: Martinus Nijhoff 1993, p 351; B. Simma, D-E. Kahn, G. Nolte, A. Paulus (eds.). The Charter of the Uniter Nations. A Commentary. 3rd ed. Volume 1. Oxford: OUP 2012, p 135.
[63] H. Kalmo, Q. Skinner. Introduction: a concept in fragments. – H. Kalmo, Q. Skinner (eds.). Sovereignty in Fragments: The Past, Present and Future of a Contested Concept. Cambridge: CUP 2010, p 1.
[64] L. Henkin. International Law: Politics and Values. Dordrecht: Martinus Nijhoff Publishers 1995, p 8.
[65] M. Koskenniemi. From Apology to Utopia. Cambridge: CUP 2005, p 236.
[66] J. Crawford, M. Koskenniemi (eds.). The Cambridge Companion to International Law. Cambridge: CUP 2012, p 30; D. Philpott. Revolutions in Sovereignty: How Ideas Shaped Modern International Relations Princeton: Princeton University Press 2001, Chapter 5.
[67] ICJ. 27.06.1986. Military and Paramilitary Activities in and against Nicaragua *(Nicaragua v. United States)*. ICJ Reports 1986, para 263.
[68] S. Besson. Sovereignty. – Max Planck Encyclopedia of Public International Law, OUP 2011, online edition, opil.ouplaw.com/home/epil (visited 29.03.2016).

today's world,[69] is still inherent to Statehood and often described as the "basic constitutional doctrine of the law of nations".[70]

It is easy to get tangled in the web of different terminology and opinions.[71] In the words of Lassa Oppenheim, "there exists perhaps no conception, the meaning of which is more controversial than that of sovereignty. It is an undisputable fact that this conception […] had never had a meaning which was universally agreed upon".[72] Furthermore, much of the literature focuses on justifying State sovereignty, when in reality the crucial question in times of contestation and conflict is the extent of it.[73] Nowadays, the model of absolute or complete sovereignty cannot be considered valid, taking into account the interdependencies among States and the changes States have gone through since 1945.[74]

In the most general notion, sovereignty means the totality of international rights and duties recognised by international law[75] that reside in a State.[76] However, the appropriate legal starting point of this analysis ought to be the UN Charter Article 2(1), which establishes the principle of sovereign equality of States,[77] assuring the legal equality of States.[78] One of the corollary principles deriving from the notion of State sovereignty is the principle of territorial sovereignty, which defines sovereignty by reference to State's physical territory. Leaving aside the various theories on the legal function of territory,[79] there is a consensus according to

---

[69] M. Koskenniemi. What Use for Sovereignty Today? – Asian Journal of International Law 2011, Vol. 1, p 62.
[70] J. Crawford. Brownlie's Principles of Public International Law, 8th ed. Oxford: OUP 2012, p 447.
[71] A. Plekksepp. Riigi suveräänsus karistusõiguse ajaloolises ja euroopastumise kontekstis. – H. Kalmo, M. Luts-Sootak. Iganenud või igavene? Tekste kaasaegsest suveräänsusest. Tartu: Tartu Ülikooli Kirjastus 2010, p 186-187.
[72] L. Oppenheim. International Law: A Treatise Vol 1, 4th ed. A.D. McNair (ed.) London: Longmans, Green & Co 1928, p 137.
[73] For further discussion on the pure fact view *versus* the legal view, see M. Koskenniemi. From Apology to Utopia, p 238-239. He argues that sovereignty is essentially torn between the two approaches. The legal approach seeks to bring sovereignty under the umbrella of international law as the higher normative code, which would them tame States' subjective politics and offer States thus sovereignty within the law. The pure fact approach on the other hand states that sovereignty is external to international law and it is rather to be construed as a means to fulfill the inherent liberties of States. Sovereignty as a concept is contested, because no adequate choice can be made between the two positions.
[74] L. Condorelli, A. Cassese. Is Leviathan Still Holding Sway over International Dealings? – A. Cassese (ed.) Realizing Utopia: The Future of International Law. Oxford: OUP 2012, p 22. Cf. L. Mälksoo. Russian Approaches to International Law. Oxford: OUP 2015, p 100 ff.
[75] ICJ. 11.04.1949. Reparation for Injuries Suffered in the Service of the United Nations. Advisory Opinion. ICJ Reports 1949, p 180.
[76] J. Crawford. Chance, Order, Change: The Course of International Law. The Hague: Hague Academy of International Law 2014, p 88.
[77] UN Charter, Article 2(1).
[78] Academics emphasise that Article 2(1) assures juridical, not political, military, economic, geographic, demographic or other equality of States. K. Ziolkowski. General Principles of International Law as Applicable in Cyberspace. – K. Ziolkowski (ed.). Peacetime Regime for State Activities in Cyberspace. Tallinn: NATO CCD COE Publications 2013, p 156.
[79] For various theories on the legal function of State's territory, see S. Torres Bernárdez. Territorial Sovereignty. – R. Bernhardt (ed.). Encyclopedia of Public International Law Vol. IV. Amsterdam: Elsevier 2000, p 823 ff.

which a State exercises full and exclusive authority over its territory.[80] Max Huber in the 1928 Island of Palmas Arbitration award links the exercise of effective power over certain territory with sovereignty by stating as follows: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusivity of any other States, the functions of a State."[81] International Court of Justice (hereinafter ICJ) added to that notion stating that "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations". [82] Thus, sovereignty has always been, at least in part, grounded in the idea of territoriality and the extent of sovereign's reach was usually decided by geographic borders,[83] extending "to the internal waters and territorial sea of every State and to the air space above its territory".[84]

Hence, territoriality is not only an essential aspect of sovereignty, but also of the capacity of the State sovereignty. It refers to the supreme and full authority over certain territory, over its people to the exclusion of any other State. To take the myth-like character out of the notion, it is the "functional power possessed by a ruler or a government to rule a population for its own good".[85] Within the State, the sovereign power makes law with the assertion that it is supreme and ultimate. Its validity does not depend on any other higher authority and thus, it is often also called internal sovereignty, which allows State itself to determinate the order in that State. State's exclusive right to decide on what acts shall take place on its territory has been generally "virtually undisputed".[86]

In inter-State relations, a sovereign State obeys no other authority.[87] This notion is connected to the idea of independence, i.e. State's legal position vis-à-vis other States.[88] Permanent Court of International Justice (hereinafter PCIJ) held in the Lotus case that "restriction upon the independence of States […] cannot be presumed".[89] Moreover, in the case of S.S. Wimbeldon, the PCIJ held that restrictions placed upon the exercise of sovereignty "must be

---

[80] PCIJ. 07.09.1927. Case of S.S. Lotus (*Turkey v. France*). PCIJ Series A, No. 10, p 18-20; PCIJ. 07.07.1932. Free Zones of Upper Savoy and the District of Gex. PCIJ Series A/B, No. 46, p 166–168.
[81] PCA. 04.04.1928. Island of Palmas case (*Netherlands. v. US*). Reports of International Arbitral Awards, Vol. 2, p 838.
[82] ICJ. Corfu Channel, para 202.
[83] R. Buchan. Cyber Attacks, p 222.
[84] ICJ. Nicaragua, para 212.
[85] M. Koskenniemi. What Use of Sovereignty Today, p 63.
[86] M. Koskenniemi. From Apology to Utopia, p 237.
[87] B. Simma et al. UN Charter Commentary, p 136.
[88] M. Koskenniemi. From Apology to Utopia, p 241. The idea of independece was also defined by the PCIJ in the Austro-German Customs Union Case, as "the continued existene of [a State – emphasis added LA] within her present frontiers as a separate State with the sole right of decision in all matters economic, political, financial or other". PCIJ. 05.09.1931. Customs Regime Between Germany and Austria. Advisory Opinion. Series A/B 41, p 45.
[89] PCIJ. S.S. Lotus, p 18.

construed as restrictively as possible and confined within its narrowest limits".[90] Yet, accepting treaty obligations is not regarded as a confinement of sovereignty, but rather an exercise of it. Being able to bind themselves under international treaties is an attribute of State's sovereignty.[91] The PCIJ made in the S.S. Wimbeldon case the distinction between the possession of sovereignty *in abstracto* and the exercise of sovereignty *in concreto*. Meaning, even if the State were stripped all of its attributes that belong to its notion of sovereignty, e.g. the power to conclude treaties, the State itself remains fully sovereign. As such, the S.S. Wimbeldon case broke ground: sovereignty was no longer an absolute phenomenon, but became relative, disaggregated phenomenon that encompasses a bundle of rights and obligations.[92] Thus, when the PCIJ claimed in 1923 in the Nationality Decrees case that sovereignty is a "relative matter",[93] then it is not the concept of sovereignty itself that is relative, but the amount of rights and obligations that the State has at any given moment in international relations deriving from its exercise of sovereignty vis-à-vis other States.

So, sovereignty does not merely afford protection but also imposes obligations on States, notably the "obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability in peace and in war, together with the rights which each State may claim for its nationals in foreign territory."[94] In essence, States have the obligation to recognise the sovereignty of other States, the obligation to follow the principle of non-intervention and the obligation to control the actions that occur within the sovereign's geographic boundaries.[95]

Besides the traditional legal notion, several other approaches have been proposed over time, which emphasise that the concept and practice of sovereignty are not always uniformly accepted. For example Stephen Krasner advocates for distinguishing between different forms of sovereignty that States can enjoy to a greater or a lesser degree. According to Krasner, the concept of sovereignty ought to embed three distinctive notions: international legal

---

[90] PCIJ. 17.08.1923. Case of the S.S. Wimbeldon. PCIJ Series A, No 1, p 24.
[91] B. Simma et al. UN Charter Commentary, p 138; PCIJ. S.S. Wimbeldon, p 25.
[92] J. Klabbers. Clinching to the concept of sovereignty: Wimbeldon redux. – Austrian Review of International and European Law 1999, Vol. 3, No. 3, p 362.
[93] PCIJ. 07.02.1923. Nationality Decrees Issued in Tunis and Morocco (French Zone) on November 8th. Advisory Opinion. Series B04, p 23-24. M. Koskenniemi. From Apology to Utopia, pp 258-272.
[94] PCA. Island of Palmas, p 839. In his separate opinion in the Corfu Channel case, Judge Alvarez stated, "By sovereignty, we understand the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other States, and also in its relations with other States. Sovereignty confers rights upon States and imposes obligations upon them." ICJ. Corfu Channel, separate opinion of Judge Alvarez, p 43.
[95] E.T. Jensen. Cyber Sovereignty, p 282.

sovereignty, domestic sovereignty and Westphalian or Vattelian sovereignty.[96] International legal sovereignty flows from the concept of external sovereignty explained above. It entails international recognition of independent territorial entities, which implies the right to enter into any agreement the State chooses. Domestic sovereignty refers to the particular order how the public authority is organised and implemented within a State, i.e. effective control over the territory of the State including the ability to regulate trans-border movements. Lastly, the Westphalian sovereignty implies the obligation not to intervene in the internal affairs of other sovereign States. It signifies the absence of submission to external authority structures.[97] According to Krasner, all three of these forms are distinct and do not form an organic whole. The elements of sovereignty have also not been conjoined in practice.[98] Krasner's theory, while at times radical, emphasises excellently, how sovereignty in essence has different angles that need to be considered. It exemplifies that sovereignty is not monolithic, but can be considered rather a "sponge concept" that can manifest itself in different forms.[99]

Thirdly, Nicholas Tsagourias proposes that it is important to disentangle sovereignty as a concept from the notion of territory, as territory as an element of sovereignty is a "lego-political construct", which aims at organising space for political or legal purposes.[100] As such State's territory is not only the object, but also the container of sovereignty, as it draws State's legal and political borders. With his approach, Tsagourias distances himself from the traditionally accepted concept of sovereignty. He explains that "whereas sovereignty as *summa potestas* is unbounded, territory localises sovereignty"[101] and acts as the "constraint that unravels the assertion of unconstrained sovereignty".[102] Seeing sovereignty bound to one territory on which it is exercised, can be considered a political act, which is a result of a political process and successful assertions of power. According to Tsagourias, there is no inherent nexus between territory and sovereignty. Territory offers a tangible space, where sovereignty can manifest itself in political and legal terms. Thus, sovereignty could extend

---

[96] In his earlier work "Sovereignty: Organized Hypocrisy" (1999) Krasner distinguishes four forms, adding interdependence sovereignty, however, in his later works, he has excluded the form focuses on the three main ones as mentioned above. S.D. Krasner. Sovereignty: Organized Hypocrisy, pp 9-25. Cf. S.D. Krasner. The Hole in the Whole: Sovereignty, Shared Sovereignty, and International Law. – Michigan Journal of International Law 2004, Vol. 25, p 1077; S.D. Krasner. The durability of organized hypocrisy. – H. Kalmo, Q. Skinner (eds.). Sovereignty in Fragments: The Past, Present and Future of a Contested Concept. Oxford: OUP 2010, p 96.
[97] S.D. Krasner. The Hole in the Whole, p 1077. S.D. Krasner. The durability of organized hypocrisy, p 96.
[98] S.D. Krasner. The durability of organized hypocrisy, p 97.
[99] J. Bartelson. A Geneology of Sovereignty. Cambridge: CUP 1993, p 26.
[100] N. Tsagourias. Legal Status of Cyberspace, p 18.
[101] *Ibid*, p 17.
[102] J.P. Trachman. Cyberspace, sovereignty, jurisdiction and modernism. – Indiana Journal of Global Legal Studies 1998, Vol. 5, Iss. 2, p 567.

beyond any allocated territory and also to non-territorial entities.[103] Even though novel, Tsagourias' view leaves unclear where the extent of one State's sovereignty ends and another one's begins. That would also challenge the application of multiple principles deriving from the concept of sovereignty, e.g. the principle of non-intervention.

The present thesis adopts the first and most traditional legal view of sovereignty, with the addition of taking into account the political sensitivities that accompany the notion. Sovereignty implies on the on the one hand the monopoly of the governing authority within the state, which is generally seen as exclusive. On the other hand, it implies relations between the States, where each State is externally independent and where the amount of rights and obligations may vary as a result of exercises of sovereignty by the State.

2.2. Is sovereignty withering away?

For various reasons a considerable amount of works on the erosion, loss, waning, withering of sovereignty, or on its decline, retreat or apparent death have been produced by scholars.[104] Argument can be made that sovereignty in general accounts for less in today's world. After all, States have used sovereignty to limit sovereignty to a great extent through voluntarily binding themselves with an increasingly dense network of formal and informal rules and regimes.[105] However, that is not to say it counts as a derogation or loss of sovereignty: States have been able to bind themselves, because they are sovereigns.[106] States have tamed down sovereignty through exercising sovereignty. As an organized hypocrisy it "upholds egoistic interests of limited communities against the world at large, providing unlimited opportunities for oppression at home."[107] We have observed its failure to deal with global threats, while obstructing global beneficial cooperation. Instead of a "narrow, ethnocentric way to think about the relations of human beings,"[108] in several fields global approaches have become prevalent, which cross the "artificial national boundaries".[109] Not to mention threats that have

---

[103] N. Tsagourias. Legal Status of Cyberspace, p 18.
[104] For example, E. Lauterpacht. Sovereignty – Myth or Reality? – International Affairs 1997, Vol. 73, No. 1; C. Schreuer. The Waning of the Sovereign State: Towards a New Paradigm for International Law. – European Journal of International Law 1993, Vol. 4; T.G. Weiss, J. Chopra. Sovereignty under Siege: From Intervention to Humanitarian Space. – G.M. Lyons, M. Mastanduno (eds.). Beyond Westphalia?: State Sovereignty and International Intervention. Baltimore: Johns Hopkins University Press 1995; J.A. Camilleri, J. Falk. The End of Sovereignty? The Politics of a Shrinking and Fragmenting World. – Foreign Affairs Fall 1992, www.foreignaffairs.com/reviews/capsule-review/1992-09-01/end-sovereignty-politics-shrinking-and-fragmenting-world (visited 01.04.2016).
[105] M. Koskenniemi. What Use for Sovereignty Today, p 62.
[106] *Ibid*; PCIJ. S.S. Wimbeldon, p 25.
[107] M. Koskenniemi. What Use for Sovereignty Today, p 61.
[108] *Ibid*, p 62.
[109] *Ibid*; M. Koskenniemi. The Wonderful Artificiality of States. – American Society of International Law Proceedings 1994, Vol. 88, pp 22–29.

become not only cross-border but also global, influencing interdependent system of States more than ever through inter-connectedness of networks and information infrastructure. Thus, at first glance "[t]o suggest that there might be good use for state sovereignty sounds counter-intuitive,"[110] even more so in the context of cyberspace.

Furthermore, it has been suggested that the concept of sovereignty should be abandoned from the vocabulary of international law completely. Reason being that not only is its meaning confusing, its uses various, but some of those uses are unworthy, some destructive of human values.[111] Predictions of the demise of State sovereignty due to interdependence have surfaced then and again throughout the 20th century. For example, the former US Secretary of State Robert Lansing opined in the beginning of 1920s that world sovereignty would become a reality in the practice of States due to interdependence among States.[112] Similarly, Georg Schwarzenberger, a distinguished international law scholar of the 20th century, noted that it is fashionable to argue that independence is giving way to interdependence on the international level, however, that might just seem so at the first glance.[113]

Thus, before declaring the concept of sovereignty dead and moving on in an unorganized hypocrisy, what perhaps is needed is an understanding of its realisation on the most varied fields of international conduct.[114] States are still free to exercise their sovereignty – protection of their interest practically requires it.[115] If States have pooled, shared, delimited or delegated away some of their powers through treaties and participation in various international organisations and venues, they can always take back the powers that they have previously negotiated away,[116] since that is also a sovereign prerogative. If a State's capacity to act on a domestic as well as on the international level is usually referred to as sovereignty, there is no reason to speak about the demise of sovereignty. Regardless of the particular philosophy of sovereignty one follows, sovereignty has had and continues to have an important role in the development of international law as well as the concept of the State. Thus, the present work continues with the approach that focuses on the concept of sovereignty as well as the exercise thereof.

---

[110] M. Koskenniemi. What Use for Sovereignty Today, p 61.
[111] L. Henkin. That "S" Word: Sovereignty, and Globalization, and Human Rights, et cetera. Lecture. – Fordham Law Review 1999, Vol. 68, p 1. See also L. Henkin. The Mythology of Sovereignty, p 352.
[112] R. Lansing. Notes on Sovereignty. – Washington DC: Carnegie Endownment for International Peace 1921, p 56.
[113] G. Schwarzenberger. The Forms of Sovereignty. – Current Legal Problems 1957, Vol. 10, p 264.
[114] M. Koskenniemi. From Apology to Utopia, p 237.
[115] J. Crawford. Sovereignty as a legal value. – J. Crawford, M. Koskenniemi (eds.). The Cambridge Companion to International Law. Cambrige: CUP 2012, p 132.
[116] J.E. Alvarez. State Sovereignty is Not Withering Away: A Few Lessons for the Future. – A. Cassese (ed.). Realizing Utopia: The Future of International Law. Oxford: OUP 2012, p 26.

Another criticism is that States do not own the monopoly of governing authority. According to the functional view, States lose their normative priority and compete with supranational, private and local actors for the allocation of regulatory authority. If one were to discard the concept of sovereignty, Benedict Kingsbury argues, it would only intensify the inequality, weaken the restraints on coercive intervention and diminish the critical roles of the State in the international system.[117]

Much of the debate surrounding sovereignty in recent decades has been binary: States' sovereignty is or is not disappearing. Supranational organisations and inter-connectedness are apparently turning States into only half-sovereigns,[118] global problems challenge State sovereignty since they need global solutions. As Antonio Cassese notes, "we are dealing at the moment with a substantial alteration of the modes of exercising the sovereignty of States, rather than the real decline of it."[119] One should not forget, how and by whom decision-making power is actually exercised within the supranational institutions.[120] Those who really decide on the supranational level, e.g. in the UN, are States. Global problems find solutions still among States. If States in need decide to include the private sector, they are not giving part of their sovereignty away, instead, they are making a sovereign decision to cooperate with the private sector and that is exercise of State sovereignty. Thus, if there is a crisis in sight, it is a crisis of a particular mode of exercising State sovereignty that has grown to be accustomed to be connected with States. Sovereignty has never been an absolute but an aggregation of power subject to different degrees of sovereign control. No single description of State sovereignty at any given point is likely to satisfy the inquiry, since the set of attributes that defines a State and its sovereignty changes through time and varies with the State in question.[121] Sovereignty is not a monolith, thus it would be wise to move away from the dichotomies and focus on how States are actually exercising their sovereignty and the flexibility that States are creating within the concept of sovereignty. Therefore, the present work will turn its focus on how sovereignty is applied.

---

[117] B. Kingsbury. Sovereignty and Inequality. – European Journal of International Law 1998, Vol. 9, p 599.
[118] S.D. Krasner. Pervasive nor Perverse: Semi-Sovereigns as the Global Norm. Symposium Making Peace Agreements Work: The Implementation and Enforcement of Peace Agreement Between Sovereign and Intermediate Sovereign. – Cornell International Law Journal 1997, Vol. 30, p 652.
[119] L. Condorelli, A. Cassese. Referenced work, pp 18-19.
[120] *Ibid*.
[121] J. Alvarez. Referenced work, p 31.

3. Sovereignty in cyberspace – a necessary oxymoron

Cyber operations challenge the traditional concept of sovereignty. At a first glance, sovereignty seems to have morphed in the present context into something formalistic, with no real meaning – something that can be easily breached without any following consequences. However, this is not a recent development. The impact of information technology on the power of sovereign States was recognised already in the 1990s.[122] Many premised that the Information Age would lead to the 'demise of the nation-state through the erosion of state power and, as a result, state sovereignty'.[123] Alf Ross opined that there is hardly any domain, in which the obscurity and confusion are as great as when it comes to sovereignty.[124] Adding to the notion the ambiguity of the cyber domain, the effect is multiplied.

Cyberspace does not abide State boundaries, as it is inherently a cross-border construct. The interdependent global information infrastructure, consisting *inter alia* of submarine cables, satellites, telecommunication networks etc., and the resident data flowing in the networks challenge the traditional notions of territory. One cannot easily establish physical State boundaries or mark a certain territory as one's own, for it is a connected web of infrastructure and architecture that often relies on several actors cooperating. Here, the questions about the relevance of sovereignty in the 21st century once again emerge. The doubts, whether cyberspace could be immune from State sovereignty, fears of anarchy in cyberspace, considerations of interpreting cyberspace as a global commons – all these questions have been prevalent in the scholarly works.[125]

The following chapter looks at sovereignty in cyberspace from three different angles. As the sovereignty debate may be divided into phases of cyber libertarianism, considering cyberspace as global commons and thirdly, trying to reconcile the general notion of sovereignty and territory with a largely intangible space, the following chapter gives an overview of the development of the modern sovereignty in cyberspace.

---

[122] H.H. Perritt Jr. Cyberspace and State Sovereignty. – Journal of International Legal Studies 1997, Vol. 3, p 157.
[123] C. Kavanagh. Cybersecurity, Sovereignty, and U.S. Foreign Policy. – American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy 2015, Vol. 37, pp 100–101.
[124] A. Ross. A Textbook of International Law. London. Longmans, Green & Co 1947, p 34.
[125] See for example, D.G. Post. Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace. – Journal of Online Law 1995; J.L. Goldsmith. Against Cyberanarchy. – University of Chicago Law Review 1998, Vol. 65.

3.1. Cyber libertarianism: Cyberspace as a law-free zone

Not long ago, cyberspace was described as a Wild West,[126] where no State would be able to exercise territorial control and drawing a connection between cyberspace and sovereignty seemed more of an oxymoron than reality. The early views of cyberspace were largely primitive and still trying to grasp the complexity of the cyberspace. The belief that cyberspace ought to be free from State interference led to the misconception or "utopia" that cyberspace is immune from State sovereignty.[127] Online freedom activists, sometimes also called cyberlibertarians, saw cyberspace as free from regulatory intervention already in 1990s, when John Perry Barlow stated in *A Declaration of Independence of Cyberspace* that,

> "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."[128]

Barlow's famous manifesto declared cyberspace immune from territorial sovereignty of nation States, influenced by the second half of the cyberlibertarian thought, which comes from David Post and David Johnson, whose paper "Law and Borders – The Rise of Law in Cyberspace", made the point that cyberspace not only cannot be subjected to sovereignty, but instead it should be subject to its own distinct legal regulation, which would be based on self-regulation.[129] Their no-sovereignty thesis, founded on the concept of cyber-exceptionalism,[130] reflected that the open, decentralised and participatory space ought to not be hampered by legal regulations imposed by States.[131] After all, cyberspace is different from real spaces by being a-territorial, borderless and ubiquitous in character. As such, it differentiates from physical and bounded spaces or domains that are currently subject to legal regulation.[132] They claimed that "the Net radically subverts a system of rule-making based on borders between

---

[126] For example International Institute of Humanitarian Law has put forward the opinion that "[t]he distinctive feature of cyberspace is that it is a notional environment and beyond the jurisdiction of any single nation." International Institute of Humanitarian Law. San Remo Handbook on Rules of Engagement. – 2009, www.iihl.org/Media/Default/PDF/Publications/RoE/ROE%20HANDBOOK%20ENGLISH%2009.05.2011%20PRINT%20RUN.pdf (visited 20.03.2016), p 15.
[127] P.W. Franzese. Referenced work, pp 11–12.
[128] J.P. Barlow. A Declaration of Independence of Cyberspace. – 1996, projects.eff.org/~barlow/Declaration-Final.html (visited 10.04.2016). See also D.R. Johnson, D. Post. Law and Borders – The Rise of Law in Cyberspace. – Stanford Law Review 1996, Vol.48, p 1371.
[129] D.R. Johnson, D. Post. Law and Borders, p 1367.
[130] N. Tsagourias. Legal Status of Cyberspace, p 16.
[131] T. Wu, J. Goldsmith. Who Controls the Internet? Illusions of a Borderless World. Oxford: OUP 2006, p 23.
[132] D.R. Johnson, D. Post. Law and Borders, p 1367. Cf. J.L. Goldsmith. Against Cyberanarchy.

physical spaces".[133] Cyberspace itself undermined the ability for a State to assert *de facto* jurisdiction over online activities. Thus, cyberspace should be a separate legal jurisdiction from the "real world". Whereas traditional State sovereignty is based on notions of physical borders, it cannot effectively function in cyberspace. Individuals and different actors can move effortlessly between zones that are governed by different regimes, choosing one they wish.[134] Moreover, the sovereignty's principles of validity – power, legitimacy, effects, notice – which are generally exhibited in territorial entities, were considered impossible or at best diluted when it comes to cyberspace.[135] Since Internet, in Johnson and Post's mind did not recognise existing physical borders, it was not falling under State's authority, whose sovereignty was confined to one territory, separated from others by boundaries.[136] Thus, the rules for governing said space would have derived from the generative community that uses cyberspace, not from externally imposed laws from nation States.[137]

Barlow took the argument further, noting that not only is it impossible to impose external legal controls in cyberspace, because *de facto* authority cannot be imposed on an intangible, borderless space, but any such attempt to exercise sovereignty therein would lack legitimacy, since there is no recognised law-making authority for said space. From the latter argument, the historical perspective of mid-1990s shines through, when cyberspace was much less regulated space and movements to regulate online activities were in their infancy.[138]

Jack Goldsmith presented soon after an opposite view to cyberlibertarians. He claimed that their view was infected by three particular fallacies, which would undermine their arguments. Firstly, the fallacy that cyberspace was a separate space. Secondly, that territorially bound governments cannot regulate the non-territorial cyberspace. Thirdly, he claimed that there is over-optimism that there will be cheap and plentiful information.[139] Essentially, Goldsmith

---

[133] D.R. Johnson, D. Post. Law and Borders, p 1370.
[134] A. Murray. Uses and Abuses of Cyberspace: Coming to Grips with the Present Dangers. – A. Cassese. Realizing Utopia: The Future of International Law. Oxford: OUP 2012, p 500.
[135] D.R. Johnson, D. Post. Law and Borders, pp 1370-1376; N. Tsagourias. Legal Status of Cyberspace, p 16.
[136] A. Murray. Referenced work, p 500.
[137] D.R. Johnson, D. Post. And How Shall the Net be Governed?: A Mediation on the Relative Virtues of Decentralized, Emergent Law. – B. Kahin, J.H. Keller (eds.). Coordinating the Internet. Cambridge: MIT Press 1997. See also, D.B. Hollis. Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack? – J.D. Ohlin, K. Govern, C. Finkelstein (eds.). Cyberwar: Law and Ethics for Virtual Conflicts. Oxford: OUP 2015, p 132-133.
[138] A.Murray. Referenced work, p 500. See also IISS. Dossier, pp 53-68. However, Barlow seems to still be of the opinion that cyberspace is immune to sovereignty and always will be. See further, A. Greenberg. It's Been 20 Years Since This Man Declared Cyberspace Independence. – Wired, 08.02.2016, www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/ (visited 20.04.2016).
[139] J.L. Goldsmith. Regulation of the Internet: Three Persistent Fallacies. – Chicago-Kent Law Review 1998, p 1119. Goldsmith also challenged the descriptive and normative premises of the no-sovereignty thesis in his article Against Cyberanarchy, where he states that the impossibility of sovereign power in cyberspace, as identified by Johnson and Post, have been largely exaggerated. J.L. Goldsmith. Against Cyberanarchy, p 1199 ff.

made the point that actors in cyberspace are not removed from our world and thus, he understood cyberspace more like a communications media rather than a physical space. For Goldsmith, cyberspace is an extension of a pre-existing communications media and there is no distinction needed between space and cyberspace.[140] As a communication media, similarly to telephone and other communications equipment, which all have real-world existence and are located at least partly in one of physical world legal jurisdictions, cyberspace activities are undertaken from within sovereign jurisdictions,[141] where States can effectively regulate said activities.

Even though Goldsmith's view was a more realistic than cyberlibertarians' one, it did not count for the exponentially increasing extent of cyberspace activity States would have to consider in the next decade. At the same time, States started to realise the immense potential of ICTs. Russia was the first one to express its concerns about the information weapons and the threat of information wars already in 1998, emphasising the importance of sovereignty in the fight against such arms race.[142] Soon, after Russia's initiative, States started to grasp that the global, largely intangible, conceptual element of cyberspace clearly differs from the traditional spaces onto which the principle of sovereignty is usually applied, i.e. land, sea, air and space.[143]

Whether or not cyberspace is a subject to international law is to a great extent not disputable anymore. As will be explained below, the UN GGE affirmed the applicability of existing international law, especially the UN Charter, to cyberspace with its 2013 Report.[144] Thus, the cyberlibertarian view of cyberspace as a non-legal domain, even though noble, has been in the practice overturned for a more traditional view of State sovereignty and its applicability to cyberspace.

3.2. Common misconception: cyberspace as a global commons

Lawyers love to reason by analogy, but as Brown puts it "analogies fail us in cyber operations."[145] Due to the differences of cyberspace from any other physical domain, most attempts to draw analogies are bound to fail. Even though cyberspace is a unique manmade formation, one of the suggestions often made is that cyberspace is part of the global commons

---

[140] J.L. Goldsmith. Regulation of the Internet: Three Persistent Fallacies, p 1121. See also A. Murray. Reference work, p 501.
[141] C. Reed. Internet Law: Text and Materials, 2nd ed. Cambridge: CUP 2004, p 188.
[142] UN Disarmament Committee. A/C.1/53/3. 30.09.1998. Letter Dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations Addressed to the Secretary-General.
[143] V. Lowe. International Law, 1st ed. Oxford: OUP 2007, p 151.
[144] UNGA. UN GGE 2013 Report, para 19.
[145] G.D. Brown. The Wrong Questions About Cyberspace, p 220.

similar to natural domains such as air,[146] international waters[147] and space,[148] i.e. not a non-legal domain, but rather a resource belonging to everyone and subject to appropriation by no one, characterised by collective governance autonomous from the territorial sovereignty model.[149] US Department of Defence (hereinafter DoD) seemingly followed the analogy stating that "the global common consists of international waters and airspace, space and cyberspace,"[150] yet has by now abandoned the view. NATO claimed the same, stating that "The Global Commons comprise four domains: maritime, air, space and cyber."[151] However, there is no universally accepted definition regarding "global commons". Depending on the bias added by different actors, the definition provided is slightly different in each case. Most definitions that have been provided, however, share one common trait: they focus on natural resources that cannot be fully appropriated and are not under the control of one specific State.[152]

It is widely held that cyberspace "is not a physical place – it defies measurement in any physical dimension or time space continuum. It is a short-hand term that refers to the environment created by the confluence of co-operative networks of computers, information systems, and telecommunication infrastructures."[153] It is also characterised by anonymity and ubiquity.[154] Thus using high seas, international airspace or outer space as an analogy[155] seems

---

[146] Convention on International Civil Aviation. 07.12.1944. – www.icao.int/publications/Documents/7300_cons.pdf (15.04.2016).

[147] Convention on the Law of the Sea. 10.12.1982. – www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf (15.05.2016).

[148] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies. 19.12.1966. – www.unoosa.org/pdf/publications/STSPACE11E.pdf (15.04.2016). Like other *res communis* areas, the ozone layer is subject to collective governance. See Montreal Protocol on Substances that Deplete the Ozone Layer. 16.12.1987. – ozone.unep.org/pdfs/Montreal-Protocol2000.pdf (15.04.2016).

[149] D.B. Hollis. Re-Thinking Boundaries, p 135.

[150] US Department of Defence. The Strategy for Homeland Defense and Civil Support. – 2005, www.hsdl.org/?view&did=454976 (visited 20.03.2016), p 12.

[151] M. Barrett, D. Bedford, E. Skinner, E. Vergles. Assured Access to the Global Commons. – Supreme Allied Command Transformation, North Atlantic Treaty Organization, Norfolk, Virgina USA, 2011, www.alex11.org/wp-content/uploads/2013/01/aagc_finalreport_text.pdf (visited 01.04.2016), p 5.

[152] P.W. Franzese. Referenced work, p 15.

[153] T.C. Wingfield. The Law of Information Conflict: National Security Law in Cyberspace. Falls Church: Aegis Research Group 2000, p 17; W. Heintschel von Heinegg. Territorial Sovereignty and Neutrality in Cyberspace. – International Law Studies 2013, Vol. 89, p 123.

[154] G.L. Herrera has put forward that "global digital networks have the features they do – of placelessness, anonymity, and ubiquity – because of politics, not in spite of them." G.L. Herrera. Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space. – Prepared for the 47th Annual International Studies Association Convention March 22–25, 2006, kms2.isn.ethz.ch/serviceengine/Files/CRN/46419/ieventattachment_file/1443347D-7CD7-40E2-871D-33202AA7A91E/en/CISS-ETH_Herrera.pdf. (visited 13.04.2016), p 12.

[155] For an analysis on drawing analogies from space, airspace and high seas, see P.W. Franzese. Referenced work, pp 18-32.

tempting. Yet, the proposals to ground the regulation of cyberspace in the regulation of the rest of the global commons have failed to gather widespread support.[156]

Even though cyberspace shares some traits that are similar to the global commons, e.g. no one sovereign could assert authority over it, the lack of physical boundaries *per se* does not make it a global commons. Patrick W. Franzese has proposed that all existing global commons share five similarities, offering thereby a litmus test for cyberspace.

> "First, a global commons has a governing international treaty. Second, this treaty provides specific permissible uses and prohibitions of that global commons. Third, the global commons has boundaries and is definable. Fourth, nations have agreed to forgo, or at least leave unasserted […], claims of exclusive sovereignty over any portion of the global commons. Finally, no single state is capable of controlling the global commons. In other words, a global commons is not the absence of sovereignty but rather the presence of a shared global sovereignty.'[157, 158]

When trying to apply this test, it becomes clear that the characteristics are not applicable to cyberspace. It is not fully intangible, it rests on a man-made physical and clearly tangible construct[159] and uses all other global commons to function. For example, submarine cables are often laid across the high seas between Europe and the US. Wireless networks send signals through the air. Cyberspace has a physical technical infrastructure that is owned by States or private entities and is located in their territory, which is under State's sovereign control. There is no moment when bits, data or information moving from one computer to another are not on a network that someone owns, be it the State or the private sector, and that is physically located in a sovereign state. The sole exceptions might be undersea cables or satellite transmissions; however, the action still takes place on an owned facility where the

---

[156] Numerous scholars have claimed that cyberspace cannot be viewed as part of the global commons. See for example, D. Willson. A Global Problem. – Armed Forces Journal 2009, www.armedforcesjournal.com/a-global-problem/ (visited 01.04.2016); J.A. Lewis. Sovereignty and the Role of Government in Cyberspace. – Brown Journal of World Affairs 2010, Vol. 16. No. 2, p 56; K. Ziolkowski. General Principles, p 182; S.J. Shackelford. Managing Cyber Attacks in International Law, Business, and Relations. Cambridge: CUP 2014, pp 61-62; J.S. Nye Jr. The Regime Complex for Managing Global Cyber Activities. – Global Commission on Internet Governance 2014, p 6.

[157] P.W. Franzese. Referenced work, p 17.

[158] Another test is offered by Benedikt Pirker, who claims that when it comes to cyberspace, (1) there is no 'tradegy of the commons', (2) there are no common rules and they cannot be effectively enforced in cyberspace, (3) infrastructure of cyberspace remains subject to private property rights. Thus, cyberspace cannot be seen as part of the global commons. B. Pirker. Territorial Sovereignty and Integrity and the Challenges of Cyberspace. – K. Ziolkowski (ed.). Peacetime Regime for State Activities in Cyberspace. Tallinn: NATO CCD COE Publications 2013, p 195.

[159] J.A. Lewis. Sovereignty and the Role of Government, p 63.

owner is subject to some country and its laws.[160] Thus, besides the physical information infrastructure, there are no accepted boundaries in cyberspace.[161] Pointing at cyberspace will be a daunting task for any actor in the field. Furthermore, the mere fact that part of cyberspace is intangible does not mean States have waivered their claims of sovereignty in that space. Similarly, if States have not chosen to assert sovereign control in the given domain or are not capable of doing so due to lack of capabilities or digital divide, it does not mean cyberspace is not or could not be covered by sovereignty. Lastly, there are no common rules established, since States cannot reach a consensus on the core questions, one of them being sovereignty. Similarly, there is no treaty governing the domain and States have not agreed on permissible and prohibited uses of cyberspace. The work done by the three UN GGE's in 2010, 2013 and 2015 aims at establishing responsible State behaviour in cyberspace, yet is largely political and States have shown no interest in designating cyberspace as a global commons. Essentially the Group has not established any effectively enforceable rules for governing cyberspace (UN GGE work is elaborated in Chapter 4.2.1.).

If cyberspace were to be considered a global commons, it would clearly not only distort the essence of real global commons and discount the role of States in governing them[162] but also undercut national and international security. Given the growing level of State interests and the search for technical and policy solutions to extend their control in cyberspace, an interpretation where no State can claim and protect their sovereignty in cyberspace is not feasible. It would lead to a situation, where no amount of interference within cyberspace would amount to an intervention,[163] taking effectively away the opportunity of States to protect themselves and assert their rights under international law. Thus, it is a general consensus that sovereignty applies to cyberspace[164] and the current thesis adopts this view going forward.

[160] J.A. Lewis. Sovereignty and the Role of Government, p 63.
[161] For a broader discussion on boundaries in cyberspace see, D.B. Hollis, Rethinking Boundaries.
[162] P.W. Franzese. Referenced work, p 10.
[163] J.A. Lewis, Sovereignty and the Role of Government, p 56; D. Midson. Geography, Territory and Sovereignty in Cyber Warfare. – H. Nasu, R. McLaughlin (eds.). New Technologies and the Law of Armed Conflict. The Hague: T.M.C. Asser Press 2014, p 88.
[164] See UNGA. UN GGE 2013 Report, para 20; UNGA. UN GGE 2015 Report, para 27. Both reports stated that State sovereignty and principles flowing from sovereignty apply to State conduct of ICT-related activities.

3.3. Cyberspace and territorial sovereignty

Sovereignty is considered a cornerstone of international law and international politics. Yet, the meaning of the term has provided a topic of debate for centuries[165] and is contested once again in the context of cyberspace.[166] Walter B. Wriston predicted in the end of 1980s that new technology would eventually rewrite old concepts of sovereignty as well as change national objectives. However, the shift in the power structure seen in the 1980s[167] was not a novelty but just another wave of change brought about technology's impact on State-on-State relations, altering the balance of power between States.[168]

As discussed, cyberspace is not considered a global commons as if now.[169] Thus, States are and will remain sovereign even in cyberspace, where there is *de facto* nor physical territory nor a tangible domain. Some scholars are of the opinion that a definition of sovereignty grounded in territory is ill suited for discussions surrounding cyberspace and cyber operations,[170] however, that is not necessarily so. Essentially, sovereignty in cyberspace, or as some call it "cyber sovereignty", is the extension of territorial sovereignty.[171] Taking into consideration the architecture and infrastructure of cyberspace, it becomes clear that States may *de facto* effectively exercise sovereign control over the information infrastructure physically located in its sovereign territory and activities originating therefrom. The State or corporations own the terrestrial, underwater and outer space infrastructure.[172] At the same time, it might be difficult to exercise sovereignty with regard to information architecture due

---

[165] See for example Saint Augustine. The City of God, translation, V.J. Bourke *et al*. New York: Doubleday 1958, p 88; J. Austin. The Province of Jurisprudence Determined and the Uses of the Study of Jurisprudence. Isaiah Berlin, Stuart Hampshire, Richard Woolheim (eds.). London: Weidenfeld and Nicolson 1954, pp 191–361; T. Hobbes. Leviathan or The Matter, Form, and Power of a Commonwealth, Ecclesiastical and Civil. R. Tuck (ed.). Cambridge: CUP 1991, pp 121–129; J. Locke. Two Treatises of Government. T.I. Cook (ed.). New York: Hafner Press 1947, p 105.

[166] See E.T. Jensen. Cyber Sovereignty, footnote 9 and 10.

[167] IISS. Dossier, p 29 ff.

[168] W.B. Wriston. Technology and Sovereignty. – Foreign Affairs 1988, Vol. 67, p 73.

[169] That does not mean that States could not agree to declare it a global commons some time in the future.

[170] For example Gary D. Brown has stated that: "There is no universally agreed definition [for sovereignty], but considerations of international sovereignty revolve around the recognition of a government's right to exercise exclusive control over territory, and this definition is ill suited for cyber discussions. For convenience we might refer to "the geography of cyberspace," but I challenge you to point to cyberspace. Although cyberspace is all around us, when trying to point at it you will be as unable to as the Square in [Edwin] Abbott's Flatland was to point to "up." […] [I]n any meaningful sense of the word, cyber lacks geography." G.D. Brown. The Wrong Questions About Cyberspace, pp 225–226.

[171] However, for example Brown is of the opinion cyber activities are "simply different than traditional physical activities and for this reason, cyber sovereignty is by its nature less complete than traditional sovereignty'. *Ibid,* pp 226–227.

[172] J.E. Kastenberg. Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law. – Air Force Law Review 2009, Vol. 64, p 64.

to its intangible nature.[173] Another controversial question is data sovereignty, i.e. to what extent can States control the flow of the data both within and across their borders, taking into account that it prevents the productive and efficient use of the Internet for users.[174] Technically, States can exercise jurisdiction over data and information that is circulated around cyberspace and networks at the point of delivery and the point of reception or when information crosses through infrastructure that falls within its territory.[175]

While all previously mentioned does not mean that any State may claim sovereignty over the entirety of cyberspace *per se*, States can exercise control over the infrastructure, i.e. physical components, situated in their "land territory, internal waters, territorial sea, archipelagic waters, or national airspace".[176] Furthermore, whilst the infrastructure is inherently part of the global Internet, a State will not thereby waiver its right to exercise jurisdictional or sovereign authority over the infrastructure.[177] Even though cyberspace definitely challenges States' ability to technically control trans-border movements, deriving from the notion of sovereignty, States can control access and egress from their territory and according to Wolff Heintschel von Heinegg that also applies to all forms of communications.[178] Moreover, States, for example the USA, have continuously emphasised their right to exercise control over and protect their information infrastructure against trans-border interference and assert authority over cyber activities on their territory.[179] Therefore, as cyberspace has a physical as well as a virtual component, where activities do not always manifest in physical world, they still have real effects on other spaces, humans and institutions.[180] Thus, States can exercise jurisdiction within their territory over cyber infrastructure located on its territory and over cyber activities that have been engaged in thereon.

Another important implication of territorial sovereignty in the context of cyberspace is its relative nature, which aims to protect the territorial sovereignty and integrity of other States. As stated by PCA already in in the beginning of the 20th century, sovereignty embodies rights

---

[173] M.N. Schmitt. Tallinn Manual, p 15; W. Heintschel von Heinegg. Legal Implications of Territorial Sovereignty in Cyberspace. – C. Czosseck, R. Ottis, K. Ziolkowski (eds.). 2012 4th International Conference on Cyber Conflict, Proceedings. Tallinn: NATO CCD COE Publications 2012, p 8.
[174] J. De Jong-Chen. Spotlight on Cyber V: Data Sovereignty, Cybersecurity and Challenges for Globalization. – Georgetown Journal of International Affairs, 12.10.2015, journal.georgetown.edu/data-sovereignty-cybersecurity-and-challenges-for-globalization/ (visited 15.04.2016).
[175] N. Tsagourias. The Legal Status of Cyberspace, p 19. S. Kanuck. Sovereign Discourse on Cyber Conflict Under International Law. – Texas Law Review 2010, Vol. 88, No. 7, pp 1273-1575.
[176] M.N. Schmitt. Tallinn Manual, p 16.
[177] W. Heintschel von Heinegg. Legal Implications of Territorial Sovereignty, p 14.
[178] *Ibid*, p 8.
[179] *Ibid*, p 10; E.T. Jensen, Cyber Sovereignty, p 295; See for example US Department of Defense. The Department of Defense Cyber Strategy. – April 2015, www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (visited 01.04.2016).
[180] N. Tsagourias. Legal Status of Cyberspace, p. 18.

as well as responsibilities, especially the "obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability in peace and in war."[181] Relative nature, as was implied by the PCIJ, suggests that the extent of international rights and obligations is different State by State, depending on its international relations. The same was affirmed in the separate opinion of Judge Alvarez in the *Corfu Channel* case in 1949, where he stated, "By sovereignty, we understand the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other States, and also in its relations with other States. Sovereignty confers rights upon States and imposes obligations on them".[182] Thus, territorial sovereignty does not mean only the right to exercise control over a certain territory, but includes also as a corollary principle the respect for territorial integrity, i.e. the right to be free from interference and the duty to avoid interference with another State's territory.[183] When sovereignty has been established, States that are exercising their authority in cyberspace are on the one hand entitled to be free from intervention but on the other hand, must prevent possible breaches of another State's territorial integrity originating from its territory. Therefore, States must accept the obligations that come with the assertion of that authority. Besides the actual effective control over certain territory and the right to be free from interference, territorial sovereignty includes also political independence of a State, which ought to allow the State to pursue economic, social and cultural development without coercion.[184]

While it is clear that there is no possibility to establish a fixed limit of sovereignty based on States' capabilities, such as the original three-mile limit of the territorial sea,[185] cyberspace is more territorial than probably thought, whilst still maintaining its non-territorial characteristics. The partly intangible nature does not restrict States from exercising sovereign control over the infrastructure located in their territory and that has two distinct implications. Firstly, the cyber infrastructure located in the State is subject to legal and regulatory control by the State. Secondly, regardless of whether the infrastructure is owned by the government or private entities, protection deriving from State's territorial sovereignty protects such infrastructure from interference by other States.[186] The opponents of applying the concept of

[181] PCA. Island of Palmas, p 839.
[182] ICJ, Corfu Channel, p 43, separate opinion of Judge Alvarez.
[183] B. Pirker. Referenced work, p 191.
[184] *Ibid.*
[185] Historically the limit of sovereignty was the amount of territory the State was thought to be able to protect. The three-mile limit on territorial seas was said to have been chosen, because it was the range of a shore-based cannon. Nowadays, the breadth of the territorial sea is 12 nautical miles. H.S.K. Kent. The Historical Origins of the Three-Mile Limit. – American Journal of International Law 1954, Vol. 48, No. 4; UNCLOS, Article 3.
[186] M.N. Schmitt. Tallinn Manual, p 16.

territorial sovereignty to cyberspace often note that it is such a different space from all known natural spaces that it would need its own regulation.[187] The argument could be made that old laws cannot protect, provide for the effective management and restrict abusive uses in this man-made domain. However, as Judge Alvarez noted already in 1949, exercising and asserting sovereignty can take different forms in different spheres.[188] As such, sovereignty is a bundle of rights and obligations that allows for interpretative elasticity, and can therefore, be applied in the context of new technologies. The UN GGE 2013 Report supported the view by concluding that State sovereignty and international norms and principles that flow from sovereignty, apply to State conduct of ICT-related activities and to jurisdiction over ICT infrastructure within a State's territory.[189]

If one were to ask a Koskenniemi-esque question, "What is the use of sovereignty today in cyberspace?"[190] the answer would be two-fold. On the one hand, cyberspace has provided States an additional domain where to conduct their defensive and offensive activities, develop strategic capabilities as well as compete, leading to States having a valid interest in exercising control in cyberspace. Sovereign equality offers States the freedom to do as they choose. Each State is free to develop or not to develop their cyber capabilities according to their resources and interests. However, everyone has the opportunity to do so, thus realising the principle of sovereign equality. At the same time, sovereignty offers boundaries that otherwise would be lost in a partly intangible domain, protecting States from unlawful interferences and providing remedies if breached. However, as Gary D. Brown notes, "[p]owerful cyber nations do what they can to defend their own Internet infrastructures, with some success. Weaker nations suffer what they must in cyberspace. Victim nations are often, undoubtedly, never even know their Internet infrastructure is being used for foreign espionage or as a staging point for cyber criminals, hacktivists and foreign government actors."[191] Even though we are unable to set physical boundaries to sovereignty, putting it that way illustrates that cyber sovereignty "extends exactly as far as each country can make it".[192]

On the other hand, as cyberspace can be considered increasingly Hobbesian, sovereignty and State control offer somewhat of a stability needed in such a domain. The original vision

---

[187] See Chapter 3.1. on cyberlibertarianism.
[188] ICJ. Corfu Channel, separate opinion of Judge Alvarez, p 43.
[189] UNGA. UN GGE 2013 Report, paras 19-20.
[190] See Koskenniemi. What Use for Sovereignty Today?
[191] G.D. Brown. The Wrong Questions About Cyberspace, p 228. Inspired by Thucydides. History of the Peloponnesian War. The Melian Dialogue. – lygdamus.com/resources/New%20PDFS/Melian.pdf (visited 15.04.2016). "[T]he strong do what they have the power to do and the weak accept what they have to accept."
[192] G.D. Brown. The Wrong Questions About Cyberspace, p 228.

presented by the online freedom activists and cyberlibertarians decades ago, where cyberspace ought to be free from State and regulatory intervention, is not sustainable taking into account the exponentially growing amount of activities undertaken in said space. Simply put, it would lead to a chaos. Waiting for a social contract to form between all the different actors conducting activities in cyberspace without State interference is either not feasible at all or takes a very long time to form.[193] Lengthy non-regulation, however, would have serious implications for international and national security. At the same time, it would be naïve to hope that States as the main actors in the international system would relinquish their claims in a domain, where strategic advantage could benefit the State on multiple levels. Thus, it is apt to point out that the reports of "the death of sovereignty are much exaggerated: not only is the state free to exercise its sovereignty, the protection of its interests practically requires it."[194] It is thus the concept of sovereignty and the principles deriving therefrom that are the foundation for determining the legality of the conduct of States in cyberspace.

[193] J.A. Lewis. Sovereignty and the Role of Government, p 63.
[194] J. Crawford, M. Koskenniemi. Cambridge Companion to International Law, p 132.

4. Exercising sovereignty in cyberspace

While it has been claimed that the limits to the sovereignty of States are increasingly growing in quantity and in depth,[195] cybersecurity and national security may be considered few of the areas, where traditional notions of sovereignty are soaring and blossoming. Academics and experts alike focus mostly on whether sovereignty as a concept applies to cyberspace in the first place.[196] In parallel, as will be explained, States are already exercising sovereignty in cyberspace for their benefit without having agreed upon the rules for the "game", i.e. how international law applies in cyberspace. In order to provide legal certainty and clarity, it is of outmost importance to analyse how States exercise sovereignty in cyberspace.

The State practice shows that States are exercising their sovereign rights in the domestic level through their exclusive jurisdiction as well as in international in normative discussions pertaining to cyberspace. Furthermore, States can make the sovereign decision of non-compliance, i.e. decide to not respect the sovereignty of other States. International law at the hands of scholars look different than international law in the hands of States.[197] Low-intensity cyber operations have offered States who have the appropriate capabilities the loophole they need to exert power and achieve their strategic or tactical goals without crossing the threshold of the use of force according to the UN Charter Article 2(4). What are considered below the threshold breaches of sovereignty and how does the principle of non-intervention apply to offensive cyber operations conducted by States has not as of date been agreed upon, which reflects also in the State practice.[198] The unclear legal regulations and States' growing capabilities in a highly contested environment create perfect conditions for an organised hypocrisy, where long-standing established rules have been ignored numerous times.

The legal concept of sovereignty cannot be divided from the power politics. Although there are some, who argue that "sovereignty is essentially a political and not a legal concept".[199] Others contest the view by contending that "sovereignty is essentially a political and not a

---

[195] L. Condorelli, A. Cassese. Referenced work, p 14.
[196] For example, P.W. Franzese. Referenced work.
[197] E. Tikk-Ringas. Presentation at UNIDIR International Security Cyber Issues Workshop Series: The Application of International Law in the Context of International Cybersecurity. – 19-21.04.2016, www.unidir.org/programmes/emerging-security-threats/international-security-cyber-issues-workshop-series/international-security-cyber-issues-workshop-series-the-application-of-international-law-in-the-context-of-international-cybersecurity (visited 25.04.2016).
[198] Cyber Policy Institute. State Practice and International Law in Cyberspace: A Study of Major Cyber Incidents and Applicable Law. – forthcoming at the Conference on State Practice and the Future of International Law in Cyberspace, 05.05.2016.
[199] G. Leibholz. Sovereignty and European Integration: Some Basic Considerations. – G. Leibholz (ed.). Politics and Law. Leiden: Sijthoff 1965, p 217.

legal concept".[200] Policy considerations are an integral part of the international legal process[201] and the exercise of sovereignty can be highly political, strategic and calculated. States are not only free to exercise their sovereignty, but protecting and promoting their interests in the cyber discourse requires it. As sovereignty is "the very guarantor of the unstable union of politics and law",[202] the present chapter analyses is based on State practice, how States exercise their sovereign rights in cyberspace.

4.1. Internal sovereignty

As a general rule, States assert legal authority regularly over actors and activities taking place in cyberspace within the confines of their territory. States can exercise jurisdiction based on the physical location of the networks or servers employed or the physical location where the effects of the activity occur.[203]

However, exercising sovereignty vis-à-vis cyberspace is in different stages of maturity among States. Some, as is the case of certain States in Africa, are only developing the necessary local physical infrastructure to be connected to the global network of networks. Even if such infrastructure exists, maintaining its security has proven to be a challenge to a number of States. Different levels of maturity in the field will likely be the trend also in the future. However, when it comes to power players in the field, their exercise of exclusive jurisdiction is carried by two different ideologies among the major cyber powers – the US, Russia, and China. From liberal to more restrictive, the exercise of sovereignty in cyberspace is often characterised by multi-polarisation among respective powers.

The US is generally the proponent of a more open, cooperative system without strict borders that would reflect in cyberspace *per se*. Adopting a more liberal approach, the US is committed to an "open, secure, interoperable, and reliable Internet that enables prosperity, public safety, and the free flow of commerce and ideas".[204] Carried by its hegemonic nature and possibly the aspiration to expand its cyber sovereignty, the US promotes a global and open cyberspace, where multiple stakeholders participate in governance issues without content restrictions.[205] US, as one of the founding States of the global information

[200] G. Leibholz. Referenced work, p 217.
[201] R. Higgins. Problems and Process: International Law and How We Use it. Oxford: Clarendon Press 1994, p 5.
[202] H. Kalmo, Q. Skinner. Referenced work, p 3.
[203] D.B. Hollis. Re-Thinking Boundaries, p 134.
[204] US DoD. Cyber Strategy, p 1.
[205] D.B. Hollis. Re-Thinking Boundaries, p 134.

infrastructure,[206] has shown high adaptability to the changes brought about by the fast development of technology. In the light of their "new normal" doctrine, put forward by Michael Daniel, the special assistant to the president and White House cybersecurity coordinator, their political approach recognises that persistent intrusions, violations of privacy, thefts of business information and denial of service on multiple levels is the reality that every actor must endure.[207]

As polar opposites, Russia and China, who are emphasising sovereignty as the greatest value in the international system and the foundational principle of international law,[208] are firm believers in the fact that the State alone can and should control access and egress from State's territory. Aspirations of establishing a cyber-Westphalia are in this context not exaggerations. Both of the States are in the process of asserting their technological sovereignty by designing "national Internets", which are connected to the rest of the world only in protected and channelled ways[209, 210] allowing the State to control the connection as well as the content.[211] By defining a ".ru" internal network or "internal cyberspace" only open to Russian citizens[212] Russia effectively tries to ensure their interests by exerting maximum possible control. Even though it has made efforts to reduce the dependence on foreign suppliers,[213] the technology that Russia uses is still similar to that used by many other States, the logical layers of it will be adapted to allow the control the State needs through filtering, permitting or blocking what

---

[206] IISS. Dossier, p 19 ff.

[207] M. Daniel. 007 or DDoS: What is Real World Cyber? – 28.02.2013. Remarks as prepared for delivery by special assistant to the president and White House cybersecurity coordinator. RSA Conference USA 2013 San Francisco.

[208] See further L. Mälksoo. Russian Approaches to International Law, p 100 ff. X. Hanqin. Chinese Perspectives on International Law: History, Culture and International Law. The Hague: Hague Academy of International Law 2012, p 68 ff.

[209] C. Demchak, P. Dombrowski. Cyber Westphalia: Asserting State Prerogatives in Cyberspace. – Georgetown Journal of International Affairs: International Engagement on Cyber III 2013/2014, p 32. As Panayotis A. Yannakogeorgos has stated, "The result has been the emergence of alternative national networks that essentially create alternate domain name systems for in-country use, allowing for censorship of content and stifling the productivity of the current Internet topology. China is one country that has implemented this on a national scale, and Iran is closely following suit." P.A. Yannakogeorgos. Internet Governance and National Security. – Strategic Studies Quarterly Fall 2012, p 119.

[210] H. Zhe, T. Shi. China Security Bill Calls for Protecting 'Cyber Sovereignty'. – Bloomberg Technology, 09.05.2015, www.bloomberg.com/news/articles/2015-05-08/new-china-security-bill-calls-for-protecting-cyber-sovereignty- (visited 10.04.2016).

[211] For example, Russia banned Twitter twice in 2014. First in May so that tweets stemming from Ukrainian nationalist groups would no longer reach Russian users. Secondly in July, banning access to a hackers' groups Twitter account that had previously leaked several internal Kremlin documents. B. Ries. Twitter Blocks Pro-Ukrainian Political Account for Russian Users. – Mashable, 19.05.2014, mashable.com/2014/05/19/twitter-blocks-account-russia/#Kl0O_zOuIZq9 (visited 20.04.2016); K. Rothrock. Twitter "Blocks" Access to Russia's Most Infamous Hackers. – Advox, Global Voices, 28.07.2014, advox.globalvoices.org/2014/07/28/twitter-blocks-access-to-russias-most-infamous-hackers/ (visited 20.04.2016).

[212] C. Demchak, P. Dombrowski. Referenced work, p 32.

[213] S. Charney, E.T. Werner. Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust. – Microsoft, 26.07.2011, 6, www.microsoft.com/en-us/download/details.aspx?id=26826 (visited 10.04.2016).

the State defines as its prerogatives.[214] As such, Russia is trying to enact rules of data sovereignty and residency, which would allow firstly, to apply government control over all data collected within a country and secondly, to establish a mandatory data storage location and efficiently contain data flow within its borders.[215] First steps towards the restrictive data flows have already been made. In July 2014 Russia passed a law coming to force in September 2016 mandating that cloud-service providers engaging in business in Russia must hold the data they collect in databases located within the territory of the Russian Federation.[216] It is believed to be a response to the June 2013 Edward Snowden revelations, when classified information about US government's global surveillance programs was leaked, making States, among others also Brazil,[217] reconsider or strengthen their position on sovereignty in cyberspace and especially data sovereignty.[218]

Similarly, China puts forward that every State should be able to independently choose their own path of cyber development, model of cyber regulation and Internet public policies,[219] which is consistent with their foreign policy approach deriving from the Five Principles of Peaceful Coexistence.[220] The principles emphasise very strongly respect for State sovereignty and the right to make decisions as a State without outside interference or scrutiny. Thus, their latest security bill calls for the protection of cyber sovereignty,[221] which includes also purging most foreign technology from critical infrastructure, such as banks and military, but also from State-owner enterprises.[222] Free flow of information should be guaranteed under the premises that national sovereignty as well as security is safeguarded.[223] To that extent, Chinese

---

[214] C. Demchak, P. Dombrowski. Referenced work, p 32.
[215] J. de Jong-Chen. Referenced work.
[216] *Ibid*. Russian Duma. Bill number 553424-6: On Amendments to Certain Legislative Acts of the Russian Federation (to clarify the processing of personal data in information and telecommunications networks). – asozd2.duma.gov.ru/main.nsf/%28Spravka%29?OpenAgent&RN=553424-6&02 (visited 10.04.2016).
[217] B. Brooks, F. Bajak. Brazil Looks to Break Free from U.S.-Centric Internet. – TPM, 17.09.2013, talkingpointsmemo.com/idealab/brazil-looks-to-break-from-u-s-centric-internet (visited 20.04.2016).
[218] J. de Jong-Chen. Referenced work.
[219] Remarks by H.E. Xi Jinping, President of the People's Republic of China at the opening ceremony of the Second World Internet Conference. – 16.12.2015, www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml (visited 16.04.2016).
[220] 139. Agreement between the Republic of India and the People's Republic of China on trade and intercourse between Tibet region of China and India (Panchseel Treaty). 22.04.1954. – treaties.un.org/doc/publication/unts/volume%20299/v299.pdf (15.04.2016). The treaty establishes five main principles that the agreement is based on, which up to date the Chinese foreign policy adheres to. X. Jinping. Address by H.E. Mr. Xi Jinping President of the People's Republic of China At Meeting Marking the 60th Anniversary Of the Initiation of the Five Principles of Peaceful Coexistence: Carry forward the Five Principles of Peaceful Coexistence to build a better world through win-win cooperation. – 28.06.2014, www.china.org.cn/world/2014-07/07/content_32876905.htm (visited 30.04.2016).
[221] H. Zhe, T. Shi. Referenced work.
[222] *Ibid*.
[223] UNGA. A/61/161. 18.07.2006. Developments in the Field of Information and Telecommunications in the Context of International Security, p 4.

government has controlled domestic access to content on the Internet since 2003 through the Great Firewall of China.[224] Through filtering Internet traffic through eight gateways that connect the Chinese Internet to the global Internet and configuring Internet routers at those gateways to block certain website addresses and keywords, the Chinese government effectively prevents information from entering China that it deems threatening to its own regime.[225] For example, China has banned since 2009 until present Twitter, all Google sites and platforms, including Youtube and Facebook[226] as a response to political protest after which private sector actors, such as Google, refused to cooperate with the government in its efforts to censor search results.[227] It goes to show that States, such as China,[228] are asserting their sovereign right to control what takes place within their territory quite aggressively, interpreting the right of States to control access and egress from its territory as broadly as possible, which is mostly at odds with the concept of freedom of information.

Juxtaposed to the US approach, Russia as well as China prefer to exercise sovereignty in cyberspace rather defensively and restrictively. Since they are not at the level of technological sophistication and performance that the US technological supremacy in the field shows, the restrictive approach allows both States to create national and pursue for international normative environments that promote their views and aspirations. By retaining the possibility to disconnect from the global network and filter the content as deemed necessary, both States are effectively fighting one of their greatest online threats – internal dissident and anti-government writings disseminated on the Internet – through censoring information and limiting access to the Internet.[229] However, China and Russia are not the only ones to use Internet bans to curb the mushrooming of dissent within the country. Several States, for example Turkey, North Korea, Vietnam, Libya, Pakistan, Egypt, Iran, Syria, Iraq, Congo, Bangladesh[230] have banned certain services for a shorter or a longer period of time for

---

[224] X. Qiang. How China's Internet Police Control Speech on the Internet. – Radio Free Asia, 24.11.2008, www.rfa.org/english/commentaries/china_internet-11242008134108.html (visited 20.04.2016).
[225] M.C. Libicki. Crisis and Escalation in Cyberspace. Santa Monica: RAND Corporation 2012, p 100. C. Lotrionte. State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights. – Emory International Law Review 2012, Vol. 26, p 846.
[226] D. Liebelson. Map: Here are the Countries the Block Facebook, Twitter, and Youtube. – 28.03.2014, www.motherjones.com/politics/2014/03/turkey-facebook-youtube-twitter-blocked (visited 20.04.2016). See also Google Transparency Report. Recent and ongoing disruptions of traffic to Google products. – www..google.com/transparencyreport/traffic/#expand=CG (visited 20.04.2016).
[227] C. Lotrionte. State Sovereignty, p 848.
[228] For a broader discussion on Chinese views on cybersecurity, see, J.R. Lindsay, T.M. Cheung, D.S. Reveron. China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain. Oxford: OUP 2015.
[229] C. Lotrionte. State sovereignty, p 847. Generally for an overview of the practice of global Internet filtering, see, R. Deibert, J. Palfrey, R. Rohozinski, J. Zittrain. Access Denied: The Practice and Policy of Global Internet Filtering. Cambridge: MIT Press 2008.
[230] Cyber Policy Institute. Table: Internet Bans. – 20.04.2016.

numerous political reasons, such as curbing the dissemination of opposition views ahead of elections or taming protest.[231] Technology, freedom of information and social media enable the widespread dissemination of dissenting ideas.[232] The most prominent example would be during the so called Arab Spring, where dissident groups used social media to coordinate their activities and Algeria, Tunisia, Egypt, Cameroon, and Malawi reacted with a social media ban.[233]

For other countries, the monopoly of control, autonomy and even "territoriality" rest in using and relying on indigenous technologies. For Germany, the importance of relying on German-only technologies reflects a form of control.[234] Similarly, Chinese Indigenous Innovation policies, require an indigenous innovation product catalogue be used for its government procurement and implementing a Multi-Level Protection Scheme (MLPS), which requires product developers and manufacturers to be Chinese citizens or legal person, and product core technology and key components must have independent Chinese or indigenous intellectual property rights.[235] Indian 2013 National Cyber Security Policy recognises risks accompanying technology from foreign suppliers,[236] but instead of excluding specific products, India focuses on Indigenous Innovation policies and thus, placed restrictive regulations on government-purchased technology through adopting Preferential Market Access (PMA) rules that favour domestic ITC suppliers and domestically manufactured electronic goods for government purchase instead of foreign ones.[237] Interestingly enough, contrary to its mostly prevalent open approach, the US made a similar decision, when it banned Huawei and ZTE technology from its governmental systems, claiming that they pose a national security threat due to the Chinese government's influence on the companies.[238]

---

[231] See also, Google Transparency Report. Referenced work.
[232] For example, Russia's Security Council has stated, "Advanced technologies of 'color revolutions' applied to removal of political regimes unwanted but the USA will become more and more widespread and with high probability will be used against Russia." Security Council of the Russian Federation. On the National Security Strategy of the United States of America. – 25.03.2015, www.scrf.gov.ru/news/865.html (visited 20.04.2016).
[233] OpenNet Inititive. Social Media Filtering Map. – opennet.net/research/map/socialmedia (visited 20.04.2016).
[234] C. Demchak, P. Dombrowski. Referenced work, p 32.
[235] D. Ernst. Indigenous Innovation and Globalization. The Challenge for China's Standardization Strategy – UC Institute on Global Conflict and Cooperation, East-West Center; June 2011, pp 36-37.
[236] India's Ministry of Communications and Information Technology. Department of Electronics and Information Technology. National Cyber Security Policy. – 02.07.2013, deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf (visited 10.04.2016).
[237] 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. – 05.10.2012; www.dot.gov.in/sites/default/files/5-10-12.PDF (visited 10.04.2016).
[238] US Congress House of Representatives. Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE. – 08.10.2012, pp 1-7,

Thus, States exercise cyberspace control within their territory in multiple different ways: both *de facto* and with reference of their understanding of *de jure*. Whether the approach is more liberal and open or defensive and restrictive depends on State's general politics towards international community.

4.2. International norms development in the field of cybersecurity

The novelty of cyberspace has some scholars calling for new norms or reforms to the existing international legal framework[239] in order to face the multitude of threats the said space enables. Continued calls for a "new, comprehensive legal framework" that is needed to address cyberattacks[240] have led to calls for an international treaty that would be similar to the Outer Space Treaty (1967)[241] or the UN Convention on Law of the Sea (1982),[242] which would regulate the use of ICTs, establish the limits of sovereignty and prohibit hostile actions in cyberspace.[243] However, in a multipolarised world, where different ideologies, doctrinal interpretations and strategic aspirations of major cyberpowers, such as USA, Russia and China, conflict, reaching a consensus agreement regarding any of the topics put forward is difficult an international treaty and the successful implementation thereof seems rather unlikely.[244]

However, it is one of State's sovereignty's attributes to be able to bind itself with international obligations. A state bound by treaties and international obligations is not considered an encroachment on its sovereignty, but an effect of it.[245] As the search for international cybersecurity norms, existing international law interpretations and a possible treaty are continuing, at some point States have to make the sovereign decision whether to bind themselves or not. Through exercising their sovereignty in this regard, States can influence where the consensus on the contested matters pertaining to cyberspace is formed. At the

---

intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf (visited 15.04.2016).

[239] Joyner and Lotrinote note that "Given such realities, international legal rules must be dramatically adapted if new cyberspace technologies are to be regulated, or even managed, in their increasingly pervasive transnational applications." C.C. Joyner, C. Lotrionte. Referenced work, p 826. A. Krutskikh, A. Streltsov. International Law and the Problem of International Information Security. – International Affairs 2014, Vol. 60, No. 6, p 64 ff.

[240] O.A. Hathaway, et al. The Law of Cyber Attack. – California Law Review 2012, Vol. 100, No. 1, p 821.

[241] Outer Space Treaty. 19.12.1966.

[242] UNCLOS. 10.12.1982.

[243] D. Brown. A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict. – Harvard International Law Journal 2006, Vol. 47. No. 1, p 179; S.J. Shackelford. From Nuclear War to Net War; J. Barkham. Referenced work; M. Hildebrandt. Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace. – University of Toronto Law Journal 2013, Vol. 63, No. 2, p 224.

[244] See also M.C. Waxman. Referenced work, pp 425–426.

[245] PCIJ. S.S Wimbeldon, p 25.

moment, the discourse on norms for cyberspace as well as any interpretation of existing international law is a constant battle between the main stakeholders: China, Russia and the US, each of whom wish to promote their value systems in line with their political ambitions, strategic calculations, habits and traditions.[246]

The following chapter presents two influential dialogues pertaining to the matter of international law and cyberspace. Firstly, UN GGE is an expert group tasked with examining the existing and potential threats, the application of international law and possible cooperation measures within cyberspace. Secondly, the discussion that is revolving around the adoption of a new treaty, which is lead largely by members of the Shanghai Cooperation Organization (hereinafter SCO) in the form of a proposed Code of Conduct.

4.2.1. United Nations Group of Governmental Experts

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 1998 letter to UN Secretary-General Russia condemned the creation of information weapons and warned of the threat of information war. It also 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 States' internal affairs, respect for human rights and freedoms, arms race pertaining to 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.[247] As it was one of the first initiatives of its kind, Russia proposed that the topic of international information security be substantively discussed at the United Nations.[248]

Thus, the Russian resolution initiated the international cyber security dialogue at the UN. The following UNGA resolution, which was adopted without a vote,[249] 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

[246] IISS. Dossier, p 115.
[247] UN Disarmament Committee. A/C.1/53/3. For comprehensive overview, see IISS. Dossier, Chapter 8: Normative Approaches to Cyber Security.
[248] UN Disarmament Committee. A/C.1/53/3, p 2.
[249] UN Office for Disarmament Affairs. GGE Information Security. – www.un.org/disarmament/topics/informationsecurity/ (visited 20.04.2016).

and telecommunications systems and help to combat information terrorism and criminality.[250] The first substantial report of the UN GGE, which at the time brought together 15 States under the chair of Russia,[251] was adopted in 2010. It highlighted the threat landscape that States were facing elaborating on threats, risks and vulnerabilities as well as cooperative measures among States.[252] The 2013 UN GGE expanded substantially in the content-matter covered and became more explicit in the issues the group aimed to cover. The report spoke of existing and potential threats in the sphere of information security, cooperative measures to address them, including norms, rules or principles of responsible behaviour 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.[253] The 2013 Report affirmed the applicability of international law to cyber security,[254] which was at the time ground breaking. Whether or not cyberspace is subject to international law was a deeply political question and a wide range of States, including generally diverging China, Russia and the US, agreed on the notion.

The 2015 UN GGE report, which aimed to explain how international law applies to State ICT related activities, reiterated that State sovereignty and international norms and principles that flow from the notion of sovereignty apply to State conduct in cyberspace and to their jurisdiction over ICT infrastructure within their territory. Furthermore, the report specified quite laconically that in their use of ICTs, States must observe among others the principles of State sovereignty, sovereign equality and non-intervention in the internal affairs of other States.[255] The report was highly anticipated due to the ambition of the task at hand and the clarity it would have provided. It was hoped that deeper discussions and a larger group of States considering the issues would have moved the discourse of cybersecurity past its "infancy" stage. Yet it failed to deliver on the matter. The task – to explain the application of international law – was no doubt an extensive one. Even though, the report accepted the application of LOAC to cyberspace, the more burning question of how international law applies, still requires an answer.

---

[250] UNGA. A/RES/53/70, 04.01.1999. Developments in the field of information and telecommunications in the context of international security.
[251] IISS. Dossier, Table 8.1, p 116.
[252] UNGA. UN GGE 2010 Report.
[253] UNGA. UN GGE 2013 Report.
[254] *Ibid*, para 19.
[255] UNGA. UN GGE 2015 Report, para 27, para 28(b). The 2014/2015 UN GGE brought together a wider range of States as well, rising the amount of participants from 15 in previous two GGEs to 20 in the said group. IISS. Dossier, Table 8.1, p 116.

A consensus report with concrete instructions of how to apply existing concepts to cyberspace, which is inherently a dynamic environment, would have provided guidance and clarity for the future State practice. Even though we have moved away from considering it a Wild West, there is a lot of uncertainty and perplexity concerning questions of to what extent and how international law exactly regulates it. That in turn leads to State practice being far from consistent, which affects achieving consensus on fundamental matter to a large extent. For example, even though the determination of sovereignty in the areas of sea, air and outer space ultimately required an international regime, avid State practice influenced those emerging international solution.[256] This applies here as well. Even though the creation of a new regime is at the moment unlikely (see Chapter 4.2.2), yet not impossible, at first glace, the practice that States create influences at the minimum the interpretations States are going to agree or disagree upon.

The UN GGE process allows not only diverging cyber powers, but also other States, who are interested in fostering a dialogue on international law and cyberspace, to come together in order to discuss their views and work towards a consensus solution. The format pushes States to take the lead and responsibility on steering the international debate on the development of international law pertaining to cyberspace, which one day could result for example in a binding interpretation of matters at hand, in a separate treaty or a normative regime that would govern States' activities in cyberspace. For the main stakeholders in the process, that is China, Russia and the US, the group allows them to test their views, explain their value systems and find connections to likeminded States.

However, the other side of the process is far less optimistic. UN GGE is still highly politicised, where every decision is backed by political ambition and States' strategic calculations. One would only have to consider the fact that the group gathers only 15 to 20[257] States out of 193 countries in the world. It is not hard to see how it could be considered an elitist group, not reflecting the opinion of the international community writ large. This was further emphasised by Angela Kane, the UN High Representative for Disarmament Affairs at the Global Conference on Cyberspace 2015, where she noted that the 2013 UN GGE Report, which produced the conclusion that international law applies to cyberspace was accepted at the UNGA only lukewarmly. The report, which was ground breaking for the participants in the GGE as well as for the wider cybersecurity community, was not even supported by the

[256] P.W. Franzese. Referenced work, p 29.
[257] In the UN GGE 2016-2017 session 25 countries will participate.

larger international community.[258] Thus, it is a wise strategic move for the main stakeholders to keep the discourse going in the UN GGE, as odds are that their views would not gather a widespread support, if put on a vote on the UNGA. Secondly, it brings together States, such as the US and Russia, who look at the issues from a threat perspective. At the same time, it includes also States such as Ghana and Kenya, who see the problems from a development perspective. The possibility to find consensus, when the starting point is at the opposite direction is bound to be difficult. However, offering an avenue, where the discussion keeps going will most likely contribute to cultivating a global culture of cyber security as envisioned by the UN over two decades ago.[259]

4.2.2. The quest for a new treaty?

The topic of the necessity and viability of a new treaty catered solely for the regulation of cyberspace has been a contested issue for years. Academics have argued for the usefulness of a separate treaty regime,[260] whereas States have mainly argued that the international landscape is too premature for a comprehensive international agreement to govern international security.[261]

Two main stakeholders – the US and Russia, have long had differed views over the need for a treaty. The US 2011 International Strategy for Cyberspace, put forward by the Obama administration stated that the "development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behaviour – in times of peace and conflict – also apply in cyberspace."[262] While it is definitely true, that does not necessarily mean that the rules and principles would have to be applied in their traditional interpretation. The novel character of cyberspace, the vulnerability of information infrastructure and other "unique attributes of networked technology" might require

---

[258] A. Kane. Remark at the Global Conference on Cyberspace 2015 ICT4Peace Panel on Norms of International Peace and Security in Cyberspace. – 17.04.2015.
[259] UNGA. A/RES/57/239. 20.12.2002. Creation of a Global Culture of Cybersecurity; UNGA. A/RES/58/199. 23.12.2003. Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures.
[260] See footnote 238.
[261] K. Aiken, J. Woodall. Tallinn 2.0: cyberspace and the law. – The Strategist, Australian Strategic Policy Institute, 14.05.2015, www.aspistrategist.org.au/tallinn-2-0-cyberspace-and-the-law/ (visited 20.04.2016). Australia was the country to make the point at the Global Conference on Cyberspace 2015.
[262] The US President opined in the 2011 International Strategy for Cyberspace that the existing international law applies to cyberspace and essentially it is not of importance to create new norms. What is important is to clarify how the norms apply in cyberspace. The White House. President of the United States of America. International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World. – May 2011, www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (visited 20.04.2016), p 9.

clarification and reconsideration of *lex lata*.[263] The US approach goes to show that the US does not want to use their sovereign rights to bind themselves with an international treaty before it is absolutely necessary or beneficial for them. That is also consistent with its general practice vis-à-vis international treaties and other binding instruments. In a comparison analysis of major international law instruments, the US had accepted a total of 16 instruments, compared to Russia having accepted 18 and China respectively 24 fundamental international law treaties and instruments.[264] Moreover, there are few examples in the history, where the US has exercised its sovereign right to withdraw the consent of being bound to an international instrument. For example, the US withdrew the optional clause declaration[265] binding US with the ICJ jurisdiction, during the ICJ Nicaragua case, arguing that ICJ did not have jurisdiction.[266] Similarly, the US signed the Rome Statute[267] establishing the ICC, having been part of the negotiations. However, the signature was later suspended and the UN Secretary General was informed that the US recognised no obligation toward the Rome Statute and had no intention to become a party thereof.[268] Even though unusual, it still represented a valid exercise of State sovereignty and it is clear that the US has as of yet no intention to increase its obligations under international law pertaining to cyberspace in the form of a new treaty.

Whereas USA is of the position that existing international law norms are sufficient in order to address State activities in cyberspace,[269] Russia, China and a few other SCO Member States put forward in 2011 a proposal for a voluntary International Code of Conduct for Information Security regulating State behaviour in cyberspace. Indicating thus that the Sino-Russo thinking sees the need for additional special regulation of cyberspace. In 2015 the same circle of countries (with added supporters Kazakhstan and Kyrgyzstan) presented the UN Secretary-

---

[263] White House. International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World, p 9; Heintschel von Heinegg. Legal Implications of Territorial Sovereignty, p 10.
[264] N. Tocci (ed.) Who is a Normative Foreign Policy Actor? The European Union and its Global Partners. – Centre for European Policy Studies 2008, aei.pitt.edu/32609/1/48._Who_is_a_Normative_Foreign_Policy_Actor.pdf (visited 15.04.2016), pp 321-323.
[265] Statute of the International Court of Justice. 26.06.1945. – www.icj-cij.org/documents/?p1=4&p2=2 (visited 15.04.2016), Art 36(2).
[266] ICJ. 26.11.1984. Military and Paramilitary Activities in and Against Nicaragua (*Nicaragua. v. US*), Jurisdiction of the Court and Admissibility of the Application. ICJ Reports 1984.
[267] Rome Statute of the International Criminal Court. 17.07.1998. – www.icc-cpi.int/nr/rdonlyres/ea9aeff7-5752-4f84-be94-0a655eb30e16/0/rome_statute_english.pdf (15.04.2016).
[268] AMICC. Bush Approach to the ICC. Suspension of the Rome Statute Signature: The US Disengages. – www.amicc.org/usicc/bush (visited 10.04.2016).
[269] White House. International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World, p 9.

General with the revised version of the Code of Conduct.[270] The Codes of Conduct represent a strict enforcement of cyber sovereignty, which emphasised the government's legal right to enforce its own laws within its own borders and control the flow of data. In the UN GGE process, both Codes of Conduct have been noted, yet not substantially discussed or considered.[271] The possible reason could lie in the absolutist interpretation of the State and territorial sovereignty enshrined in the proposed Codes of Conduct. They also miss essential questions such as the use of proxies and the regulation of activities of non-State actors, and do not reflect the adequate level of protection of human rights, which does not sit well with the West. However, since a consensus on the basis of Codes of Conducts does not seem to be achieved any time soon, Russia and China have started to forge a bilateral relationship pertaining to cybersecurity, leaving the US as one of the major cyberpowers to the sidelines.[272]

Governments as well as other actors alike are employing ICTs and other high technologies in pursuit of their strategic interest. Since 1998, leading powers – most notably the US, Russia and China – have discussed the issue of applicability of international law to the development and use of ICTs and "cyber security" in different venues.[273] National positions and expert contributions to the theme have failed to provide an inclusive, holistic, theoretically grounded and critical discourse on the subject.

In general, the international dialogue on the matter at hand is dominated by few cyber and normative powers with strong national interests in the issue. Leading powers differ in their underlying assumptions as to whether proliferation and dissemination of ICTs is to be regarded as an opportunity or a threat. The majority of countries lack strategic understanding and the role as well as implications of ICTs are still emerging in most countries. Due to technology-heavy emphasis, the discourse of international norms development pertaining to

---

[270] UNGA. A/66/152. 15.07.2011. Developments in the field of information and telecommunications in the context of international security, reply from the US Government. Cf. UNGA. A/55/359. 14.09.2011. 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; UNGA. A/69/723. 13.01.2015. Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.

[271] UNGA. UN GGE 2013 Report, para 18. UNGA. UN GGE 2015 Report, para 12.

[272] Worldcrunch. China and Russia Forge Cybersecurity Partnership without the US. – TheWorldPost. 30.10.2014. www.huffingtonpost.com/worldcrunch/why-russia-and-china-see-_b_6071528.html (visited 15.04.2016).

[273] The UN GGE has called for views on 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. UNGA. UN GGE 2013 Report, page 2. Seeking to further international dialogue on the issue, the Hague Global Conference on Cyber Security stressed the need for broad and inclusive engagement to enhance the shared understanding of how international law applies to State activities in cyberspace. Global Conference on CyberSecurity 2015. – www.gccs2015.com (15.04.2016).

activities in cyberspace has been largely disconnected from developments in international law and normative thought more broadly. On the one hand, the UN GGE has not been able to offer States viable interpretations of international law applicable to State conduct in cyberspace. On the other hand, we are a long way away from an international treaty governing cyberspace, similar to the Outer Space Treaty. Yet, in the meanwhile, the issue of international law as applied to advanced technologies is gaining further urgency and acuteness due to the interrelation between ICTs and other advanced technologies, in particular unmanned and autonomous systems. If conscious effort is not made by States to develop a realistic solution for cyberspace, the advancement of technologies combined with States' strategic and political interests will reduce international law to virtuous yet marginal system of rules in the organised hypocrisy.

4.3. From the breach of sovereignty to intervention: an organized hypocrisy

> "When major tides of change wash over the world, power structures almost inevitably reject the notion that the world really is changing and they cling to their old beliefs. In the past some changes came slowly and gave us the time we needed to adjust to a new reality. In the last years of this century, however, the velocity of change in the world has become so great that there are literally no precedents to guide us. Policymakers are discovering that many of the events that are altering the world come not in response to their actions but are driven by technologies which they may only dimly understand."[274]

International law has created norms for States to respect each other's sovereignty. Yet, in cyber domain, where physical borders are elusive, most activities take place inherently cross-border choosing the fastest way to arrive to its destination, regardless of the ownership of underlying networks, several jurisdictions or sovereign authority over them. The interconnectedness is used and abused by States for several purposes, e.g. cyber attacks with the aim of achieving a specific goal, subversion or espionage. When deploying an offensive cyber operation, a State makes the sovereign choice of non-compliance with the existing and well-established law, accepting the consequences of their behaviour. Depending on whether the operation possesses also a coercive element to be used on the victim State's, such operations can be categorised from breaches of sovereignty to violations of the non-intervention principle.[275] Intervention is seen as coercive interference, leaving out non-

[274] W.B. Wriston. Referenced work, p 63.

[275] The non-intervention principle has been often described as having a dual legal basis. It is based both on customary international law as well as treaty law. The principle is not explicitly mentioned in the UN Charter, however, it is prominent in multilateral, regional and bilateral treaties, such as the Montevideo Convention,

coercive forms of interference as simple violations of sovereignty outside of the scope of intervention. Intervention in essence aims to impose certain conduct of consequence on a sovereign State.[276] For the purposes of this thesis, the term intervention will include coercive acts that influence the internal or external matters that each State is permitted to decide freely.[277] It follows that not all violations of territory or sovereignty immediately concern the principle of non-intervention. Intervention lies between the prohibition on the use of force deriving from Article 2(4) UN Charter and the prohibition of simple violations of sovereignty, being thus "not insignificant, but also not supreme among wrongful acts."[278]

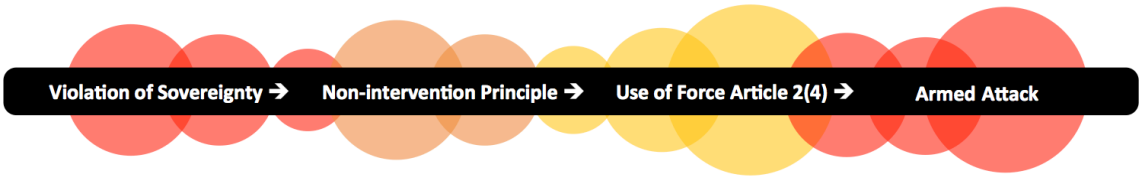

Figure 2. Spectrum of State activities from violation of sovereignty to armed attack

Observation that there is "a rather serious gap between what a broad view of the nonintervention norm would require and what states actually do"[279] is not a novelty. Stephen Krasner called such practice already in 1999 an "organised hypocrisy". The past decade of State practice in low-intensity offensive cyber operations conducted by States has not managed to constructively contribute to the development nor clearer interpretation of existing rules. There have been claims that operations that do not cross the threshold of UN Charter Article 2(4) are either legal[280] or the current international law regulation is not sufficient in order to provide an effective legal framework for low-intensity cyber operations[281] that breach State's sovereignty. Thus, they are often brushed aside, reasons being for example the difficulty of technical attribution of the attack or the lack of political prowess to challenge the

---

Charter of the Organization of the Americas, ASEAN Treaty, but also the Constitutive Act of the African Union, in the Pact of the League of Arab States etc. Non-intervention principle pertaining to States is implicitly provides also as a corollary principle of the sovereign equality of States in Art 2(1) of the UN Charter. (ICJ. Nicaragua, para 202.) The principle is also represented in numerous UNGA resolutions, most significant of them, the Friendly Relations Declaration.

[276] P. Kunig. Prohibition of Intervention. – The Max Planck Encyclopedia of Public International Law 2008, online edition, para 1.

[277] The definition follows the wording ICJ used in Nicaragua, para 205.

[278] S. Watts. Low-Intensity Cyber Operations, p 256.

[279] L.F. Damrosch. Politics Across Borders: Non-intervention and Nonforcible Influence over Domestic Affairs. – American Journal of International Law 1989, Vol. 83, p 2.

[280] R. Buchan. Cyber Attacks, p 211.

[281] P.W. Franzese. Referenced work, p 6; J. Barkham. Referenced work, footnote 112; M. Benetar. The Use of Cyber Force: Need for Legal Justification. – Gottingen Journal of International Law 2009, Vol. 1, p 377.

attacking State on the basis of international law and the rights and obligations deriving from it. As State practice of cyber operations with an offensive, yet low-intensity character has shown in the past, the victim States are not likely to contest the breach under international law, the only exception being USA after the Sony hack in 2014. However, failing to perceive low-intensity cyber operations as a threat and neglecting addressing them in the international discourse hampers States' long-term security, gives the advantage to the attackers,[282]creates non-constructive State practice that ignores international law and creates a perfect storm, where rules exist, but are not followed. Thus, the gap appears to be even wider today, where oftentimes the references to the non-intervention principle "are no more than *pro forma* incantations, with political, not legal, import."[283]

Recourse to the principle of non-intervention is most likely taken, when the State is the victim, not when it is conducting its own offensive activities. States respect international law, if it brings them valuable objectives, such as security, rule of law or good governance.[284] However, the lack of discussion on the topic of non-intervention in the cyber domain has proven the low priority of the principle among States, a decision that has wider political and strategic implications. Instead, the focus is on the opportunities provided by the cyberspace: it has offered States a new domain, where to expand their power, and pursue national interests. States do not need to recourse to the use of force anymore to achieve majority of their goals. Due to the interconnected and global nature of cyberspace, States are able to achieve wanted effects remotely, without placing their assets at physical risk at the location.[285, 286] In a largely interdependent word, cyber operations, especially the low-intensity ones allow States to be more intrusive with less destructive means, which has been proven in the last decade numerous times. Subsequently, States of all sizes find it easier than ever to accomplish their national security objectives and exercise sovereignty through breaching other State's sovereignty. From disrupting an adversary's propaganda efforts to sending active and visible

---

[282] S. Watts. Low-Intensity Computer Network Attack and Self-Defense. – International Law Studies 2011, Vol. 87, pp 61–72.
[283] M. Jamnejad, M. Wood. The Principle of Non-Intervention. – Leiden Journal of International Law 2009, Vol. 22, p 358.
[284] M. Koskenniemi. What use for Sovereignty today, p 63.
[285] P.A. Walker. Law of the Horse to Law of the Submarine: The Future of State Behavior in Cyberspace. – M. Maybaum, A-M. Osula, L. Lindström (eds.). 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace. Tallinn: NATO CCD COE Publications 2015, p 95.
[286] For example UK's MI6 conducted a cyber operation dubbed *Operation Cupcake*. In order to disrupt the dissemination of al Qaeda's *Inspire* magazine, which contained instructions for assembling a homemade bomb, the MI6 replaced the instructions with a cupcake recipe from Ellen Degeneres Show's Best Cupcakes in America. E. Flock. Operation Cupcake: MI6 Replaces al-Qaeda Bomb-Making Instructions with Cupcake Recipes. – Washington Post, 03.06.2011, www.washingtonpost.com/blogs/blogpost/post/operation-cupcake-mi6-replaces-al-qaeda-bomb-making-instructions-with-cupcake-recipes/2011/06/03/AGFUP2HH_blog.html (visited 01.04.2016).

messages of their own, from aggressive intelligence collection to subversion, supporting military operations and conducting sabotage,[287] limits of sovereign conduct in cyberspace are often determined by States' capabilities rather than traditional State boundaries and international law.

The first case that caught the attention of the international community at large and brought the subject matter of cyber operations and state sovereignty into the consciousness of Governments was the cyber attack on Estonia in 2007. However, States are suspected of taking actions against other nation-States already decades before that. In the so-called "Cuckoo's Egg" espionage case in 1986 Soviet Union's Committee for State's Security (hereinafter KGB) paid German hackers to steal information from the US.[288] The series of intrusions, dubbed "Moonlight Maze" took place a decade later, in the late 1990s, when US Government sites were intruded once again.[289] Yet, it was 2007 when supposedly Russian originated attacks on Estonian governmental and private servers started shedding light on State actions in cyberspace. Followed by attacks in Georgia in 2008 where again Russia was the supposed perpetrator,[290] the Stuxnet attack in 2010, with USA and Israel suspected in deploying the attack[291] and Saudi Aramco attack in 2012, where connection was sought to Iran looking for a retaliatory response to the Stuxnet attack two years earlier,[292] it was clear that the State offensive cyber operations were on the rise. Shortly after Saudi Aramco attack, several banks in the US were hit with large-scale DDoS attacks. Even though an Islamist cyber-fighters group claimed responsibility for the actions, international attention focused quickly on Iran, presumably seeking revenge for US-led economic sanctions and the Stuxnet attack on Iran's nuclear power plant in Natanz in 2010.[293] Lastly, the recent alleged hack of Sony Pictures Entertainment in 2014 brought about the first official "attribution," when the

---

[287] P.A.Walker. Referenced work, p 95.
[288] See for example J. Healey. A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association 2013.
[289] Since US had at the time ongoing tensions with Iraq, it was suspected that the attacks came from the latter. A. Gamero-Garrido. Cyber Conflicts in International Relations: Framework and Case Studies. – Massachusetts Institute of Technology, Engineering Systems Devision 2013, p 15.
[290] See E. Tikk, K. Kaska, L. Vihul. International Cyber Incidents, Legal Considerations. Tallinn: NATO CCD COE Publications 2010, pp 66-90.
[291] For a technical analysis of the attack, see, M. De Falco. Stuxnet Facts Report. A Technical and Strategic Analysis. – NATO CCD COE database Portal 2002.
[292] S. Van Der Meer. Foreign Policy Responses to International Cyber-attacks, Some Lessons Learned. – Clingendael, Netherland's Institute for International Relations 2015, p. 4 www.clingendael.nl/sites/default/files/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf (visited 10.03.20156).
[293] *Ibid*. Additionally, see E. Nakashima. U.S. rallied multinational response to 2012 cyberattack on American banks. – Washington Post, 11.04.2014, www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html (visited 04.04.2016).

US Federal Bureau of Investigation (hereinafter FBI) claimed to have evidence that North Korea was responsible for the attack.[294]

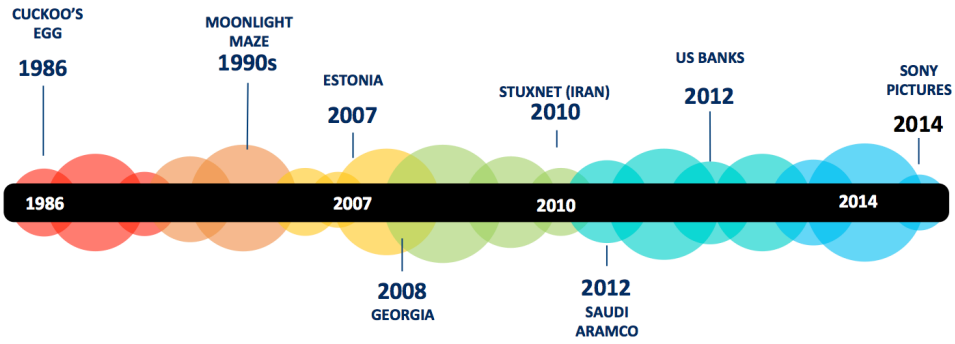

Figure 3. Timeline of most prominent State-on-State operations

The present work makes the claim that none of the above-mentioned cases crossed the threshold of UN Charter Article 2(4), yet several of the attacks, such as extensive DoS and DDoS attacks aimed at important governmental, economic or financial networks in order to influence State's policy decisions or actions can amount to an unlawful intervention.[295] Secondly, operations aimed at critical infrastructure or activities that yield significant economic consequences could be considered to have possessed the coercive element needed to categorise them as unlawful interventions,[296] given that successful attribution would be achieved. If no coercive element can be found, the attacks would still amount to violations of State sovereignty. Thus, international law provides long-standing rules that ought to protect State sovereignty from violations. Yet, these are also the norms that are most frequently breached.

If the attack does not amount to intervention, the logical question is what constitutes a breach of a State's sovereignty in cyberspace, yet it has no unified answer. The UN GGE 2015 Report did not elaborate on what constitutes a breach of sovereignty. It has been opined that territorial sovereignty, including in cyberspace, is violated by any acts causing physical effects.[297] It definitely violates State's sovereignty, if damage is caused.[298] However, such

---

[294] Federal Bureau of Investigation. Update of Sony Investigation. – FBI National Press Office. 19.12.2014, www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (visited 01.04.2016).
[295] This could be the case in Estonia and Georgia, respectively in 2007 and 2008.
[296] Operations of this nature can also be conducted, e.g. through DDoS attacks. Yet, not all DDoS attacks are aimed at critical infrastructure or cause significant economic damage. The range of mehtods used for these kinds of operations is not limited to a particular type. Similarly, low-intensity cyber operation may or may not cause physical damage. For example, when DDoS attacks are deployed, generally no physical damage ensues. Nevertheless, if the target is crucial, e.g. the banking sector, the following economic damage may be substantial. This could be the case of Stuxnet in 2010, Saudi Aramco in 2012 and even the attacks on the US banking sector.
[297] K. Ziolkowski. General principles, p 163.
[298] M.N. Schmitt. Tallinn Manual, p 6.

restrictive interpretation would only magnify non-compliance. Majority of low-intensity cyber operations that can affect severely the everyday functioning of a heavily technology dependent State, yet yield no physical damage. They are also inexpensive, easy to employ and can be used during peacetime to target for example political leadership, military systems, banking or communication sector wherever in the world with the benefit of attacker anonymity.[299]

Hence, the question is, whether State's offensive cyber operations that yield no physical effects would be considered a breach of sovereignty? That would be the situation, for example, when a malware has been entered in a State's information system or critical infrastructure by another State. It may have other functionalities, but in essence it does not affect the system in any adverse way. Here, it is useful to think about what are we protecting when talking about a breach of sovereignty. When a breach occurs, another State or its actors enter the sovereignty space of another State without permission. The right in question is the sovereign right to decide what is happening on your territory. When exercises of sovereignty can be limited due to external obligations that States have taken upon them, then sovereignty *in abstracto*, i.e. as a concept is a whole and should be protected as a whole. One cannot breach sovereignty "a little bit". Either sovereignty is breached or not. If a State actor enters the territory of another State without prior consent or permission, that actor is violating the sovereignty of that State, unless there is a justification recognised by law to allow such conduct in extraordinary circumstances. To exemplify the logic, a useful parallel here could be found in the airspace. Every State has a complete and exclusive sovereignty over the airspace above its territory.[300] Whereas States must provide civil aircrafts the right to fly over its territory, it does not have provide that for other State's military vehicles.[301] Thus, if such a vehicle enters State's airspace, it has breached its sovereignty. If the vehicle was in the airspace for a few minutes and it had no other effects on the State whose airspace was violated, was it still a breach of sovereignty? The present work would argue that it was. Breach of sovereignty requires an act. Those acts can either take place or not and depending on States' modes of action, the act is detected and attributed if possible. The question that follows from there is if the State is going to react to the breach or not. Yet, whether political or legal action is taken as a response depends already on the political decision-making. Taking into account the inherent interconnectedness that is created by the global information infrastructure, it is not optimal to think that a State would raise each breach as a violation on

[299] K. Geers. Strategic Cyber Security. Tallinn: NATO CCD COE Publications 2011, p 12.
[300] P.W. Franzese. Referenced work, pp 22-23.
[301] *Ibid*.

the international plane. However, the State retains the right to do so, should it wish, since it derives from their sovereignty.

Thus, it can be argued that physical damage or even physical effects are irrelevant in the cyber context. For example, the US has indicated that it considers its territorial sovereignty violated also by "disruption of networks and systems".[302] This approach includes intrusions, which may or may not show a physical effect. Similarly, Russia has concluded that cyber espionage, which does not yield any physical consequences, is a direct violation of their sovereignty.[303] Different playing rules reinforce the State practice, which essentially ignores the standards that international law has set. Clarity as to the matter, what can and cannot be considered a breach of sovereignty or intervention in the context of cyberspace, helps States to understand the ground rules in State-on-State conduct. Slowly but steadily moving issues pertaining to cyberspace and security thereof to the scope of issues regulated by international law through interpretation of existing norms according to the needs of new technologies might lead to a reduced expectation of protection from foreign States' intervention or overall meddling in these areas,[304] because an organised hypocrisy ought to not become the norm of State behaviour in cyberspace.

As the State's interventionist techniques have changed, the broader question will be: should the international community try to apply the established framework and existing standards or just conclude that the existing standards indeed do not afford for effective legal solutions, and thus leave the regulation of described cyber operations in a legal vacuum. As Judge Alvarez noted in the Corfu Channel case, the rights and obligations are not the same and not exercised in the same way in every sphere of international law. Thus, the violation of sovereign rights is not of equal gravity in all these spheres.[305] ICTs have provided States with a new domain, in which to expand their power and compete with one another. As threats emanating from cyberspace and malicious uses of ICTs continue to morph and disrupt established legal frameworks, ways in which States assert their sovereignty and power will continually develop and adapt to changing circumstances.[306] International law, in turn, is slow to adapt to new realities and the changing security landscape. The State practice elaborated above exemplifies that States are willing to non-comply with existing international law, if it benefits them. Yet,

---

[302] White House. International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World, p 4.
[303] Interfax. Putin: cyber espionage is direct violation of State's sovereignty. – 11.07.2014, www.interfax.com/newsinf.asp?id=519963 (visited 20.04.2016).
[304] S. Watts. Low-Intensity Cyber Operations, p 265.
[305] ICJ. Corfu Channel, separate opinion of Judge Alvarez, p. 43.
[306] C. Kavanagh. Referenced work, pp 100-101.

turning a blind eye to minor breaches of sovereignty impairs legal certainty. Whatever the new circumstances, sovereignty will always mean freedom within the law, not freedom from the law.[307]

Rethinking existing standards, or interpretations that do not consider changed circumstances and rapidly evolving technologies is to a certain extent necessary, otherwise, the current structure of cyberspace makes it "very attractive to ignore international law".[308] The aim of the non-intervention principle and respect for sovereignty is not only to allow States to operate free from outside interference but also to reinforce the notion of sovereign equality among States.[309] The reality is, that when an objective can be achieved either with forceful coercive measure or with the help of a rather cost-effective cyber operation, the natural choice today will be the latter.[310] Thus, one must look beyond LOAC and use of force and start seeing what is the coercive "force" of 21st century. More than ever, it becomes clear that modern assertions of power replace violence and force of arms with 'more gentle constraint of uninterrupted visibility'.[311] As Nancy Fraser observed already in the 1980s,

> "Modern power, then, is distinctive in that it keeps a low profile. It has no need of the spectacular displays characteristic of the exercise of power in the *ancien regime*. It is lower in cost (economically, since it requires less labor power; and also socially, since it is less easily targeted for resistance). Yet it is more efficacious."[312]

This is even more the case in today's security landscape. The international framework of sovereignty has not become desolate. It belongs to the core of international law. Yet, when visible violence and physical coercion is replaced with the "more gentle constraint of uninterrupted visibility,"[313] the legal checks and balances of low-profile power determine its efficacy. The more straightforward and clear the legal standards and principles are, the less likely it is that cyber operations are justified by the high standards adopted in a completely different security landscape and vagueness of existing regulation that lets States escape responsibility for their exercises of sovereignty. States have not realised their full capabilities. Furthermore, those, who have the appropriate capabilities will not want to constrain them, rather the opposite. Focusing solely on visible, i.e. traditional military, political and economic

---

[307] J. Crawford. Chance, Order, Change, p 93.
[308] P.A. Walker. Referenced work, p 94.
[309] ICJ. Nicaragua, para 302.
[310] K. Geers. Strategic Cyber Security, p 13.
[311] N. Fraser. Foucault on modern power: Empirical insights and normative confusions'. – Praxis international 1981, Vol. 3, p 278.
[312] *Ibid.*
[313] *Ibid.*

violations automatically exclude the most advanced and intrusive ones that can create even more serious effects. The State power exercised through the low-intensity cyber operations is more penetrating and less observable than earlier forms of power. As Sean Watts observes, comparisons to the "death by a thousand cuts" are apt.[314] They offer anonymity, low-visibility, can be timed to look like unrelated or isolated events, are unlikely to provoke debilitating responses from targets, yet are able to target the deepest part of State's infrastructure if needed, and the best part: if one were to follow the currently prevalent approach and discard all breaches that do not yield physical consequences, such uses of power and exercise of sovereignty may might fall outside of the scope of legal regulation. As Frasier noted, modern assertions of power get "hold of its objects at the deepest level – in their gestures, habits, bodies and desires."[315] The targets rarely see the attacks coming, are mostly unaware, if someone is exploiting their infrastructure, and in an interdependent and interconnected world with relatively large amount of ICT reliant States, it is easy to hit where it hurts the most effectively.

[314] S. Watts, Low-Intensity Computer Network Attack and Self-Defense, pp 61-74.
[315] *Ibid.*

5. International law and cyberspace juxtaposed

International law and politics cannot be considered to exist detached from each other. Delimiting international law from the politics and political of it would make more for a scholarly exercise than a relevant problem solving undertaking. As Martti Koskenniemi has put forward, they present a Wittgensteinian duck-rabbit, where what point of view one has, depends on the angle the object is being observed from.[316] International law is politics as much as politics is international law. Taking the politics out of international law, disconnects the latter from the reality. It becomes a utopia, which may be virtuous its goals, but marginal in the world's functioning. Yet, over-emphasising the political and State practice in turn undermines the normativity of international law.[317] Finding balance between the two has been engaging international lawyers for years.[318]

The balancing act must be taken into account in the cybersecurity discourse as well. Rules and concepts alone tell very little about their application in real life. Habits and traditions play a crucial role in the interpretation of those rules and concepts.[319] Thus, the pressure to the concept of sovereignty as well as to international law in general comes from two sources. Firstly, the technology itself and the accompanying development challenge international rules, concepts, and practices that have been created largely in the middle of last century. Inquiries into what technology changes and how the new technological reality affects the relationships between States are crucial ones. The development of technology and increased cooperation in inter-State relations has already changed the security landscape: almost half of the mankind has become connected,[320] very few issues can be considered isolated so that one could claim that they do not affect other States and for the most part, States are not able to tackle today's security threats alone. That is already true in the cyber domain, where State activities take place not only on their territory, but also in an intangible domain, threats are often cross-

[316] M. Koskenniemi. Lecture on Politics of International Law at the Lauterpacht Centre for International Law, University of Cambridge. – 26.01.2012, www.youtube.com/watch?v=-E3AGVTHsq4 (visited 30.04.2016).
[317] M. Koskenniemi. The Politics of International Law, p 40.
[318] See for an overview, *Ibid*, p 40 ff.
[319] P. Legrand. European Legal Systems Are Not Converging. – International and Comparative Law Quarterly 1996, Vol. 45, p 56.
[320] World Economic Forum. The Global Information Technology Report 2015: ICTs for Inclusive Growth. – 2015, www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf (visited 15.04.2016), p xvi. "There are as many mobile subscriptions as human beings on the planet. But half of the world's population do not have mobile phones and 450 million people still live out of reach of a mobile signal. In developing countries, a huge divide exists between well-connected urban centers and off-the-grid rural areas. Some 90 percent of population in low-income countries and over 60 percent globally are not online yet. Finally, most mobile phones are of an older generation. The ICT revolution will not be carried over voice and SMS but will require universal and high-speed Internet."

border, affect multiple States and one State's decision to close access to its infrastructure has the possibility to disconnect and isolate a whole State.

Depending on technologies, certain States are always the ones to have an upper hand when it comes to technological development. States will never be equal in technological prowess. Thus, the question is, for whom the new technologies (e.g. 5G networks, autonomous weapons systems, artificial intelligence, Internet of things) will provide most benefits in the future. Thus far, the US has been a clear dominant in the field and that shines through in the international law discussions as well,[321] leading at times the State to follow the ethos of the Schmittian decisionism. An approach according to which the State can be the final decision-maker on the exception,[322] regardless of what international law says, enforces the idea that "[n]orms are nice, but in cases of necessity, we are better off with decisions".[323] For example, after the 2014 Sony hack in the US, president Obama stated that "We will respond proportionally [to North Korea's hack of Sony], and we'll respond in a place and time and manner that we choose."[324] The latter approach clearly emphasises that those who have the technology, have the upper hand and thus, can be considered the decision-makers and they are very much aware, that States do not enjoy the sovereign equality that international law formally bestows upon them.[325] Numerous advances in technology will not enable all States to level the playing field and thus, the technology itself influences who can decide over the future and development international law in the field.

Secondly, international law also shaped and affected by the thinking of the leading States. Two different schools on the adequacy of the existing international law lead the international cybersecurity discourse. On the one hand, there are those, who claim that the existing law is adequate to resolve the issues brought about by the cyberspace. The main advocates for the view are the US and likeminded countries, including Estonia. The present thesis argues as well that we do not need new laws *per se* but we must take into account the changed security landscape. The solution that aims at providing clarity and predictability must rest on established norms, yet be mindful of the new technological reality, i.e. it is not just the

---

[321] The most comprehensive academic work released to date dealing with LOAC in cyberspace is the Tallinn Manual, which, even though excluding the views of Russia and China and focusing on likeminded opinions, is a ground breaking start on the discussion of international law and cyberspace, yet represents a rather one-sided discussion enforcing the liberal views of the West.

[322] C. Schmitt. Political Theology: Four Chapters on the Concept of Sovereignty. Chicago: University of Chicago Press 2005.

[323] M. Hildebrandt. Referenced work, p 221.

[324] The White House. Remarks by the President in Year-End Press Conference. – 19.12.2014, www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference (visited 30.04.2016).

[325] J. Alvarez. Sovereignty is not Withering Away, p 37.

novelty but also the pervasive utility of ICTs that must guide the choices we make concerning international law. The core and idea of law or established concepts, be it sovereignty, use of force or self-defence, does not change just because technology changes the world. Applying and interpreting the law in new circumstances is challenging, yet as explained, this is not the first time, when technology has changed and will not be the last time. The starting point must be the law, not what judges and academics say about the law, i.e. how they interpret it according to the needed perspective. As such, the law does not change according to circumstances, but the interpretation does. Thus, one of the solutions in the cybersecurity discourse would be to reinterpret the law we already have. In order to do that, taking into account the political reality and existing State practice is paramount. However, the second point about interpreting existing law refers back to what was claimed in the beginning of this thesis. The cybersecurity discourse has leaped over fundamental concepts of international law when discussing how international law applies. We have been preparing for a cyber-Pearl Harbour,[326] yet the question of sovereignty, upon which the concepts of use of force, armed attack and self-defence rest, is very much still open for States to interpret as they choose. While NATO has confirmed that Article 5 of the North Atlantic Treaty[327] applies to cyber operations as well,[328] the discussion on when and where a State's sovereignty is being breached is unclear. The strategic goal of States here might be to allow themselves the freedom of non-compliance when it comes to low-intensity operations that can be later justified by the unclearness or vagueness of the law. Yet, it is especially here, that the organised hypocrisy must not become a norm. We do not need to re-conceptualise sovereignty, but we must take into account that although cyberspace can be construed as more territorial as expected through its infrastructure, State's sovereignty and exercises thereof have also de- and extra-territorialised. States are using their power broader than just along their territorial lines.[329] Therefore, interpretation can be one of the ways of how to move the discourse further without changing or negotiating new treaties. Even though agreeing on a

[326] In the end of last year, the US explained that they now consider the likelihood of a catastophic cyber attack from any particular actor remote. "Rather than a "Cyber Armageddon" scenario that debilitates the entire US infrastructure, we envision something different. We foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time." J.R. Clapper. Statement for the Record. Worldwide Cyber Threats. – House Permanent Select Committee on Intelligence, 10.09.2015, fas.org/irp/congress/2015_hr/091015clapper.pdf (visited 15.04.2016).
[327] North Atlantic Treaty. 04.04.1949. – www.nato.int/cps/en/natolive/official_texts_17120.htm (visited 15.04.2016).
[328] NATO. Wales Summit Declaration. – 05.09.2014, www.nato.int/cps/en/natohq/official_texts_112964.htm (visited 30.04.2016).
[329] G.L. Herrera. Referenced work, p 11. Cf. N. Tsagourias. Legal Status of Cyberspace, p 21.

singular interpretation might prove to be difficult, re-interpretation based on existing concepts allows States to remain flexible and not increase the amount of treaty obligations.

On the other hand, there are those, who say that international law applies, yet cyberspace is a special domain, where existing rules do not offer enough protection for the malicious uses of ICTs by States. Therefore, new laws or a special treaty regime is needed. The proponents of this particular view are mainly SCO member states, led by China and Russia. Even though a new, technology-driven and enabled reality offers at the moment little prospect for a treaty-based solution, it cannot be counted out as a feasible solution when consensus on the application of international law to cyberspace will not be achieved. As explained, some have though the treaty approach to be premature or unnecessary. A treaty approach to relatively unsettled issues is not only time-consuming, but also predicted by remaining differences about concepts, definitions and the scope of applicability of already existing norms. Additionally, States are likely to want to preserve their freedom of action, not to mention that the verification of treaty compliance is bound to be difficult. However, if consensus is not found based on the existing law, a new treaty could be a solution for achieving some legal clarity over States' activities in cyberspace. This would then create separate regime dedicated to cybersecurity and allow States to argue only in terms of the said special "box" of regulation.[330] Yet, here one must proceed with caution. The fragmentation of international law was thoroughly researched by the International Law Commission and culminated with their report published in 2006. The report concluded that multiple specialist systems, such as human rights law, space law, humanitarian law etc., have been created in order to govern fields what once appeared to be governed by general international law. This, in turn, has created the danger of conflicting and incompatible rules, principles, rule-systems and institutional practices. Even though it is understandable that such specialised law emerges as a response to new technical and functional realities, very often the new rules and regimes develop in order to consciously deviate from what was provided by the general law. As such, the unity and coherence of international law suffers.[331] Fragmentation to some extent is natural, i.e. the diversity of national legal systems that participate in international legal system has created inherent fragmentation.[332] However, the more self-contained regimes are created

[330] M. Koskenniemi. The Politics of International Law – 20 Years Later, p 10.
[331] UNGA. A/CN.4/L.682. 13.04.2006. Fragmentation of International Law: Difficulties Arising From the Diversification and Expansion of International Law. Report of the Study Group of the International Law Commission. Finalized by Martti Koskenniemi, pp 11-14.
[332] UNGA. A/CN.4/L.702. 18.07.2006. Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law. Report of the Study Group of International Law Commission, para 11.

by the international community, the more marginal the existing body of international law becomes, as the "exception" will be come the "rule". When it comes to cybersecurity, the pervasive utility of ICTs has penetrated almost all fields of society. Whether it would be efficient to create another self-contained regime of "cyberlaw" to regulate State behaviour is questionable, taking into account the wider development of technology. States have spent over a decade discussing whether international law applies to cyberspace or not before concluding in 2013 that it does.[333] The pace at which international community agrees or disagrees on matters at hand does not correlate adequately with the pace of the technological development, allowing thus, once again, States to ignore international law, if it benefits them.

It is clear that anyone who wishes to propose a real and viable solution to the conundrums at hand must take both viewpoints into account, which are often hard to reconcile. A solution for cyberspace that is being led by either of the schools alone, is not feasible and invites for non-compliance from the other one. Thus, the discourse on how international law applies to cyberspace, which is still in its "infancy",[334] must take into account the underlying law as well as politics and State practice in the field. It cannot be solved in a vacuum, since politics and the aspirations of States influence profoundly, in what form and how the application of international law to cyberspace is decided and where consensuses formed.

The title of this thesis asks, if sovereignty in cyberspace is an organised hypocrisy. If one accepts Krasner's view that it has always characterised the sovereign State system, the answer to a great extent is affirmative.[335] Sovereignty, respect for other States' sovereignty and prohibition of intervention are some of the longest standing norms that are frequently violated by States using low-intensity cyber operations. The pervasiveness, anonymity and ease of use have made it enticing for States to achieve set goals through cyber means. Legal uncertainty and ambiguity accompanying the discussion on how existing international law applies to State conduct and exercises of sovereignty in cyberspace offer States the "perfect storm" for violating the existing rules for their own benefit or interpret existing law as they see fit. As there is probably no single set of rules that could align interest, power and legal rules and principles,[336] States, at least the most powerful, ambitious or impatient of them, will always have the incentive to deviate from existing norms, if it supports their strategic ambition or

[333] UNGA. UN GGE 2013 Report, para 19.
[334] It was only in 2013, when the UN GGE, after about a decade of deliberations, concluded that international law was to be applied to cybersecurity. Taking into account that the question "if" changed into a "how" only three years ago, there is still much work to be done, debating trying to figure out the demarcations of international law in cyberspace.
[335] S.D. Krasner. The durability of organized hypocrisy, p 96.
[336] *Ibid*, p 98.

turns out to be otherwise advantageous. The calculative logic of immediate benefits and desirable consequences can oftentimes override the logic of virtue and appropriateness. States, seeking to maintain their own position and promote their interests, can make the sovereign decision to comply or not to comply.[337] The combination of global connectivity, vulnerable technologies and anonymity has facilitated the use of ICTs for disruptive activities in the hands of States. If they have the resources, cyberspace has enabled States to deviate from existing international law and breach other States' sovereignty more easily and oftentimes with no consequences. If one affirms the inherent existence of organised hypocrisy when it comes to State sovereignty, the goal for any normative solution to the regulation of cyberspace ought to aim for stopping it becoming the norm of accepted State behaviour.

[337] S.D. Krasner. Sovereignty: Organized Hypocrisy, p 238.

Conclusion

The main research questions of the thesis were: How does sovereignty apply and how do States assert and exercise their sovereign rights in cyberspace? As suggested in the introduction, the present thesis is not intended as an all-embracing account on sovereignty or sovereignty in cyberspace for that matter. The aim was to offer a critical and complementary perspective on the debate on sovereignty in cyberspace. Therefore, it built on the existing understanding and scholarship of these issues.

The first chapter examined briefly the expert vocabulary used in the cybersecurity discourse. The chapter also explained that different States use different lexicons. While the Western world, leading with the US utters terms with the prefix "cyber-", then Russia, China and countries that value and speak of the importance of State sovereignty focus on information, information security, and information operations, a move which is in line with their claims of control over national information space.

The second chapter took a closer look to the general concept of sovereignty. The chapter outlined the basic tenets of territorial sovereignty and explained the difference between the concept of sovereignty and respective exercises of sovereignty *in concreto*. Besides exercising territorial sovereignty, one of the attributes of sovereignty is the right to bind the State with international obligations. As such, exercising sovereignty is compiled of a bundle of rights and obligations, which can change in time, making the concept of sovereignty relative. The chapter also explored some of the claims of the decline, withering away or death of sovereignty, yet concluded that the binary inquiry into State sovereignty is not sustainable. As sovereignty has not been ultimately defined, sovereignty has the ability to change through time. It also varies from State to State, as the amount of obligations that States bind themselves with vary.

The third chapter continued with the exploration of sovereignty in connection with cyberspace. More specifically, the chapter asked how the concept of territorial sovereignty is being applied vis-à-vis ICTs. Cyberspace and sovereignty are often seen as an oxymoron, since cyberspace is largely intangible. Thus, the cyberlibertarians proposed that this new domain should be independent and self-governing. As a result, no State could exercise their sovereignty over the cyberspace. However, their arguments are undermined with different fallacies, as explained in the thesis. Besides the no-sovereignty approach, there are generally two misconceptions surrounding the discourse of sovereignty in cyberspace. Firstly, cyberspace is often mistakenly found to be part of the global commons together with airspace,

international waters and outer space. However, taking into account its artificial nature, lack of physical boundaries and rest of the characteristics that global commons as a phenomenon have according to the test offered by Patrick W. Franzese, it was concluded that cyberspace is currently not understood as part of the global commons. That, in turn, does not mean that the discourse ought to exclude this as an option. However, in the light of the Franzese test, establishing such a regime would be difficult. Secondly, partly deriving from the global commons argument, cyberspace is often seen as a domain, where sovereignty does not apply. However, States will remain sovereigns and can assert authority therein, regardless of its party intangible nature. Most importantly, States have the authority over the information infrastructure located in their territory, which means that it is subject to legal and regulatory control by the State, yet is also protected by the inviolability of territorial sovereignty.

The fourth chapter focused on the different forms of exercises of sovereignty that States are engaging in when it comes to cyberspace. States are exercising internal sovereignty vis-à-vis the infrastructure located in their territory and the access and egress of their territory. Some States, such as the US, have adopted a more liberal approach, focusing on the openness of the system, while other exercise their sovereignty rather defensively and restrictively. To exemplify the latter position examples were brought from Russia and China, both of whom are strictly proponents of the ultimate value of State sovereignty. Besides exercising territorial sovereignty, one of the attributes of sovereignty is the right to bind the State by international obligations. One of the avenues, where States exercise control is the international norms development process for cyberspace, where either in the process of UN GGE or through SCO and the proposals of Code of Conducts, States seek to promote their value systems pertaining to cyberspace. The chapter also briefly discussed the calls of academics for a new treaty, similar to the Outer Space Treaty, which would govern the use, abuse and other exploitation of cyberspace. Yet, one had to conclude that States, who possess the ability to conclude treaties, are not ready for such a comprehensive solution. Lastly, the chapter explained that besides positive exercises of sovereignty, States oftentimes make use of the ambiguous nature of cyberspace and consciously breach other State's sovereignty, knowing the law and possible consequences, but still deciding to ignore it. Stephen Krasner calls this situation the organized hypocrisy.

The last chapter juxtaposing cyberspace and international law concluded that international law is influenced by two distinct developments: technology and the thinking of leading States. Technology gives the upper hand on deciding on the regulation and development of international law to those who have said technology. Thinking of the leading States and their

practice is influencing the solutions that States offer for the problems at hand. Here, two schools can be distinguished. One, led by the US, that emphasises the applicability of existing international law and the other, that insists on the creation of new law or establishing a treaty regime. Both solutions come with their caveats. It is clear that any solution that aims at regulating cyberspace must take into account the established law, norms and principles as well as the politics and aspirations of States. Since no normative solution can satisfy the interests of all, the organised hypocrisy can be considered inherent in the international system, i.e. there will always be States who will not abide by the rules. Thus, it is not for the international law to eradicate the organised hypocrisy, but to make sure it will not become an accepted State behaviour.

The thesis took a forward-looking approach, trying offer a fresh perspective on the current discourse. It is clear that cyber-related discourse will not be the last time technology challenges international law. With every new development in technology, States are going to become more intrusive, more penetrating, yet at the same time more undetectable, anonymous and untraceable whilst achieving their goals and strategic ambitions. States do not assert power only by open diplomacy, trade and arms and violence, but increasingly as invisibly as possible. In this context, the question of sovereignty is as apt as ever before, as international law and rules that flow from the concept of sovereignty ought to offer real solutions to real situations. Thus, the international community cannot allow ignoring the fundamental questions of international law discourse. Rather, it needs deep substantial discussion and feasible interpretations as solutions for the technology future to come.

Suveräänsus küberruumis: organiseeritud silmakirjalikkus?

Resümee

Tehnoloogia kiire areng ja informatsiooniaja võidukäik on muutnud paljud riigid info- ja kommunikatsioonitehnoloogiatest (järgnevalt IKT) sõltuvaks. Viimane mõjutab aga olulisel määral nii rahvuslikku julgeolekut kui ka riigi suveräänsuse teostamist. Antud töö eesmärk ei olnud esitada suveräänsuse ajaloolist ülevaadet ega pakkuda ühte ja lõplikku interpretatsiooni suveräänsusest küberruumis, vaid käesoleva töö põhiküsimused olid: kuidas suveräänsus kui kontseptsioon kohaldub ja kuidas riigid teostavad suveräänsust küberruumis?

Küberturvalisuse diskursus rahvusvahelise õiguse raames on loomult nii poliitiline kui õiguslik. Seda näitab ka see, et riigid kasutavad antud diskursuse raames erinevat sõnavara probleemide kirjeldamiseks ning arutamiseks, asetades seeläbi rõhu problemaatika erinevatele aspektidele. Kui läänemaailm USA juhtimisel asetab fookuse eesliitele "küber-", siis Venemaa, Hiina ja teised riigid, kes väärtustavad enim riigi suveräänsust, rõhutavad eelkõige informatsiooni ning selle turvalisust. Erinevus tekib seeläbi, et pannes kokku fraasid "küberturvalisus" ja "küberruum", toonitab läänemaailm ühtse mõistena nii informatsiooni infrastruktuuri kui ka informatsiooni enda turvalisust, samas kui "informatsiooni turvalisus" ja "informatsiooniruum" hoiavad antud kaks aspekti lahus. Viimane lähenemine aga võimaldab riikidel nagu Venemaa ja Hiina kontrollida lisaks infrastruktuurile ka informatsiooni liikumist ning seda piirata, kui see peaks riigile vajalik olema.

Pöördudes suveräänsuse kui kontseptsiooni teoreetilise külje poole, analüüsis käesolev töö territoriaalse suveräänsuse põhilisi omadusi ning selgitas erinevust suveräänsuse kui kontseptsiooni ja suveräänsuse teostamise vahel. Suveräänsus on üldised defineeritud läbi riigi territooriumi. Siseriiklikult on suverään see, kes teostab jurisdiktsiooni ilma teiste riikide sekkumiseta. Suhetes teiste riikidega tähendab suveräänsust võrdsust teiste riikidega rahvusvahelisel tasandil, millest tulenevalt lasub riikidel kohustus austada üksteise suveräänsust. Antud kontseptsioon peegeldub ka mittesekkumise põhimõttes. Suveräänsuse teostamine võib aga toimuda mitmes vormis. Nimelt üks kõige levinumaid suveräänsuse teostamise vorme rahvusvahelisel tasandil on rahvusvaheliste kohustustega liitumine, st rahvusvahelised lepingud või muud instrumendid. Viimast ei peeta aga suveräänsuse äraandmiseks, piiramiseks või jagamiseks, sest riigid saavad ennast siduda rahvusvaheliste kohustustega just seetõttu, et nad on suveräänid. Seega tuleb vastavalt rahvusvahelise õiguse praktikale eristada suveräänsust kui kontseptsiooni ning suveräänsuse teostamist. Kui esimest saab rikkuda, kuid ei saa *per se* ära anda, siis suveräänsuse teostamist saab riik ise piirata

vastavalt sellele, mis kohustusi ta on endale võtnud. Suveräänsuse teostamine on seotud mitmete õiguste ja kohustustega, mille maht aja jooksul võib muutuda. Seega on õigustatud ka vaade, mille alusel suveräänsuse teostamise ulatus sõltub ajast ning riigi suhete arengust rahvusvahelisel tasandil. Samuti ei ole õigustatud väited suveräänsuse "surmast" ning ärakadumisest. Seni kaua kuni eksisteerib rahvusvahelisel tasandil iseseisvate riikide süsteem, seni kaua on oluline positsioon ka suveräänsusel. Siiski järeldas käesolev töö, et binaarsed diskussioonid sellest, kas suveräänsus on või ei ole "surnud" ei ole edasiviivad. Kuna suveräänsuse mõistele pole ühtset definitsiooni pakutud, on see ajas ning ruumis muutunud. Samuti on suveräänsuse sisustamine riigiti erinev, sest kohustuste maht, millega riigid ennast seovad on erinevate riikide puhul erinev.

Rääkides suveräänsusest küberruumi kontekstis tundub esmapilgul olevat tegemist ilmselge oksümoroniga: suveräänsus põhineb territoriaalsusel ning küberruum on mittemateriaalne ruum, mis põhineb suuresti elektromagnetspektril, mille ulatuses ei saa ükski riik piiritleda oma suveräänset ala. Seega arutles antud töö selle üle, kuidas suveräänsuse kontseptsiooni küberruumis rakendada. Varajased Interneti vabaduse eest seisnud aktivistid eesotsas David Posti, David Johnsoni ja John P. Barlow-ga nentisid, et riigid ei saa küberruumis suveräänsust teostada. Kuna see on suures osas mittemateriaalne, a-territoriaalne ning piirideta, ei olnud nende arvamuse kohaselt mõistlik allutada antud avatud ruum riikide võimule. Seega pakkusid liberaalsete vaadetega aktivistid välja, et küberruum peaks olema iseseisev ning isereguleeriv ruum, kus reeglid tekivad seda ruumi kasutavate inimeste vahel orgaaniliselt. Nende argumendid ei võtnud aga arvesse seda, et küberruum ei ole maailmast eraldiseisev ruum, vaid kommunikatsioonimeediana reaalse maailmaga tihedalt seotud.

Kui riikide poolt täiesti reguleerimata ruumi käsitlus ei leidnud suurt poolehoidu, siis pakuti välja, et küberruumi puhul võiks olla tegemist globaalse ühisomandiga, sarnaselt õhu, avamere ja kosmosega. Globaalse ühisomandi puhul on tegemist ressursiga, mis ei kuulu otseselt ühegi riigi omandisse ega suveräänse kontrolli alla, vaid on jagatud hüve, mida hallatakse ühiselt läbi rahvusvaheliste lepingute. Võrreldes eksisteerivaid ühisomandeid küberruumiga, leidub siiski mitmeid erinevusi. Küberruum on inimeste poolt loodud ning seega mitte looduslikult tekkinud. Lisaks kasutab küberruum toimimiseks kõiki teisi ühisomandeid nagu avameri, kuhu on asetatud allveekaablid, ja õhk, mille kaudu signaalid levivad. Kogu küberruumi toetav füüsiline informatsiooni infrastruktuur on aga igal hetkel teatud riigi territooriumil ja selle riigi jurisdiktsiooni all. Samuti puuduvad küberruumil otsesed piirid, samal ajal kui näiteks avameri on oma ulatuses piiratud. Seega ei ole vähemalt praegusel hetkel küberruumi riikide poolt globaalse ühisomandina tunnustatud.

Globaalse ühisomandi argument aitas osati kaasa ka väärarvamuse tekkele, justkui ei oleks võimalik suveräänsust küberruumis teostada. Võttes arvesse küberruumi mittermateriaalset olemust ning a-territoriaalsust, saavad riigid siiski küberruumis suveräänsust teostada. Neil on jurisdiktsioon nende territooriumil asuva informatsiooni infrastruktuuri ning tegevuste üle, mis seda infrastruktuuri puudutavad. Lisaks saavad riigid reguleerida juurdepääsu oma territooriumile ning ka seda, mis nende territooriumilt välja läheb, läbi ligipääsupunktide, mis riiki globaalse võrguga ühendavad. Seega on küberruum territoriaalsem kui arvatud ning nendel riikidel, kes soovivad suveräänsust teostada, on see võimalus olemas.

Eelnevale toetudes uuris antud töö, kuidas riigid suveräänsust küberruumis teostavad ja jõudis järeldusele, et seda tehakse mitmes vormis. Esiteks, teostavad riigid suveräänsust riigisiseselt infrastruktuuri osas, mis nende territooriumil asub. Osad riigid, näiteks USA, on antud küsimuses liberaalsemal positsioonil, keskendudes küberruumi avatud loomusele ning oma suveräänse haarde laiendamisele küberruumis. Vastanduval seisukohal on näiteks Venemaa ja Hiina, kes teostavad suveräänsust küberruumis kaitsepositsioonilt toetudes suveräänsuse kaitsele ning seega piiravalt. Teiseks, riigid teostavad suveräänsust küberturvalisusega seotud rahvusvahelise õiguse arendamise protsessides, otsustades aktiivselt, milliste kohustustega nad küberturvalisuse diskursuses seotud soovivad olla. Läbi osalemise ÜRO valitsusekspertide grupis või Shanghai Koostööorganisatsiooni töös edastavad riigid rahvusvahelisele kogukonnale oma seisukohti küberruumi reguleerimise osas. Samuti on üks suveräänsuse teostamise viise uue rahvusvahelise lepingu väljatöötamine. Kuigi enamik riike on uue lepingu, st täiendavate rahvusvaheliste kohustuste osas pigem negatiivselt meelestatud, on üleskutsed akadeemikute kui ka väikese hulga riikide poolt siiski aktuaalsed. Kui konsensust antud alal ei leita, võib rahvusvahelise lepingu idee muutuda taas relevantseks.

Lisaks positiivsetele suveräänsuse teostamise viisidele, juhtis töö tähelepanu sellele, et riigid kasutavad tihti ära küberruumiga seostud anonüümsust ja globaalset haaret ning rikuvad madala intensiivsusega küberoperatsioone kasutades teadlikult teiste riikide suveräänsust. Saboteerides riigi kriitilist infrastruktuuri või muutes infoühiskonnana identifitseeriva riigi e-teenused kasutamatuks teatud perioodiks, teeb ründav riik, teise riigi suveräänses ruumis ilma loata tegutsedes teadliku otsuse rahvusvahelist õigust rikkuda. Antud olukorda nimetab Stephen Krasner organiseeritud silmakirjalikkuseks: riigid rikuvad rahvusvahelist õigust, sest see on neile kasulik.

Viimaks on oluline ka küsimus rahvusvahelise õiguse ning küberturvalisuse sümbioosist. Võttes arvesse tehnoloogia kiiret arengut, on rahvusvaheline õigus survestatud kahest eri suunast: tehnoloogia ise ning juhtivate riikide mõtlemine. Tehnoloogia areng paratamatult

soosib teatud riike. Senini on olnud esiotsas USA, kelle mõtlemine on rahvusvahelise õiguse arengut antud vallas oluliselt mõjutanud. Seega on eelispositsioon rahvusvahelise õiguse interpreteerimise ning arengu üle otsustamisel nendel riikidel, kellel vastav tehnoloogia juba on. Tuleviku perspektiivis on küsimus selles, mil määral uued tehnoloogiad olemasolevat õigust muudavad ning kellele ideoloogiast ning väärtussüsteemist antud muudatuste läbiviimine kantud on.

Teisalt mõjutab rahvusvahelist õigust juhtivate riikide mõtlemine seda, millised lahendused tekkivatele probleemidele leitakse. Rahvusvaheline õigus on oma tuumas sügavalt seotud poliitikaga. Õigus, mis ei võta riikide ambitsioone ja püüdlusi arvesse, võib muutuda utoopiaks, mis ei võtaks arvesse eksisteerivat reaalsust. Teisalt liigne keskendumine poliitikale õõnestab rahvusvahelise õiguse normatiivsust. Üritades lepitada kahte poolt, on antud juhul küberturvalisuse vallas välja kujunenud kaks erinevat koolkonda. Esimene neist keskendub eksisteeriva õiguse kohaldamisele ja teine leiab, et muutunud olude efektiivseks reguleerimiseks on vaja luua uut ning spetsiifilist õigust või läbi rääkida uue rahvusvahelise lepingu vastuvõtmine. Mõlemal lahendusel on oma negatiivsed küljed. Eksisteeriva õiguse kohaldamine võib kinni jääda selle taha, et ei suudeta kokku leppida ühtses tõlgenduses või ei ole riigid nõus nn vana õigust uutele oludele kohaldama. Antud töö on seisukohal, et eksisteerivat õigust saab ja peab kohaldama küberruumile, kuid arvesse tuleb võtta uut tehnoloogiast sõltuvat tegelikkust. Põhilised rahvusvahelise õiguse normid on juba riikide poolt aktsepteeritud, kuid antud juhul on neid vaja uutes oludes tõlgendada nii, et need pakuks efektiivset kaitset ning reguleeriks riikide käitumist. Uue õiguse loomine või rahvusvahelise lepingu väljatöötamine võib osutuda ajamahukaks protsessiks, kus senini konsensust mitteleidnud küsimustes ei suudeta siiski lõpuni kokku leppida. Samuti võib uus nn spetsiaalne õigus panustada üldise rahvusvahelise õiguse edasisse fragmenteerumisse. Siiski ei saa nt rahvusvahelise lepingu loomise ideed täiel määral kõrvale heita, sest juhul, kui riigid ei suuda olemasoleva õiguse raames kokku leppida küberruumis kohalduvate reeglite osas, on just spetsiaalne lahendus see, mis võiks panustada oluliselt õigusselgusesse ning –kindlusesse. Ükskõik kumma lahenduse kasuks rahvusvaheline kogukond lõpuks otsustab, on selge, et arvesse tuleb võtta mõtlema koolkonna huvisid ning eesmärke. Kuna ükski rahvusvaheline lahendus ei ole osalejate rohkust arvesse võttes selline, mis suudaks kõigi huve parimal moel tagada, ei kao organiseeritud silmakirjalikkus rahvusvahelisest suveräänsuse diskussioonist. Alati on maailmas riike, kes ei järgi rahvusvahelise õiguse sätestatud reegleid. Samas ei ole antud õiguse eesmärgiks ei küberturvalisuse diskussioonis kui ka üldisemalt rahvusvahelise

õiguse diskursuses organiseeritud silmakirjalikkust kaotada, vaid tagada, et selline käitumine ei muutu riikidevahelises suhtluses normiks.

Riikide suveräänsuse küsimus küberturvalisuse kontekstis ei jää viimaseks korraks, mil tehnoloogia suveräänsuse teostamise küsimuse alla seab. Iga järgneva arenguhüppega leiavad riigid viisi, kuidas tehnoloogiat oma huvide kaitseks või edendamiseks veelgi efektiivsemalt, läbitungivamalt ning sügavamalt ekspluateerida, jäädes ise sealjuures nähtamatuks, anonüümseks ning jälitamatuks. Võimu teostamine ei ole enam mõttekas relvade ja füüsilise vägivallaga, kui seda saab teha palju nähtamatumalt ning väiksemate kulutustega. Selles kontekstis on küsimus suveräänsusest ja selle teostamises küberruumis üha aktuaalsem. Rahvusvaheline õigus peaks pakkuma reaalseid lahendusi reaalsetele dilemmadele, mis küberruumiga kaasnevad. Seetõttu ei saa rahvusvaheline kogukond aktsepteerida fundamentaalsete küsimuste eiramist rahvusvahelise õiguse ja küberturvalisuse diskursuses. Sisuline diskussioon ja reaalsed tõlgendused eksisteerivast õigusest, mis võtavad arvesse uut tehnoloogiast sõltuvat reaalsust valmistavad meid ette veelgi intensiivsemaks tehnoloogiatulevikuks.

Bibliography

Books, book chapters and articles

1. Alvarez, J.E. State Sovereignty is Not Withering Away: A Few Lessons for the Future. – A. Cassese (ed.). Realizing Utopia: The Future of International Law. Oxford: Oxford University Press 2012.
2. Antolin-Jenkins, V.M. Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places? – Naval Law Review 2005, Vol. 51.
3. Austin, J. The Province of Jurisprudence Determined and the Uses of the Study of Jurisprudence. Isaiah Berlin, Stuart Hampshire, Richard Woolheim (eds.). London: Weidenfeld and Nicolson 1954.
4. Austin, J. The Province of Jurisprudence Determined. London: John Murray 1832.
5. Barkham, J. Information Warfare and International Law on the Use of Force. – NYU Journal of International Law and Policy 2001, Vol. 34, No. 56.
6. Barrett, M., Bedford, D., Skinner, E., Vergles, E. Assured Access to the Global Commons. – Supreme Allied Command Transformation, North Atlantic Treaty Organization, Norfolk, Virgina USA, 2011, www.alex11.org/wp-content/uploads/2013/01/aagc_finalreport_text.pdf (visited 01.04.2016).
7. Bartelson, J. A Geneology of Sovereignty. Cambridge: Cambridge University Press 1993.
8. Benetar, M. The Use of Cyber Force: Need for Legal Justification. – Gottingen Journal of International Law 2009, Vol. 1.
9. Besson, S. Sovereignty. – Max Planck Encyclopedia of Public International Law, Oxford University Press 2011, online edition, opil.ouplaw.com/home/epil (visited 29.03.2016).
10. Biegel, S. Beyond our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace. Cambridge: MIT Press 2001.
11. Brown, D. A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict. – Harvard International Law Journal 2006, Vol. 47. No. 1.
12. Brown, G.D. The Wrong Questions About Cyberspace. – Military Law Review 2014, Vol. 217.
13. Bryant, R. What kind of space is cyberspace? – Minerva – An Internet Journal of Philosophy 2001, Vol. 5.

14. Buchan, R. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? – Journal of Conflict & Security Law 2012, Vol. 17, No. 2.
15. Buchan, R.; Tsagourias, N. Cyber War and International Law. – Journal of Conflict & Security Law 2012, Vol. 17, No. 2.
16. Camilleri, J.A., Falk, F. The End of Sovereignty? The Politics of a Shrinking and Fragmenting World. – Foreign Affairs Fall 1992, www.foreignaffairs.com/reviews/capsule-review/1992-09-01/end-sovereignty-politics-shrinking-and-fragmenting-world (visited 01.04.2016).
17. Clarke, R.A., Knake, R.K. Cyber War: The Next Threat to National Security and What to Do About It. New York: HarperCollins Publishers 2010.
18. Condorelli, L., Cassese, A. Is Leviathan Still Holding Sway over International Dealings? – A. Cassese (ed.) Realizing Utopia: The Future of International Law. Oxford: Oxford University Press 2012.
19. Crawford, J. Brownlie's Principles of Public International Law, 8th ed. Oxford: Oxford University Press 2012.
20. Crawford, J. Chance, Order, Change: The Course of International Law. The Hague: Hague Academy of International Law 2014.
21. Crawford, J. Sovereignty as a legal value. – J. Crawford, M. Koskenniemi (eds.). The Cambridge Companion to International Law. Cambridge: Cambridge University Press 2012.
22. Crawford, J., Koskenniemi, M. (eds.). The Cambridge Companion to International Law. Cambridge: Cambridge University Press 2012.
23. Damrosch, L.F. Politics Across Borders: Non-intervention and Nonforcible Influence over Domestic Affairs. – American Journal of International Law 1989, Vol. 83.
24. De Falco, M. Stuxnet Facts Report. A Technical and Strategic Analysis. – NATO CCD COE database Portal 2002.
25. De Jong-Chen, J. Spotlight on Cyber V: Data Sovereignty, Cybersecurity and Challenges for Globalization. – Georgetown Journal of International Affairs, 12.10.2015, journal.georgetown.edu/data-sovereignty-cybersecurity-and-challenges-for-globalization/ (visited 15.04.2016).
26. Demchak, C., Dombrowski, P. Cyber Westphalia: Asserting State Prerogatives in Cyberspace. – Georgetown Journal of International Affairs: International Engagement on Cyber III 2013/2014.
27. Dinstein, Y. Computer Network Attacks and Self-Defense. – International Law Studies 2001, Vol. 76.

28. Dinstein, Y. The Principle of Distinction and Cyber War in International Armed Conflict. – Journal of Conflict & Security Law 2012, Vol. 17, No. 2.
29. Ernst, D. Indigenous Innovation and Globalization. The Challenge for China's Standardization Strategy – UC Institute on Global Conflict and Cooperation, East-West Center; June 2011.
30. Farwell, J.P., Rohozinski, R. Stuxnet and the Future of Cyber War. – Survival 2011, Vol. 53.
31. Fassbender, B. Sovereignty and Constitutionalism in International Law. – N. Walker (ed.). Sovereignty in Transition. Oxford: Hart Publishing 2003.
32. Ferreira-Snyman, M.P. The Evolution of State Sovereignty: A Historical Overview. – 2006, uir.unisa.ac.za/bitstream/handle/10500/3689/Fundamina%20Snyman.finaal.pdf?sequence=1 (visited 15.04.2016).
33. Franzese, P.W. Sovereignty in Cyberspace: Can it Exist? – Air Force Law Review 2009, Vol. 64.
34. Fraser, N. Foucault on modern power: Empirical insights and normative confusions'. – Praxis international 1981, Vol. 3.
35. Gamero-Garrido, A. Cyber Conflicts in International Relations: Framework and Case Studies. – Massachusetts Institute of Technology, Engineering Systems Devision 2013.
36. Geers, K. Pandemonium: Nation States, National Security, and the Internet. – L. Vihul (ed.). The Tallinn Papers: Numbers 1-9 (2014-2015). Tallinn: NATO CCD COE Publications 2015.
37. Geers, K. Strategic Cyber Security. Tallinn: NATO CCD COE Publications 2011.
38. Geiss, R., Lahmann, H. Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space – Israeli Law Review 2012, Vol. 45.
39. Gibbons, L.J. No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace. – Cornell Journal of Law and Public Policy 1997, Vol. 6, No. 3.
40. Gibson, W. Neuromancer. New York: Berkley Publishing Group 1989.
41. Goldsmith, J.L. Against Cyberanarchy. – University of Chicago Law Review 1998, Vol. 65.
42. Goldsmith, J.L. Regulation of the Internet: Three Persistent Fallacies. – Chicago-Kent Law Review 1998.

43. Hanqin, X. Chinese Perspectives on International Law: History, Culture and International Law. The Hague: Hague Academy of International Law 2012.
44. Hathaway, O.A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. The Law of Cyber Attack. – California Law Review 2012, Vol. 100, No. 1.
45. Healey, J. A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association 2013.
46. Heintschel von Heinegg, W. Legal Implications of Territorial Sovereignty in Cyberspace. – C. Czosseck, R. Ottis, K. Ziolkowski (eds.). 2012 4th International Conference on Cyber Conflict, Proceedings. Tallinn: NATO CCD COE Publications 2012.
47. Heintschel von Heinegg, W. Territorial Sovereignty and Neutrality in Cyberspace. – International Law Studies 2013, Vol. 89.
48. Henkin, L. International Law: Politics and Values. Dordrecht: Martinus Nijhoff Publishers 1995.
49. Henkin, L. That "S" Word: Sovereignty, and Globalization, and Human Rights, et cetera. Lecture. – Fordham Law Review 1999, Vol. 68.
50. Henkin, L. The Mythology of Sovereignty. – R.St.J. Macdonald (ed.). Essays in Honour of Wang Tieya. The Hague: Martinus Nijhoff 1993.
51. Herrera, G.L. Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space. – Prepared for the 47th Annual International Studies Association Convention March 22–25, 2006, kms2.isn.ethz.ch/serviceengine/Files/CRN/46419/ieventattachment_file/1443347D-7CD7-40E2-871D-33202AA7A91E/en/CISS-ETH_Herrera.pdf. (visited 13.04.2016).
52. Higgins, R. Problems and Process: International Law and How We Use it. Oxford: Clarendon Press 1994.
53. Hildebrandt, M. Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace. – University of Toronto Law Journal 2013, Vol. 63, No. 2.
54. Hobbes, T. Leviathan or The Matter, Form, and Power of a Commonwealth, Ecclesiastical and Civil. R. Tuck (ed.). Cambridge: Cambridge University Press 1991.
55. Hoisington, M. Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense. – Boston College International and Comparative Law Review 2009, Vol 32, No. 2.
56. Hollis, D.B. An e-SOS for Cyberspace. – Harvard International Law Journal 2011, Vol. 52.

57. Hollis, D.B. Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack? – J.D. Ohlin, K. Govern, C. Finkelstein (eds.). Cyberwar: Law and Ethics for Virtual Conflicts. Oxford: Oxford University Press 2015.
58. International Institute for Strategic Studies. Strategic Dossier. The Evolution of the Cyber Domain: the Implications for National and Global Security. Abington: Routledge 2015.
59. Jamnejad, M., Wood, M. The Principle of Non-Intervention. – Leiden Journal of International Law 2009, Vol. 22.
60. Jensen, E.T. Computer Attacks on Critical National Infrastructure: A Use of Force Revoking the Right to Self-Defense. – Stanford Journal of International Law 2002, Vol. 38.
61. Jensen, E.T. Cyber Sovereignty: The Way Ahead. – Texas International Law Journal 2015, Vol. 50, No. 2.
62. Johnson, D.R., Post, D. And How Shall the Net be Governed?: A Mediation on the Relative Virtues of Decentralized, Emergent Law. – B. Kahin, J.H. Keller (eds.). Coordinating the Internet. Cambridge: MIT Press 1997.
63. Johnson, D.R., Post, D. Law and Borders – The Rise of Law in Cyberspace. – Stanford Law Review 1996, Vol.48.
64. Joyner, C.C., Lotrionte, C. Information Warfare as International Coercion: Elements of a Legal Framework. – European Journal of International Law 2001, Vol. 12.
65. Kalmo, H., Skinner, Q. Introduction: a concept in fragments. – H. Kalmo, Q. Skinner (eds.). Sovereignty in Fragments: The Past, Present and Future of a Contested Concept. Cambridge: Cambridge University Press 2010.
66. Kanuck, S. Sovereign Discourse on Cyber Conflict Under International Law. – Texas Law Review 2010, Vol. 88, No. 7.
67. Kastenberg, J.E. Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law. – Air Force Law Review 2009, Vol. 64.
68. Kavanagh, C. Cybersecurity, Sovereignty, and U.S. Foreign Policy. – American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy 2015, Vol. 37.
69. Kent, H.S.K. The Historical Origins of the Three-Mile Limit. – American Journal of International Law 1954, Vol. 48, No. 4.
70. Kingsbury, B. Sovereignty and Inequality. – European Journal of International Law 1998, Vol. 9.

71. Kissel, R. Glossary of Key Information Security Terms. – Cybersecurity, www.nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (visited 10.03.2016).
72. Klabbers, J. Clinching to the concept of sovereignty: Wimbeldon redux. – Austrian Review of International and European Law 1999, Vol. 3, No. 3.
73. Kodar, E. Computer Network Attacks in the Grey Areas of Jus ad Bellum and Jus in Bello. – Baltic Yearbook of International Law 2009, Vol. 9.
74. Koh, H.H. International Law in Cyberspace. – Harvard International Law Journal 2012, Vol. 54.
75. Koskenniemi, M. From Apology to Utopia. Cambridge: Cambridge University Press 2005.
76. Koskenniemi, M. The Politics of International Law – 20 Years Later. – European Journal of International Law 2009, Vol. 20, No. 1.
77. Koskenniemi, M. The Politics of International Law. Oxford: Hart Publishing Ltd 2011.
78. Koskenniemi, M. The Wonderful Artificiality of States. – American Society of International Law Proceedings 1994, Vol. 88.
79. Koskenniemi, M. What Use for Sovereignty Today? – Asian Journal of International Law 2011, Vol. 1.
80. Krasner, S.D. Pervasive nor Perverse: Semi-Sovereigns as the Global Norm. Symposium Making Peace Agreements Work: The Implementation and Enforcement of Peace Agreement Between Sovereign and Intermediate Sovereign. – Cornell International Law Journal 1997, Vol. 30.
81. Krasner, S.D. Sovereignty: Organized Hypocrisy. Princeton: Princeton University Press 1999.
82. Krasner, S.D. The durability of organized hypocrisy. – H. Kalmo, Q. Skinner (eds.). Sovereignty in Fragments: The Past, Present and Future of a Contested Concept. Oxford: Oxford University Press 2010.
83. Krasner, S.D. The Hole in the Whole: Sovereignty, Shared Sovereignty, and International Law. – Michigan Journal of International Law 2004, Vol. 25.
84. Krutskikh, A., Streltsov, A. International Law and the Problem of International Information Security. – International Affairs 2014, Vol. 60, No. 6.
85. Ku, R. Foreword: A Brave New Cyberworld? – Thomas Jefferson Law Review 2000, Vol. 22.
86. Kunig, P. Prohibition of Intervention. – The Max Planck Encyclopedia of Public International Law 2008, online edition.

87. Lansing, R. Notes on Sovereignty. – Washington DC: Carnegie Endowment for International Peace 1921.
88. Lauterpacht, E. Sovereignty – Myth or Reality? – International Affairs 1997, Vol. 73, No. 1.
89. Legrand, P. European Legal Systems Are Not Converging. – International and Comparative Law Quarterly 1996, Vol. 45.
90. Leibholz, G. Sovereignty and European Integration: Some Basic Considerations. – G. Leibholz (ed.). Politics and Law. Leiden: Sijthoff 1965.
91. Lewis, J.A. Sovereignty and the Role of Government in Cyberspace. – Brown Journal of World Affairs 2010, Vol. 16. No. 2.
92. Lewis, J.A. The Cyber War Has Not Begun. – Center for Strategic and International Studies 2010.
93. Libicki, M.C. Crisis and Escalation in Cyberspace. Santa Monica: RAND Corporation 2012.
94. Locke, J. Two Treatises of Government. T.I. Cook (ed.). New York: Hafner Press 1947.
95. Lotrionte, C. State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights. – Emory International Law Review 2012, Vol. 26.
96. Lowe, V. International Law, 1st ed. Oxford: Oxford University Press 2007.
97. Mälksoo, L. Russian Approaches to International Law. Oxford: Oxford University Press 2015.
98. McGraw, G. Cyber war is Inevitable (Unless We Build Security In). – Journal of Strategic Studies 2013, Vol. 36, No. 1.
99. Midson, D. Geography, Territory and Sovereignty in Cyber Warfare. – H. Nasu, R. McLaughlin (eds.). New Technologies and the Law of Armed Conflict. The Hague: T.M.C. Asser Press 2014.
100. Miller, R.A., Kuehl, D.T. Cyberspace and the "First Battle" in 21st-century War. – Defense Horizons 2009, Vol. 68.
101. Morth, T.A. Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter. – Case Western Reserve Journal of International Law 1998, Vol. 10.
102. Mudrinich, E.M. Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem. – Air Force Law Review 2012, Vol. 68.

103. Murray, A. Uses and Abuses of Cyberspace: Coming to Grips with the Present Dangers. – A. Cassese. Realizing Utopia: The Future of International Law. Oxford: Oxford University Press 2012.
104. Nye Jr, J.S. The Regime Complex for Managing Global Cyber Activities. – Global Commission on Internet Governance 2014.
105. Ohlin, J.D., Govern, K., Finkelstein, C. (eds.). Cyber War: Law and Ethics for Virtual Conflicts. Oxford: Oxford University Press 2015.
106. O'Connell, M.E. Cyber Security Without Cyber War. – Journal of Conflict & Security Law 2012, Vol. 17, No. 2.
107. Onuf, N.G. Sovereignty: Outline of a Conceptual History. – Alternatives: Global, Local, Political Fall 1991, Vol. 16, No. 4.
108. Oppenheim, L. International Law: A Treatise Vol 1, 4th ed. A.D. McNair (ed.) London: Longmans, Green & Co 1928.
109. Oppenheim, L. The Science of International Law: Its Task and Method. – The American Journal of International Law 1908, Vol. 2, No. 2.
110. Palojärvi, P. A Battle of Bits and Bytes: Computer Network Attacks and the Law of Armed Conflict. Helsinki: Publications of the Erik Castrén Institute of International Law and Human Rights, University of Helsinki 2009.
111. Perritt Jr, H.H. Cyberspace and State Sovereignty. – Journal of International Legal Studies 1997, Vol. 3.
112. Philpott, D. Revolutions in Sovereignty: How Ideas Shaped Modern International Relations Princeton: Princeton University Press 2001.
113. Pirker, B. Territorial Sovereignty and Integrity and the Challenges of Cyberspace. – K. Ziolkowski (ed.). Peacetime Regime for State Activities in Cyberspace. Tallinn: NATO CCD COE Publications 2013.
114. Plekksepp, A. Riigi suveräänsus karistusõiguse ajaloolises ja euroopastumise kontekstis. – H. Kalmo, M. Luts-Sootak. Iganenud või igavene? Tekste kaasaegsest suveräänsusest. Tartu: Tartu Ülikooli Kirjastus 2010.
115. Post, D.G. Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace. – Journal of Online Law 1995.
116. Reed, C. Internet Law: Text and Materials, 2nd ed. Cambridge: Cambridge University Press 2004.
117. Rid, T. Cyber War Will Not Take Place. – Journal of Strategic Studies 2013, Vol. 35, No. 1.
118. Rid, T. Cyber War Will Not Take Place. Oxford: Oxford University Press 2013.

119. Roscini, M. Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press 2014.
120. Ross, A. A Textbook of International Law. London. Longmans, Green & Co 1947.
121. Ryan, D.J., Dion, M., Tikk, E., Ryan, J.J.C.H. International Cyberlaw: A Normative Approach. – Georgetown Journal of International Law Summer 2011, Vol. 42, No. 4.
122. Saint Augustine. The City of God, translation, V.J. Bourke et al. New York: Doubleday 1958.
123. Schmitt, C. Political Theology: Four Chapters on the Concept of Sovereignty. Chicago: University of Chicago Press 2005.
124. Schmitt, M.N. "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law. – Virginia Journal of International Law 2014, Vol. 54.
125. Schmitt, M.N. (ed.). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press 2013.
126. Schreuer, C. The Waning of the Sovereign State: Towards a New Paradigm for International Law. – European Journal of International Law 1993, Vol. 4.
127. Schwarzenberger, G. The Forms of Sovereignty. – Current Legal Problems 1957, Vol. 10.
128. Shackelford, S.J. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. – Berkley Journal of International Law 2013, Vol. 27, No. 1.
129. Shackelford, S.J. Managing Cyber Attacks in International Law, Business, and Relations. Cambridge: Cambridge University Press 2014.
130. Shipchandler, S. Note, The Wild Wild Web: Nonregulation as the Answer to the Regulatory Question. – Cornell International Law Journal 2000, Vol. 33.
131. Simma, B., Kahn, D-E., Nolte, G., Paulus, A. (eds.). The Charter of the Uniter Nations. A Commentary. 3rd ed. Volume 1. Oxford: Oxford University Press 2012.
132. Singer, P.W., Friedman, A. Cybersecurity and Cyberwar. Oxford: Oxford University Press 2014.
133. Stone, J. Cyber War Will Take Place! – Journal of Strategic Studies 2013, Vol. 36, No. 1.
134. The Oxford Compact English Dictionary. Oxford: Oxford University Press 2003.
135. Thucydides. History of the Peloponnesian War. The Melian Dialogue. – lygdamus.com/resources/New%20PDFS/Melian.pdf (visited 15.04.2016).
136. Tikk, E., Kaska, K., Vihul, L. International Cyber Incidents, Legal Considerations. Tallinn: NATO CCD COE Publications 2010.

137. Tocci, N. (ed.) Who is a Normative Foreign Policy Actor? The European Union and its Global Partners. – Centre for European Policy Studies 2008, aei.pitt.edu/32609/1/48._Who_is_a_Normative_Foreign_Policy_Actor.pdf (visited 15.04.2016).
138. Todd, G.H. Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition. – Air Force Law Review 2009, Vol. 64.
139. Toffler, A. The Third Wave. New York: Bantam books 1981.
140. Torres Bernárdez, S. Territorial Sovereignty. – R. Bernhardt (ed.). Encyclopedia of Public International Law Vol. IV. Amsterdam: Elsevier 2000.
141. Trachman, J.P. Cyberspace, sovereignty, jurisdiction and modernism. – Indiana Journal of Global Legal Studies 1998, Vol. 5, Iss. 2.
142. Tsagourias, N. Cyber Attacks, Self-Defence and the Problem of Attribution. – Journal of Conflict & Security Law 2012, Vol. 17. No. 2.
143. Tsagourias, N. The Legal Status of Cyberspace. – N. Tsagourias, R. Buchan (eds.). Research Handbook on International Law and Cyberspace. Cheltenham: Edward Elgar Publishing 2015.
144. Walker, P.A. Law of the Horse to Law of the Submarine: The Future of State Behavior in Cyberspace. – M. Maybaum, A-M. Osula, L. Lindström (eds.). 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace. Tallinn: NATO CCD COE Publications 2015.
145. Watts, S. Low-Intensity Computer Network Attack and Self-Defense. – International Law Studies 2011, Vol. 87.
146. Watts, S. Low-Intensity Cyber Operations and the Principle of Non-Intervention. – J.D. Ohlin, K. Govern, C. Finkelstein (eds.). Cyber War: Law and Ethics for Virtual Conflicts. Oxford: Oxford University Press 2015.
147. Waxman, M.C. Cyber Attacks and the Use of Force: Back to the Future of Article 2(4). – Yale Journal of International Law 2011, Vol. 36.
148. Weiss, T.G., Chopra, J. Sovereignty under Siege: From Intervention to Humanitarian Space. – G.M. Lyons, M. Mastanduno (eds.). Beyond Westphalia?: State Sovereignty and International Intervention. Baltimore: Johns Hopkins University Press 1995.
149. Willson, D. A Global Problem. – Armed Forces Journal 2009, www.armedforcesjournal.com/a-global-problem/ (visited 01.04.2016).
150. Wingfield, T.C. The Law of Information Conflict: National Security Law in Cyberspace. Falls Church: Aegis Research Group 2000.
151. Wriston, W.B. Technology and Sovereignty. – Foreign Affairs 1988, Vol. 67.

152. Wu, T., Goldsmith, J. Who Controls the Internet? Illusions of a Borderless World. Oxford: Oxford University Press 2006.
153. Yan, D. Virtual Reality: Can We ride Trademark Law to Surf Cyberspace? – Fordham Intellectual Property, Media & Entertainment Law Journal 2000, Vol. 10.
154. Yannakogeorgos, P.A. Internet Governance and National Security. – Strategic Studies Quarterly Fall 2012.
155. Ziolkowski, K. General Principles of International Law as Applicable in Cyberspace. – K. Ziolkowski (ed.). Peacetime Regime for State Activities in Cyberspace. Tallinn: NATO CCD COE Publications 2013.
156. Ziolkowski, K. Peacetime Cyber Espionage – New Tendencies in Public International Law. – K. Ziolkowski (ed.). Peacetime Regime for State Activities in Cyberspace. Tallinn: NATO CCD COE Publications 2013.

Normative sources

157. Agreement between the Republic of India and the People's Republic of China on trade and intercourse between Tibet region of China and India (Panchseel Treaty). 22.04.1954. – treaties.un.org/doc/publication/unts/volume%20299/v299.pdf (visited 15.04.2016).
158. Charter of the Organization of American States. 30.04.1948 (amended by the protocols 1967, 1985, 1992, 1993). – www.oas.org/dil/treaties_A-41_Charter_of_the_Organization_of_American_States.htm (visited 15.04.2016).
159. Charter of the United Nations. 26 June 1945. – www.un.org/en/charter-united-nations/ (visited 15.04.2016).
160. Constitutive Act of the African Union. 11.07.2000. – www1.uneca.org/Portals/ngm/Documents/Conventions%20and%20Resolutions/constitution.pdf (visited 15.04.2016).
161. Convention on International Civil Aviation. 07.12.1944. – www.icao.int/publications/Documents/7300_cons.pdf (visited 15.04.2016).
162. Convention on the Law of the Sea. 10.12.1982. – www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf (visited 15.05.2016).
163. Convention on the Rights and Duties of States (Montevideo Convention). 26.12.1933. – http://avalon.law.yale.edu/20th_century/intam03.asp (15.04.2016).
164. Montreal Protocol on Substances that Deplete the Ozone Layer. 16.12.1987. – ozone.unep.org/pdfs/Montreal-Protocol2000.pdf (visited 15.04.2016).
165. North Atlantic Treaty. 04.04.1949. – www.nato.int/cps/en/natolive/official_texts_17120.htm (visited 15.04.2016).
166. Pact of the League of Arab States. 22.03.1945. – avalon.law.yale.edu/20th_century/arableag.asp (visited 15.04.2016).
167. Rome Statute of the International Criminal Court. 17.07.1998. – www.icc-cpi.int/nr/rdonlyres/ea9aeff7-5752-4f84-be94-0a655eb30e16/0/rome_statute_english.pdf (visited 15.04.2016).
168. Russian Duma. Bill number 553424-6: On Amendments to Certain Legislative Acts of the Russian Federation (to clarify the processing of personal data in information and telecommunications networks). – asozd2.duma.gov.ru/main.nsf/%28Spravka%29?OpenAgent&RN=553424-6&02 (visited 10.04.2016).

169. Statute of the International Court of Justice. 26.06.1945. – www.icj-cij.org/documents/?p1=4&p2=2 (visited 15.04.2016).
170. Treaty of Amity and Cooperation in Southeast Asia (ASEAN Treaty). 24.02.1976. – www.icnl.org/research/library/files/Transnational/1976Treaty%20.pdf (visited 15.04.2016).
171. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies. 19.12.1966. – www.unoosa.org/pdf/publications/STSPACE11E.pdf (visited 15.04.2016).

Case law

172. PCIJ. 07.02.1923. Nationality Decrees Issued in Tunis and Morocco (French Zone) on November 8th. Advisory Opinion. Series B04.
173. PCIJ. 17.08.1923. Case of the S.S. Wimbeldon. PCIJ Series A, No 1.
174. PCIJ. 07.09.1927. Case of S.S. Lotus (Turkey v. France). PCIJ Series A, No. 10.
175. PCA. 04.04.1928. Island of Palmas case (Netherlands. v. US). Reports of International Arbitral Awards, Vol. 2.
176. PCIJ. 05.09.1931. Customs Regime Between Germany and Austria. Advisory Opinion. Series A/B 41.
177. PCIJ. 07.07.1932. Free Zones of Upper Savoy and the District of Gex. PCIJ Series A/B, No. 46.
178. ICJ. 09.04.1949. Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. Albania). ICJ Reports 1949.
179. ICJ. 11.04.1949. Reparation for Injuries Suffered in the Service of the United Nations. Advisory Opinion. ICJ Reports 1949.
180. ICJ. 26.11.1984. Military and Paramilitary Activities in and Against Nicaragua (Nicaragua. v. IS), Jurisdiction of the Court and Admissibility of the Application. ICJ Reports 1984.
181. ICJ. 27.06.1986. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States). ICJ Reports 1986.

United Nations documents

182. UN Disarmament Committee. A/C.1/53/3. 30.09.1998. Letter Dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations Addressed to the Secretary-General.
183. UNGA. A/RES/57/239. 20.12.2002. Creation of a Global Culture of Cybersecurity.
184. UNGA. A/RES/58/199. 23.12.2003. Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures.
185. UNGA. A/CN.4/L.682. 13.04.2006. Fragmentation of International Law: Difficulties Arising From the Diversification and Expansion of International Law. Report of the Study Group of the International Law Commission. Finalized by Martti Koskenniemi.
186. UNGA. A/61/161. 18.07.2006. Developments in the Field of Information and Telecommunications in the Context of International Security.
187. UNGA. A/CN.4/L.702. 18.07.2006. Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law. Report of the Study Group of International Law Commission.
188. UNGA. A/65/201. 30.07.2010. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General.
189. UNGA. A/66/152. 15.07.2011. Developments in the field of information and telecommunications in the context of international security, reply from the US Government.
190. UNGA. A/55/359. 14.09.2011. 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.
191. UNGA. A/68/98. 24.06.2013. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by Secretary-General.
192. UNGA. A/69/723. 13.01.2015. Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.
193. UNGA. A/70/174. 22.07.2015. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General.

Other sources

194. Aiken, K. Woodall, J. Tallinn 2.0: cyberspace and the law. – The Strategist, Australian Strategic Policy Institute, 14.05.2015, www.aspistrategist.org.au/tallinn-2-0-cyberspace-and-the-law/ (visited 20.04.2016).
195. AMICC. Bush Approach to the ICC. Suspension of the Rome Statute Signature: The US Disengages. – www.amicc.org/usicc/bush (visited 10.04.2016).
196. Australian Government. Cyber Security. – www.ag.gov.au/RightsAndProtections/CyberSecurity/Pages/default.aspx (visited 10.03.2016).
197. Barlow, J.P. A Declaration of Independence of Cyberspace. – 1996, projects.eff.org/~barlow/Declaration-Final.html (visited 10.04.2016).
198. Brooks, B., Bajak, F. Brazil Looks to Break Free from U.S.-Centric Internet. – TPM, 17.09.2013, talkingpointsmemo.com/idealab/brazil-looks-to-break-from-u-s-centric-internet (visited 20.04.2016).
199. Charney, S., Werner, E.T. Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust. – Microsoft, 26.07.2011, 6, www.microsoft.com/en-us/download/details.aspx?id=26826 (visited 10.04.2016).
200. Clapper, J.R. Statement for the Record. Worldwide Cyber Threats. – House Permanent Select Committee on Intelligence, 10.09.2015, fas.org/irp/congress/2015_hr/091015clapper.pdf (visited 15.04.2016).
201. Cyber Policy Institute. Table: Internet Bans. – 20.04.2016.
202. Cyber Policy Institute. State Practice and International Law in Cyberspace: A Study of Major Cyber Incidents and Applicable Law. – forthcoming at the Conference on State Practice and the Future of International Law in Cyberspace, 05.05.2016.
203. Daniel, M. 007 or DDoS: What is Real World Cyber? – 28.02.2013. Remarks as prepared for delivery by special assistant to the president and White House cybersecurity coordinator. RSA Conference USA 2013 San Francisco.
204. Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J. Access Denied: The Practice and Policy of Global Internet Filtering. Cambridge: MIT Press 2008.
205. Federal Bureau of Investigation. Update of Sony Investigation. – FBI National Press Office. 19.12.2014, www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (visited 01.04.2016).
206. Flock, E. Operation Cupcake: MI6 Replaces al-Qaeda Bomb-Making Instructions with Cupcake Recipes. – Washington Post, 03.06.2011,

www.washingtonpost.com/blogs/blogpost/post/operation-cupcake-mi6-replaces-al-qaeda-bomb-making-instructions-with-cupcake-recipes/2011/06/03/AGFUP2HH_blog.html (visited 01.04.2016).

207. France's Strategy. Information systems defence and security. – 2011, www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf (visited 10.03.2016).
208. General Keith B. Alexander's keynote address to senior government security officials and industry executives attending a cybersecurity conference. – 30.10.2013, archive.defense.gov/news/newsarticle.aspx?id=121030 (visited 25 March 2016).
209. Global Conference on CyberSecurity 2015. – www.gccs2015.com (15.04.2016).
210. Google Transparency Report. Recent and ongoing disruptions of traffic to Google products. – www.google.com/transparencyreport/traffic/#expand=CG (visited 20.04.2016).
211. Greenberg, A. It's Been 20 Years Since This Man Declared Cyberspace Independence. – Wired, 08.02.2016, www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/ (visited 20.04.2016).
212. India's Ministry of Communications and Information Technology. Department of Electronics and Information Technology. National Cyber Security Policy. – 02.07.2013, deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf (visited 10.04.2016).
213. Institute of Information Security Issues of Moscow State University and Conflict Studies Research Centre. Russia's "Draft Convention on International Information Security", A Commentary. – 2012, www.academia.edu/1611951/Russia_s_Draft_Convention_on_International_Information_Security_-_A_Commentary (visited 10.03.2016).
214. Interfax. Putin: cyber espionage is direct violation of State's sovereignty. – 11.07.2014, www.interfax.com/newsinf.asp?id=519963 (visited 20.04.2016).
215. International Institute of Humanitarian Law. San Remo Handbook on Rules of Engagement. – 2009, www.iihl.org/Media/Default/PDF/Publications/RoE/ROE%20HANDBOOK%20ENGLISH%2009.05.2011%20PRINT%20RUN.pdf (visited 20.03.2016).

216. ISO, IEC. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity. – www.iso27001security.com/html/27032.html (visited 10.03.2016).
217. Jinping, X. Address by H.E. Mr. Xi Jinping President of the People's Republic of China At Meeting Marking the 60th Anniversary Of the Initiation of the Five Principles of Peaceful Coexistence: Carry forward the Five Principles of Peaceful Coexistence to build a better world through win-win cooperation. – 28.06.2014, www.china.org.cn/world/2014-07/07/content_32876905.htm (visited 30.04.2016).
218. Kane, A. Remark at the Global Conference on Cyberspace 2015 ICT4Peace Panel on Norms of International Peace and Security in Cyberspace. – 17.04.2015.
219. Koskenniemi, M. Lecture on Politics of International Law at the Lauterpacht Centre for International Law, University of Cambridge. – 26.01.2012, www.youtube.com/watch?v=-E3AGVTHsq4 (visited 30.04.2016).
220. Liebelson, D. Map: Here are the Countries the Block Facebook, Twitter, and Youtube. – 28.03.2014, www.motherjones.com/politics/2014/03/turkey-facebook-youtube-twitter-blocked (visited 20.04.2016).
221. Lindsay, J.R., Cheung, T.M., Reveron, D.S. China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain. Oxford: Oxford University Press 2015.
222. 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. – 05.10.2012; www.dot.gov.in/sites/default/files/5-10-12.PDF (visited 10.04.2016).
223. Nakashima, E. U.S. rallied multinational response to 2012 cyberattack on American banks. – Washington Post, 11.04.2014, www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html (visited 04.04.2016).
224. NATO CCD COE. Cyber Definitions Database. – ccdcoe.org/cyber-definitions.html (visited 15.03.2016).
225. NATO. Wales Summit Declaration. – 05.09.2014, www.nato.int/cps/en/natohq/official_texts_112964.htm (visited 30.04.2016).
226. OpenNet Inititive. Social Media Filtering Map. – opennet.net/research/map/socialmedia (visited 20.04.2016).

227. Panetta, L.E. Remarks by Secretary Panetta on Cybersecurity to the Business Execturives for National Security. – 11.10.2013, www.cfr.org/cybersecurity/secretary-panettas-speech-cybersecurity/p29262 (visited 01.04.2016).
228. Perera, D. Schmidle: Cyber Ops Might Require New Combatant Command Structure. – FierceGovernmentIT, 15.05.2011, www.fiercegovernmentit.com/story/schmidle-cyber-ops-might-require-new-combatant-command-structure/2011-05-15 (visited 15.04.2016).
229. Qiang, X. How China's Internet Police Control Speech on the Internet. – Radio Free Asia, 24.11.2008, www.rfa.org/english/commentaries/china_internet-11242008134108.html (visited 20.04.2016).
230. Remarks by H.E. Xi Jinping, President of the People's Republic of China at the opening ceremony of the Second World Internet Conference. – 16.12.2015, www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml (visited 16.04.2016).
231. Ries, B. Twitter Blocks Pro-Ukrainian Political Account for Russian Users. – Mashable, 19.05.2014, mashable.com/2014/05/19/twitter-blocks-account-russia/#Kl0O_zOuIZq9 (visited 20.04.2016).
232. Rothrock, K. Twitter "Blocks" Access to Russia's Most Infamous Hackers. – Advox, Global Voices, 28.07.2014, advox.globalvoices.org/2014/07/28/twitter-blocks-access-to-russias-most-infamous-hackers/ (visited 20.04.2016).
233. Security Council of the Russian Federation. On the National Security Strategy of the United States of America. – 25.03.2015, www.scrf.gov.ru/news/865.html (visited 20.04.2016).
234. TechTarget. Distributed Denial-of-Service Attack Definition. – searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack (visited 20.03.2016).
235. The White House. President of the United States of America. International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World. – May 2011, www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (visited 20.04.2016).
236. The White House. Remarks by the President in Year-End Press Conference. – 19.12.2014, www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference (visited 30.04.2016).

237. Tikk-Ringas, E. Presentation at UNIDIR International Security Cyber Issues Workshop Series: The Application of International Law in the Context of International Cybersecurity. – 19-21.04.2016, www.unidir.org/programmes/emerging-security-threats/international-security-cyber-issues-workshop-series/international-security-cyber-issues-workshop-series-the-application-of-international-law-in-the-context-of-international-cybersecurity (visited 25.04.2016).
238. Tikk-Ringas, E., Spirito, C. Lecture series on Information Infrastructure and Architecture at University of Tartu. – Autumn 2014/2015, www.uttv.ee/naita?id=20298&sessioon=41911740494863030249 (visited 10.03.2016).
239. UN Office for Disarmament Affairs. GGE Information Security. – www.un.org/disarmament/topics/informationsecurity/ (visited 20.04.2016).
240. US Congress House of Representatives. Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE. – 08.10.2012, intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf (visited 15.04.2016).
241. US Department of Defence. The Strategy for Homeland Defense and Civil Support. – 2005, www.hsdl.org/?view&did=454976 (visited 20.03.2016).
242. US Department of Defense. Dictionary of Military and Associated Terms. – Joint Publication 1-02, 08.11.2010 (as amended through 15.02.2016), www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (visited 15.04.2016).
243. US Department of Defense. The Department of Defense Cyber Strategy. – April 2015, www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (visited 01.04.2016).
244. Van Der Meer, S. Foreign Policy Responses to International Cyber-attacks, Some Lessons Learned. – Clingendael, Netherland's Institute for International Relations 2015, www.clingendael.nl/sites/default/files/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf (visited 10.03.20156).
245. Various authors. Open Letter to President George W. Bush. – 2002, www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/letter.html (visited 20.03.2016).

246. World Economic Forum. The Global Information Technology Report 2015: ICTs for Inclusive Growth. – 2015, www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf (visited 15.04.2016).
247. Worldcrunch. China and Russia Forge Cybersecurity Partnership without the US. – TheWorldPost. 30.10.2014. www.huffingtonpost.com/worldcrunch/why-russia-and-china-see-_b_6071528.html (visited 15.04.2016).
248. Zhe, H., Shi, T. China Security Bill Calls for Protecting 'Cyber Sovereignty'. – Bloomberg Technology, 09.05.2015, www.bloomberg.com/news/articles/2015-05-08/new-china-security-bill-calls-for-protecting-cyber-sovereignty- (visited 10.04.2016).

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Liisi Adamson (sünnikuupäev: 29.03.1991)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Sovereignty in cyberspace: organised hypocrisy?" (Suveräänsus küberruumis: organiseeritud silmakirjalikkus?), mille juhendaja on Lauri Mälksoo,

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, 02.05.2016