UNIVERSITY OF TURKU
Faculty of Law

False Comfort from Nuclear Analogies: How International Trade Restrictions Apply to Cyberspace

Eeva Laukkanen

Advanced International Law and Technology

University of Turku, Faculty of Law

May 2022

UNIVERSITY OF TURKU
Faculty of Law

Abstract page

EEVA LAUKKANEN: False Comfort from Nuclear Analogies: How International Trade Restrictions Apply to Cyberspace

Master's Thesis, 54 p.
Advanced International Law and Technology
May 2022

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin OriginalityCheck service.

This thesis evaluates the international legal framework of trade restrictions in the context of cyberspace. Certain cyber goods are recognized as dual-use goods based on their potential military applications. Thereby, the existing legal framework for governing the trade of sensitive goods is extended analogically to apply to cyber goods. The first research question presented in this paper is whether international law includes a legal basis for using trade policy as a measure for security governance in cyberspace. To answer this research question, the paper evaluates how security interests are regarded in trade policy. This evaluation is conducted by analysing the nature of security interests with the constructivist method and reviewing the General Agreement on Tariffs and Trade with the *de lege lata* approach. The second research question evaluates whether trade policy is a suitable model for governing threats in the cyberspace. This research question covers the evaluation of existing non-proliferation focused trade policies, mainly the Wassenaar Arrangement, and grounds for applying the same approach to cyber goods. This evaluation also includes observing the nature of cyber goods and the cyber goods industry with a socio-legal method. Dual-use nuclear goods are used as a reference point in a comparison between cyber goods and conventional dual-use goods.

The purpose of the thesis is to examine the implications of applying trade policy as a security measure in cyberspace. The choice of extending an existing legal framework instead of establishing a separate framework specifically for cyberspace may have a broader impact on the legal status of cyberspace. The paper evaluates whether the current legal approach to governing dual-use cyber goods takes into account the nature of cyberspace in an adequate manner.

This paper concludes that international trade law provides a legal basis for imposing trade restrictions for cyber goods based on security interests. However, the analogical extension of the non-proliferation focused trade policy framework does not fully adapt to the nature of cyber goods and the cyber goods industry. Thereby, the current model for the governance of dual-use cyber goods may result in negative effects in the industry by restricting trade without providing equivalent benefit in the form of decreasing cyber risks. The possible solutions proposed based on the research conducted in this paper include incorporating views and practices of private sector stakeholders as an essential input in any regulation related to cyberspace, establishing a separate cyber convention for properly defining the legal status of cyberspace, and promoting global initiatives for cyber resilience.

***Key words**: International law, technology, dual-use goods, cyberspace, cyberattacks, trade policy, cyber goods, security governance*

Table of contents

References

Bibliography

Aarnio, A., Luentoja lainopillisen tutkimuksen teoriasta. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja 2011.

Andress, J. – Winterfeld, S., Cyber warfare: techniques, tactics and tools for security practitioners. Elsevier 2013.

Ashley, W., A retrospect of free-trade doctrine. The Economic Journal, 34(136) 1924, p. 501.

Aubin, Y. – Idiart, A. (eds.), Export control law and regulations handbook: a practical guide to military and dual-use goods trade restrictions and compliance. Kluwer Law International BV 2016.

Baker, S. – Filipiak, N. – Timlin, K., In the Dark. McAfee, Inc. and the Center for Strategic and International Studies 2011.

Barbieri, C. – Darnis, J.P. – Polito, C., Non-proliferation Regime for Cyber Weapons. A Tentative Study. Documenti IAI, 18(03) 2018.

Black-Branch, J., Nuclear terrorism by states and non-state actors: global responses to threats to military and human security in international law. Journal of Conflict and Security Law, 22(2) 2017, p. 201.

Blank, S., Cyber war and information war a la russe, 2017. In Perkovich, G. – Levite, A.E. (eds.), Understanding Cyber Conflict: Fourteen Analogies. Georgetown University Press 2017, p. 81.

Catrain, L. – Peters, B. – Boyette, H. – Lock, C., Embargoes and Related Sanctions (European Union and United States Perspective), 2016. In Aubin, Y. – Idiart, A. (eds.), Export control law and regulations handbook: a practical guide to military and dual-use goods trade restrictions and compliance. Kluwer Law International BV 2016, p. 15.

Chang, H.J., Kicking away the ladder: the "real" history of free trade, 2003. In Shaikh, A. (ed.), Globalization and the Myths of Free Trade: History, Theory and Empirical Evidence. Routledge 2007, p. 23.

Cotterrell, R., Why Must Legal Ideas Be Interpreted Sociologically? Journal of law and society. 25 (2) 1998, p. 171.

Egeland, K., A theory of nuclear disarmament: Cases, analogies, and the role of the non-proliferation regime. Contemporary Security Policy, 43/2022, p. 106.

Enderwick, P., Understanding the rise of global protectionism. Thunderbird International Business Review, 53(3) 2011, p. 325.

Fellmeth, A.X. – Horwitz, M., Guide to Latin in international law. Oxford University Press 2021.

Grimmett, R.F., Military technology and conventional weapons export controls: the Wassenaar Arrangement. Library of Congress Washington DC Congressional Research Service, 2006.

Henckels, C., Permission to act: the legal character of general and security exceptions in international trade and investment law. International & Comparative Law Quarterly, 69(3) 2020, p. 557.

Herr, T., Malware counter-proliferation and the Wassenaar Arrangement. 8th International Conference on Cyber Conflict, IEEE 2016, p. 175.

Humphrey, W.S. – Over, J.W., Leadership, teamwork, and trust: Building a competitive software capability. Addison-Wesley Professional 2010.

Inkster, N., Information warfare and the US presidential election. Survival, 58(5) 2016, p. 23.

Kohl, U., Jurisdiction in cyberspace. Research Handbook on International Law and Cyberspace. Edward Elgar Publishing 2015.

Krahmann, E., Conceptualizing security governance. Cooperation and conflict, 38(1) 2003, p. 5.

Limnéll, J., The exploitation of cyber domain as part of warfare: Russo-Ukrainian war. International Journal of Cyber-Security and Digital Forensics, 4(4) 2015, p. 521.

Macdonald, M. – Frank, R., The network structure of malware development, deployment and distribution. Global Crime, 18(1) 2017, p. 49.

Makinda, S.M., Sovereignty and global security. Security Dialogue, 29(3) 1998, p. 281.

Mauroni, A.J., Countering Weapons of Mass Destruction: Assessing the US Government's Policy. Rowman & Litterfield Publishers 2016.

Miller, S.E., Cyber Threats, Nuclear Analogies? Divergent Trajectories in Adapting to New Dual-Use Technologies, 2017. In Perkovich, G. – Levite, A.E. (eds.), Understanding Cyber Conflict: Fourteen Analogies. Georgetown University Press 2017, p. 161.

Nayyar, D., Globalization and free trade: theory, history, and reality, 2006. In Shaikh, A. (ed.), Globalization and the Myths of Free Trade-History, Theory, and Empirical Evidence. Routledge 2007, p. 69.

Nye Jr, J.S., Deterrence and dissuasion in cyberspace. International security, 41(3) 2016, p. 44.

Olson, P., We are anonymous. Random House 2013.

Paulson, S.L., Hand Kelsen's Earliest Legal Theory: Critical Constructivism. Mod. L. Rev., 59/1996, p.797.

Pearson, Z., Non-Governmental Organisations and International Law: Mapping New Mechanisms for Governance. Aust. YBIL, 23/2004, p.73.

Perkovich, G. – Levite, A.E. eds., Understanding Cyber Conflict: Fourteen Analogies. Georgetown University Press 2017.

Reeder, J.R. – Hall, T., Cybersecurity's Pearl Harbor Moment. The Cyber Defense Review, 6(3) 2021, p. 15.

Roche, E.M. – Blaine, M.J., International convention for the peaceful use of cyberspace. Orbis, 58(2) 2014, p. 282.

Russell, J., Russell Einstein Manifesto. Book On Demand Limited 2012.

Sabillon, R. – Cavaller, V. – Cano, J., National cyber security strategies: global trends in cyberspace. International Journal of Computer Science and Software Engineering, 5(5) 2016, p. 67.

Schmitt, M.N. (ed.), Tallinn Manual 2.0 on the international law applicable to cyber operations. Cambridge University Press 2017.

Schroeder, U., The Transformation of Security Concepts, 2021. In Geiß, R. – Melzer, N. (eds.), The Oxford Handbook of the International Law of Global Security. Oxford University Press 2021, p. 54.

Shaffer, G., The New Legal Realist Approach to International Law. Leiden Journal of International Law, 28(2) 2015, p. 189.

Shaikh, A., Globalization and the myths of free trade. Routledge 2006.

Sokova, E., Non-state actors and nuclear weapons, 2017. In Borrie, J. – Caughley, T. – Wan, W. (eds.), Understanding Nuclear Weapon Risks, UNIDIR Report, 87/2017, p. 83.

Sommer, P., Criminalising hacking tools. Digital investigation, 3(2) 2006, p. 68.

Stevens, C., Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet. Contemporary Security Policy, 41(1) 2020, p. 129.

Stockholm International Peace Research Institute, SIPRI Yearbook 2021. Oxford University Press 2021.

Tsagourias, N., The legal status of cyberspace, 2015. In Tsagourias, N. – Buchan, R. (eds.), Research handbook on international law and cyberspace. Edward Elgar Publishing 2021, p. 9.

Tsvetanov, T. – Slaria, S., The effect of the Colonial Pipeline shutdown on gasoline prices. Economics Letters, 209/2021, p. 110.

Valverde, M., Analyzing the governance of security: Jurisdiction and scale. Behemoth - A Journal on Civilisation, 1(1) 2008, p. 3.

Wolfers, A., "National security" as an ambiguous symbol. Political science quarterly, 67(4) 1952, p. 481.

Zeiler, T.W., Managing protectionism: American trade policy in the early cold war. Diplomatic History, 22(3) 1998, p. 337.

Zetter, K., Countdown to zero day: Stuxnet and the launch of the world's first digital weapon. Broadway books 2014.

Official sources

European Commission, Communication to the Council and the European Parliament: Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre (COM/2012/0140), EUR-Lex 2012.

European Commission, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (JOIN/2013/01), EUR-Lex 2013.

European Council Decision 2017/809, 11.5.2017.

European Council, Weapons of mass destruction: combating proliferation. EUR-Lex 2.3.2018 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al33234 accessed on 9.3.2022).

GATT 1949, Article XXI – United States Export Restrictions, Czechoslovakia v. United States.

GATT, Summary record of the Thirtieth Session (C/W/264/Add.1), 1975.

GATT, Summary Record of the Twenty-Second Meeting (CP3/SR22 – II/28), 1949.

IAEA, Statute of the International Atomic Energy Agency, IAEA 1956.

U.S. Bureau of Democracy, Human Rights and Labor, Country Reports on Human Rights Practices for 2015. U.S. Department of State 2015.

U.S. Department of Commerce's Bureau of Industry and Security, Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items. Bureau of Industry and Security 2015.

U.S. Department of State, Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments. U.S. Department of State 2021.

U.S. Department of State, Proposals for Expansion of World Trade and Employment, U.S. Department of State 1945.

U.S. Joint Chiefs of Staff, The national military strategy of the United States of America. U.S. Joint Chiefs of Staff 2004.

United Nations General Assembly, Rome Statute of the International Criminal Court. United Nations General Assembly 1998.

Wassenaar Arrangement, Explanatory Note: Elements for Objective Analysis and Advice Concerning Potentially Destabilizing Accumulations of Conventional Weapons. Wassenaar Arrangement 1998.

Wassenaar Arrangement, Public Documents Volume I: Founding Documents. Wassenaar Arrangement 1995.

Wassenaar Arrangement, Public Documents Volume II: List of Dual-Use Goods and Technologies and Munitions List. Wassenaar Arrangement 1995.

Wassenaar Arrangement, Public Documents Volume III: Compendium of Best Practice Documents. Wassenaar Arrangement 1995.

Wassenaar Arrangement, Public Documents Volume IV: Plenary-related and Other Statements. Wassenaar Arrangement 1995.

Wassenaar Arrangement, Summary of Changes List of Dual-Use Goods & Technologies and Munitions List. Wassenaar Arrangement 2017.

Wassenaar Arrangement, Plenary Session: Revisions to the Commerce Control List Related to WA 2016 Plenary Agreements. Wassenaar Arrangement 2016.

WTO 2019, Traffic in Transit, Russia v. Ukraine (DS512).

WTO, Agreement on Technical Barriers to Trade. WTO 1995.

Online references

Arms Control Association, The Wassenaar Arrangement at a Glance. Arms Control Association 2/2022 (https://www.armscontrol.org/factsheets/wassenaar accessed on 3.3.2022).

Arms Control Association, Estimated Global Nuclear Warhead Inventories statistic. Arms Control Association 1/2022 (https://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat accessed on 9.2.2022).

Cardozo, N. – Galperin, E., Victory! State Department Will Try to Fix Wassenaar Arrangement. Electronic Frontier Foundation 29.2.2016 (https://www.eff.org/deeplinks/2016/02/victory-state-department-will-try-fix-wassenaar-arrangement, accessed on 4.1.2022).

EDRi, Amesys – Complicity in torture: surveillance tech export control needed. EDRi 23.5.2012 (https://edri.org/our-work/edrigramnumber10-10amesys-complicity-in-torture/ accessed on 18.3.2022).

Galperin, E., What Is the U.S. Doing About Wassenaar, and Why Do We Need to Fight It? Electronic Frontier Foundation 28.5.2015 (https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation accessed on 4.1.2022).

Galperin, E., Commerce Department FAQ on Proposed Wassenaar Implementation Gives Answers, Raises More Questions. Electronic Frontier Foundation 12.6.2015 (https://www.eff.org/deeplinks/2015/06/commerce-department-faq-proposed-wassenaar-implementation-gives-answers-raises accessed on 4.1.2022).

Herjavec Group, 2017 Cybercrime Report. Herjavec Group 18.10.2017 (https://www.herjavecgroup.com/cybercrime-report-2017/ accessed on 18.1.2022).

Kluth, Andreas, This Nuclear Arms Race Is Worse Than the Last One. Bloomberg Opinion 18.6.2020 (https://www.bloomberg.com/opinion/articles/2020-06-18/this-nuclear-arms-race-is-worse-than-the-lastone accessed on 11.3.2022).

Marquis-Boire, M., Backdoors are Forever - Hacking Team and the Targeting of Dissent. The Citizen Lab 10.10.2012 (https://citizenlab.ca/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/ accessed on 18.3.2022)

McAfee: What is Stuxnet? (https://www.mcafee.com/enterprise/en-gb/security-awareness/ransomware/what-is-stuxnet.html#:~:text=Stuxnet%20is%20a%20computer%20worm,used%20to%20automate%20machine%20processes. accessed on 18.11.2021)

Merriam-Webster Dictionary, Laissez-faire (https://www.merriam-webster.com/dictionary/laissez-faire accessed on 23.11.2021).

Merriam-Webster Dictionary, Zero-day vulnerability (https://www.merriam-webster.com/dictionary/zero-day accessed on 23.11.2021).

NATO, NATO Industry Cyber Partnership (https://www.ncia.nato.int/business/partnerships/nato-industry-cyber-partnership.html accessed on 9.2.2022).

Statista, Worldwide digital population as of January 2022. Statista 26.4.2022 (https://www.statista.com/statistics/617136/digital-population-worldwide/ accessed on 28.4.2022).

Turton, W. – Mehrotra, K, Hackers Breached Colonial Pipeline Using Compromised Password. Bloomberg 4.6.2021 (https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password accessed on 11.12.2021).

World Nuclear Association, The Many Uses of Nuclear Technology. World Nuclear Association 5/2021 (https://world-nuclear.org/information-library/non-power-nuclear-applications/overview/the-many-uses-of-nuclear-technology.aspx accessed on 4.1.2022).

Abbreviations

Bureau of Industry and Security	BIS
Central Intelligence Agency	CIA
Coordinating Committee for Multilateral Export Controls	CoCom
Distributed Denial of Service attack	DDOS
Electronic Weapons of Mass Destruction	eWMD
General Agreement on Tariffs and Trade	GATT
International Atomic Energy Agency	IAEA
North Atlantic Treaty Organization	NATO
Treaty on the Non-Proliferation of Nuclear Weapons	NPT
Non-Nuclear-Weapon State	NNWS
Nuclear-Weapon State	NWS
United Nations	UN
United States	U.S.
Wassenaar Arrangement	WA
Weapons of Mass Destruction	WMD
Weapons of Mass Destruction or Effect	WMD/E
World Trade Organization	WTO

1 Introduction

1.1 Introducing the topic and setting the societal framework

1.1.1 The ever-changing international threat landscape

404 page not found. Servers down, program not answering. A few decades ago, receiving a message like this on a computer screen would have caused minor nuisance at worst. It may have meant that some information was missing, or a service was temporarily unavailable. There was, however, rarely a need for further concern. Through digitalization more and more of our daily lives are attached to the internet and various computer systems, and thus encountering errors in cyberspace[1] is more likely than ever and their consequences may be severe. For essential organizations, such as banks, electrical power plants or government offices, a seemingly minor technical problem may indicate that the organization's operations are at stake due to a cyberattack. A simple error message could indicate that massive countermeasures need to be implemented to avoid the severe consequences a cyberattack may cause. Cyberspace has significance for almost all our everyday activities from retrieving information to connecting people. Regardless of the term cyberspace having a sci-fi-like resemblance, its legal aspects are already governed as any other fundamental aspect of the society.

Practically all industries are connected to computer networks in some way. The increase in data utilization has arguably changed how organizations, individuals, and states interact and operate. Like Microsoft's CEO Satya Nadella has repeatedly stated, every company is a software company.[2] The driving force of digitalization has not skipped the public sector either, resulting in most governmental operations being just as dependent on computer systems as private actors are. As computer systems have achieved a fundamental role in how institutions and infrastructure function, they have become more favourable targets for malicious attacks. Cybercrime has become a significant industry, which, by some estimates, costs the global society $6 trillion annually.[3] Since cyberattacks affect private companies and public entities alike, the incentives behind an attack may range from vandalism or pursuing monetary profit to causing international conflict or warfare. Since the society has grown to being deeply reliant on computer systems and the internet, attacks on these systems cannot be overlooked. Whereas

[1] Cyberspace can be defined as a global domain that lacks physicality and is virtual in nature. Cyberspace consists of a physical layer (hardware and other infrastructure), logical layer (connections between devices), and social layer (individuals and groups engaging in cyber activities). See more on the Tallinn Manual 2.0.
[2] Microsoft's Satya Nadella has repeatedly made the phrase known, but the quote is originally by Watts S. Humphrey. See e.g., Humphrey – Over 2010.
[3] Herjavec Group 18.10.2017.

causing damage or interfering with another state's operations previously required having some physical presence in the targeted territory, cyberspace has a reach beyond any physical domains.

Due to the significance cyberspace has in the modern society, it has created a new realm for conflict. Besides conventional military operations taking place on land, sea, air, and space, cyberspace is considered as a fifth dimension which has rules and logic of its own.[4] The virtual nature of cyberspace changes what measures are feasible in a conflict situation. Cyberspace is not fully tied to a specific location or physical resources, which enables discreet but impactful operations, such as information manipulation or network interference. The rapid pace of technological development has created regulatory challenges. New threats demand fast and efficient solutions, which legislative processes may not always facilitate. During the beginning of the 21st century, the most significant cyberattacks have been distinguished into their own category of international conflict, cyber warfare. The urgency of the matter is undeniable, since cyberattacks have already proven to be capable of causing political or economic turbulence, information manipulation or even physical damage.[5] Adapting to the changing threat landscape requires states and international organizations to establish new measures, since the capabilities and character of cyber technologies exceeds what has previously been considered as conflict.

1.1.2 Seeking parallels from existing terminology

Since the problems arising from operating in cyberspace have emerged in the last few decades, its terminology is still only forming and constantly evolving. Regardless, defining the scope of cyber operations helps determining how cyberspace differs from the conventional domains. In order to define cyber operations, reference can be sought from how international conflicts are generally evaluated in international law. The Protocol Additional to the Geneva Convention Relative to the Protection of Civilian Persons in Time of War, 12 August 1949, defines attacks in the following way:

> *1. "Attacks" means acts of violence against the adversary, whether in offence or in defence.*
>
> *2. The provisions of this Protocol with respect to attacks apply to all attacks in whatever territory conducted, including the national territory belonging to a Party to the conflict but under the control of an adverse Party.*
>
> *3. The provisions of this Section apply to any land, air or sea warfare which may affect the civilian population, individual civilians or civilian objects on land. They*

[4] See e.g., Tsagourias 2015.
[5] Perkovich – Levite 2017, p. 6.

> *further apply to all attacks from the sea or from the air against objectives on land but do not otherwise affect the rules of international law applicable in armed conflict at sea or in the air.*

When defining an attack, it can be observed that an attack can be either offensive or defensive, it can take place on any territory, and it can affect either people or objects. Similar elements can be recognized in the definition of cyberattacks. In the Tallinn Manual 2.0 cyberattacks are defined in the following way:

> *A 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.*[6]

The definition refers to 'attack' similarly as is understood in conventional domains, leading to certain limitations. The cyberattack definition provided in the Tallin Manual shares some of the same elements as the definition of conventional attacks. Like other attacks, cyberattacks can also be either offensive or defensive and affect either people or objects. In the same manner, many other general principles of the law of armed conflict apply to cyberattack, such as the general prohibition of targeting civilians or civilian objects in attacks.[7] Attack is construed as an act of violence, leaving non-violent cyber operations such as espionage or information warfare outside the definition's scope. In cyberattacks, the violent nature is reflected through the consequences, extending the definition outside of mere kinetic violence.[8] The analogical extension of the term 'attack' to cover certain operations in cyberspace is one example of how pre-existing concepts can be used as tools to navigate the obscurity of cyberspace. The shared elements in the terminology of conventional attacks and cyberattacks demonstrates that operations in cyberspace can be evaluated with similar criteria as operations on conventional domains. Nonetheless, focusing merely on the common ground of conventional attacks and cyberattacks may be misleading. The concept of security at large is exceeding the state-centric understanding of the matter[9] as conflicts seize global arenas, such as cyberspace. The similarities between cyberattacks and conventional attacks as terms in international law do not yet entail that cyberspace and conventional domains could or should be assimilated in a broader context. In the following sub-section, three examples of cyber operations are evaluated to further describe what security threats in cyberspace may entail.

---

[6] Tallinn Manual 2.0, Rule 92.
[7] Tallinn Manual 2.0, Rule 94 and 99.
[8] Tallinn Manual 2.0, Rule 92, paragraph 3.
[9] See e.g., Schroeder 2021.

1.1.3 Examples of past cyber operations

In 2007, Estonia was targeted by a series of cyber operations that actively impacted the country for almost a month before the affected systems could be recovered. The cyberattack temporarily immobilized part of Estonia's essential infrastructure by targeting technology-based services, such as government offices, bank services, and communication networks.[10] Various techniques were used to conduct the attack, including distributed denial of service attacks (DDOS) and botnets.[11] The attacks were traced to have been operated by hackers from around the world, but the attacks were allegedly coordinated by Russia.[12] The operation can be evaluated with similar criteria as if it would have taken place on land, sea, or air. Applying the Tallinn Manual's definition of a cyberattack, the cyber operation has similar traits as a conventional act of violence. The Estonia cyberattack was an *offensive cyber operation* which caused *damage or destruction to objects*. By extending what is generally comprehended as damage, destruction, or conflict, operations in cyberspace may be evaluated more easily regardless of the disrupting nature of cyberspace.

In 2010 the Stuxnet virus was discovered, providing a preview of what digital warfare could look like.[13] Stuxnet was a highly destructive computer worm, that was created to attack Iran's uranium enrichment facilities.[14] The Stuxnet virus has been described as the world's first digital weapon because of its capability of affecting hardware.[15] The virus exploited a zero-day exploit[16] in the Windows operating system to install a virus that was capable of taking control of programmable industrial control systems and causing the equipment controlled by those systems to malfunction.[17] The significance of Stuxnet was not limited to infiltrating Iran's nuclear program, since it eventually spread onto millions of other computers running the Windows operating system.[18] The Stuxnet attack's significance is further increased by the assumption that its creation was a joint effort by the U.S. National Security Agency, the Central Intelligence Agency (CIA), and Israeli intelligence.[19] Similar to the cyberattack in Estonia, the Stuxnet attack demonstrates that operations in cyberspace can lead to similar consequences as

[10] Blank, 2017, p. 85.
[11] Ibid.
[12] Nye Jr. 2016, p. 48.
[13] Zetter 2014, p. 3.
[14] Ibid.
[15] McAfee "What is Stuxnet?".
[16] Defined by Merriam-Webster Dictionary as a vulnerability (as in a computer or computer system) that is discovered and exploited (as by cybercriminals) before it is known to or addressed by the maker or vendor.
[17] McAfee "What is Stuxnet?".
[18] Zetter 2014, p. 6.
[19] McAfee: "What is Stuxnet?".

conventional military operations. Stuxnet was capable of causing physical damage to nuclear centrifuges by overheating them. The Stuxnet attack demonstrates why the juxtaposition of cyberattacks and conventional attacks may be reasonable: regardless of the means and circumstances being different, the consequences may be as severe despite the attack taking place through cyberspace.

The third example of significant cyberattacks is a malware attack targeting Colonial Pipeline, a fuel pipeline company in charge of oil distribution across the South-Eastern part of the United States. This cyberattack was conducted in 2021 using compromised user credentials, which enabled the attackers to access Colonial Pipeline's network. The attackers stole 100 gigabytes worth of data from the network and threatened to publish it if a ransom of $4.4 million was not paid.[20] Since Colonial Pipeline had to temporarily close all its pipelines in fears of critical operations being compromised,[21] supply chains endured a corollary effect of the attack.[22] Terminology of conventional attacks may not analogically apply to the Colonial Pipeline cyber operation, regardless of it causing severe consequences. The operation did not cause physical effects to humans or destruction to objects but it severely impacted critical infrastructure. Evaluating the Colonial Pipeline cyber operation in the context of international law emphasizes an important aspect of pursuing to categorize operations in cyberspace with pre-existing doctrines. If the legal status of cyber operations relies on analogical extension of existing concepts, at what point should cyberspace be considered an individual legal realm that requires tailored means for governance?

The three examples above demonstrate the broad spectrum of cyber operations and how terminology used to construe conventional attacks may be analogically extended to cover operations in cyberspace. Adapting the term cyberattack already juxtaposes operations in cyberspace to those taking place on conventional domains. Like proposed by the Tallinn Manual, categorizing certain cyber operations as cyberattacks unites them with the conventional attacks under the law of armed conflict. Regardless of the means and methods being different, having conventional military operations as a baseline for comparison may help defining cyber-related threats and establishing controlling measures. Separating operations in cyberspace from those taking place on land, sea, or air may not be purposeful, since the domains are already deeply intertwined. Hybrid warfare offers an example of why it can prove difficult

[20] Turton – Mehrotra 4.6.2021.
[21] Reeder – Hall 2021, p. 16.
[22] The corollary effects included temporary shortage of oil and price spikes, see e.g., Tsvetanov – Slaria 2021.

to evaluate cyberspace as a separate domain from conventional warfare. The conflict between Ukraine and Russia that has been ongoing since 2014 can be described as hybrid warfare based on the variety of measures utilized. Strategic objectives may be achieved by conducting operations in various domains, such as military operations, economic sanctions, cyberattacks and information manipulation.[23] Drawing the line between cyber and non-cyber operations seems impossible as more and more cyber assets are utilized in conventional operations as well.[24] Evaluating cyberspace as a separate phenomenon seems to be counterproductive to the objective of defining its legal status and general implications to society. The emergence of cyberspace entails considering a more diverse group of measures, techniques, actors, and incentives as factors behind security-threatening operations.[25] Applying pre-existing legal concepts and terminology may contribute to how the new threat landscape is analysed, but the disrupting nature of cyberspace sets limitations to how widely old concepts cover new threats.

1.1.4 Trade policy as a security measure

Like explored in the previous section, cyber operations may pose a threat for security. Security threats can be managed with various governance models executed from different levels of society, ranging from local to global.[26] Models for managing global security threats include both measures for prevention and for retribution. Global security governance may be managed through multilateral security regimes, such as security communities like North Atlantic Treaty Organization (NATO) or security agreements like the Treaty on the Non-Proliferation of Nuclear Weapons, 5 March 1970 (NPT or Non-Proliferation Treaty).[27] Prohibiting security-threatening activities is a possible control measure when security threats originate in distinct activities, like cyber operations. In the case of cyber operations, security governance through prohibition is executed with trade and criminal legislation on the international level. In this paper, trade policy is evaluated as a security measure for preventing security threats created by cyber operations. Regardless of the virtual nature of cyberspace, the resources used for cyber operations can be produced and traded similar to other sensitive goods, like conventional weapons or harmful chemicals.[28] Using trade policy as a security measure entails prohibiting

[23] See e.g., Limnéll 2015.
[24] Ibid.
[25] Nye Jr. 2016, p. 50.
[26] Valverde 2008, p. 5.
[27] See e.g., Krahmann 2003.
[28] Resources used in cyber operations may include viruses, rootkits, botnets, and worms, which can be traded online. See e.g., Andress – Winterfeld 2013, p. 22.

the production or trade of potentially harmful goods as a preventative measure of security governance.

The items used in cyberspace for different cyber operations can be described as cyber goods. For the purpose of this thesis, cyber goods are defined as offensive or defensive items used in cyberspace capable of operating or contributing to a cyber operation.[29] As tradeable objects, cyber goods can be compared to nuclear technologies. In the wrong hands, nuclear technology can be used to create nuclear weapons which cause vast damage. Thus, cyber goods and nuclear technology may both be categorized as dual-use goods. This relation will be evaluated in more detail later in this paper. Trade policies can be useful tools against security-threatening conflicts or operations. If items used for malicious operations are not available, the operation cannot be carried out, or at least it must be conducted by alternative means. This applies to operations on any of the conventional domains, as well as in cyberspace.

Security governance can be evaluated with a legal realist approach, since security policy is tightly knitted with (geo-)political, historical, and societal factors.[30] The choices made on national and international levels regarding security interests reflect a broader perception on the governed issues. With the still changing legal status of cyberspace, the policy choices made regarding cyber goods may affect the perception of cyberspace as a domain. The implications of trade policy impact various stakeholders, including non-governmental organisations, private companies, and individuals. In this paper, trade policy is examined critically as one possible model of security governance.

1.2 Setting the research questions

This thesis explores how dual-use trade restrictions apply to goods in cyberspace in the general context of international trade law. As the society has developed and become more reliant on cyberspace, new possible scenarios threatening international security have emerged. The purpose of the thesis is to assess the nature of cyberspace in order to evaluate whether trade policy is a suitable approach to governing dual-use cyber goods. This paper compares cyberspace to conventional domains in order to distinguish similarities and differences in the threat scenarios and potentially harmful goods within those domains. The objective of this paper includes systematizing the legal basis for restricting the trade of certain goods based on security

[29] Offensive cyber goods include e.g., cyber surveillance technology as defined in European Council Regulation 428/2009 article 4.
[30] See e.g., Krahmann 2003.

interests. The applicability of the non-proliferation focused regime to cyber goods is examined based on the comparison of conventional and cyber domains and the evaluation of the general legal basis of trade restrictions. The basis for trade restrictions set in the General Agreement on Tariffs and Trade, 30 October 1947 (GATT) is observed in the context of both nuclear and cyber goods. Additionally, the Wassenaar Arrangement, 1996 (WA) is evaluated as a framework applicable to dual-use cyber goods. Threats relating to cyberspace are a new concern in international relations, so a critical approach is applied in this paper while evaluating options for legal governance. As a combining factor, both nuclear and cyber goods have a close link to national security, importance of which is evaluated in the framework of international law. The specific focus within this framework is to answer the following research questions:

1. Does international law include a legal basis for using trade policy as a security measure for governing threats in cyberspace?

2. Is trade policy a suitable model for governing threats in the cyberspace?

The first research question covers analysis of how security interests are regarded in international trade law. The second research question covers evaluating the current non-proliferation focused trade policy and comparing the nature of nuclear and cyber goods as objects for trade.

1.3 Methodology

To answer the paper's research questions, relevant legal instruments in the field of international law are evaluated by using the legal dogmatic method with the *de lege lata* approach. The legal dogmatic method is used to evaluate and interpret the existing legal frameworks regarding international trade restrictions.[31] For evaluating the general basis for trade restrictions, the General Agreement on Tariffs and Trade is examined as an applicable instrument. For a more detailed evaluation on the governance of dual-use goods, the research focuses on the Wassenaar Arrangement. With the *de lege lata* approach, the research focuses on the current form of the legislation rather than what it should be.[32] The legal dogmatic method is used to achieve a comprehensive perception of what the legal basis for imposing trade restrictions is and how dual-use goods are currently governed in international trade law.

[31] Aarnio 2011, p. 104-105, 109.
[32] Fellmeth – Horwitz, 2021, p. 77.

The constructivist method is applied to observe the legal concepts of security interest and dual-use goods as part of public policy.[33] To provide a critical outlook on the current trade policies, historical and political influences are considered. The comparison between nuclear and cyber goods focuses on determining, what similarities and differences the goods have. The constructivist method is chosen to question, whether the nature of cyber goods prevents the analogical application of pre-existing legal regime. International law's core concepts, such as sovereignty and territoriality, are explored to describe the legal implications of operating in cyberspace. The constructivist method is also applied to interpret the Tallinn Manual 2.0 as a source of law in cyberspace.[34] The Tallinn Manual 2.0 is referred to when defining concepts such as cyberspace, cyberattacks and cyber weapons. It is used as a source for scholar and expert views on cyberspace and topics related to it. The constructivist approach is applied for evaluating the effectiveness and collateral consequences of governing dual-use cyber goods with trade policy. Interests beyond legislation are taken into account to provide a comprehensive description of the societal context surrounding the trade of cyber goods. By combining the legal dogmatic and constructivist methods, the objective is to analyse and interpret law in the books and based on the analysis, assess how it reflects the underlying values and policy choices. Observing the influences that have historically guided how international security is grasped aims to contribute to a more comprehensive view of why legal governance of dual-use goods is managed with the current approach and additionally, why the same approach is applied to cyber goods.

The second research question on whether the chosen legal framework is suitable for governing threats in cyberspace is based on the theory of legal realism. The legal regime on trade restrictions is viewed as one part of public policy that is not separate from the development and changes of the surrounding society.[35] The doctrinal analysis conducted while evaluating the first research question is used as a foundation for answering the second research question. The nature of cyber goods and the cyber goods industry are examined with a socio-legal approach by observing the societal context of applying trade restrictions to cyber goods.[36] The analogical extension of the scope of trade restrictions on dual-use goods is assessed with a critical approach to present internal critique.

---

[33] Paulson 1996, section I.
[34] Note that the Tallinn Manual 2.0 is not free of political influences. As a source, it reflects a certain political stand in society. For that reason, it is evaluated with a constructivist approach.
[35] See e.g., Shaffer 2015.
[36] See e.g., Cotterrell 1998.

1.4 Structure

In the introduction, cyber operations are described as a modern addition to international conflict and security threats. Cyberspace is described as a fifth domain, in addition to the "conventional domains" of land, sea, air and space. Trade policy is introduced as a security measure, especially for governing dual-use goods. The substance of the thesis begins in the second chapter, where national security is described as a concept in the framework of the customary principles of sovereignty and territoriality. The constructivist method is applied to examine how the existing legal concepts apply to cyberspace. The remarks made regarding the concepts of security, sovereignty and territoriality form a foundation for evaluating the legal status of cyber goods in the context of international trade law. Section 2.1 explores how these core concepts adapt to cyberspace and in what ways cyberattacks may constitute a threat for international safety. Section 2.2 introduces the General Agreement on Tariffs and Trade and the legal basis it forms for liberal international trade. The legal dogmatic method and its *de lege lata* approach is applied to analyse and interpret the GATT. Section 2.3 introduces how the GATT enables taking security interests into account in trade policy with the national security exception. The purpose of analysing the GATT and its security exception clause is to depict on a general level how security interests are regarded in trade policy.

The third chapter elaborates on how the GATT's national security exception is applied in dual-use regimes based on the analysis conducted in the previous chapter. Section 3.1 discusses the origin and context of the governance of dual-use goods, whereas section 3.2 continues by comparing the characteristics of nuclear and cyber goods. The comparison between nuclear and cyber goods focuses on two aspects: the nature of the industry and the nature of the goods. These aspects are chosen for the comparison to comprehensively distinguish differences that may affect what model of legal governance is suitable for cyber goods. The socio-legal approach is applied to observe the societal context surrounding nuclear and cyber dual-use goods. The third chapter focuses on distinguishing the influences behind the dual-use regime and on evaluating whether the characteristics of cyberspace and cyber goods correspond to the nature of dual-use regimes. The findings of the third chapter provide reference points for analysing the legal framework's potential shortcomings in the following chapter.

The fourth chapter discusses the Wassenaar Arrangement and its provisions applicable to certain cyber goods. Section 4.1 sets the general picture of how the Wassenaar Arrangement governs dual-use goods. The concept "destabilizing accumulations of dual-use goods and

technologies" is introduced as a core concept of the Wassenaar Arrangement. The Wassenaar Arrangement is evaluated with the legal dogmatic method's *de lege lata* approach to analyse and interpret the legal framework. Especially the concept of destabilizing accumulations and its applicability to cyber goods is assessed critically. Section 4.2 focuses on the intrusion software addition that brought certain cyber goods under the scope of the Wassenaar Arrangement. Findings of the doctrinal analysis are evaluated with the socio-legal approach to observe the societal context as one factor that affects the legal framework's applicability to cyber goods. The controversy and critical feedback given by the software industry related to the intrusion software addition is taken into account as an important stakeholder view. The two aspects used to compare nuclear and cyber goods in the third section are repeated to construe, why the inclusion of cyber goods to the trade policy framework has not been successful. Generally, the objective of the fourth chapter is to cover how trade restrictions apply to certain cyber goods in practice and to reflect the issues brought up in the third chapter.

The fifth and final chapter draws together the conclusions reached while conducting this research and answers the research questions presented at the beginning of this paper.

2 National security in trade policy

2.1 National security

2.1.1 Sovereignty

In this section, the concepts of sovereignty and territoriality are discussed in the context of cyberspace to lay a basis for exploring how the domain's nature affects its legal status. As a fundamental principle of international law, all states enjoy sovereignty over their territory. Sovereignty is tied to the state's independence, which entitles exclusion of any other state's influence.[37] Initially, cyberspace was considered outside the realm of any state's sovereignty, because cyber activities are not necessarily tied to any physical location.[38] Cyberspace can be comprehended as a global common, similar to the high seas or outer space which are governed as a *res communis*.[39] According to some views, cyberspace should not be regulated by states but rather form an independent legal system based on decentralized self-regulation.[40] Regardless, currently the prevailing understanding is that the principle of sovereignty applies to cyberspace in various ways. Territorial aspects may be recognized in cyberspace, since a state may exercise its jurisdiction over cyber infrastructure located in the state's territory or if individuals participate in activities in cyberspace while physically located in the state's territory.[41] When states enact legislation to govern cyberspace, they are exercising the territory-based jurisdiction over cyberspace.[42]

The territorial aspect is not the only link between sovereignty and cyberspace. Sovereignty entails, that other states are prohibited from using force against the sovereign state[43] and from intervening in the internal or external affairs of the sovereign state.[44] Like stated in the article 2.4 of the Charter of the United Nations (UN) 24.10.1945, the prohibition of use of force entails states refraining from the threat or use of force against another state's territorial integrity or political independence. The prohibition of intervention entails exclusion of non-domestic influences in matters that are essentially within the domestic jurisdiction. The prohibition-dimension of sovereignty helps determining, how the principle of sovereignty is relevant to cyber operations. By targeting a cyber operation to a computer system which is used in political

[37] In the context of cyberspace, see the Tallin Manual 2.0, rule 1.
[38] See footnote 1, the physical layer is one aspect of cyberspace.
[39] Tallinn Manual 2.0, rule 1.
[40] See e.g., Barlow 2019.
[41] Tallinn Manual 2.0, rules 1 and 4.
[42] Kohl 2015, p. 38.
[43] Tallinn Manual 2.0, rule 68.
[44] Tallinn Manual 2.0, rule 66.

elections may affect the political independence and internal matters of states. Similarly, cyber espionage or information manipulation can also interfere with the internal or external affairs of the targeted state. Operations in cyberspace can cause consequences that reach the threshold set for violation of sovereignty. Thus, cyberspace cannot be separated from state sovereignty. A state may have jurisdiction over cyberspace based on territoriality, but the prohibition-dimension of the principle of sovereignty also applies in cyberspace.[45] As the global dependence on cyberspace continues to grow, the interest of protecting state sovereignty from violations originating in cyberspace cannot be disregarded.

Contiguously to cyber sovereignty, national security is a concept that often comes up when discussing cyberattacks. Even without the cyber prefix, the term security is broad and hard to comprehensively define. Generally, national security can be described as preservation of national norms, rules, institutions, and values.[46] These aspects seem to reflect the same underlying values as the principle of sovereignty. Each nation ought to have the sole responsibility of making decisions regarding their internal matters. Protecting national security entails protecting values that have been previously acquired.[47] Thus, an essential aspect of security is preserving the nation's prevailing *status quo*. A violation of national security in the aforementioned meaning would entail an external entity interfering with the nation's norms, rules, institutions, and values. In a digitalized society, the role of computer systems has developed from establishing infrastructure for critical institutions and services to inhering a more fundamental meaning in providing trust and connections within the community. In this context, a cyber operation targeted to a computer system, for example, supporting critical infrastructure, operating a ballot-counting system for a national election, or controlling national emergency supplies could cause a destabilizing effect on the nation. The well-established concepts of sovereignty and territoriality as well as the less defined concept of national security can all be seen as applicable to cyberspace. The distinguished intersections between the pre-existing concepts and cyberspace prove that that phenomena in cyberspace should not be explored separately from other systems. The next section elaborates on how past cyber operations have violated either state sovereignty or security.

[45] See e.g, Tsagourias 2015.
[46] Makinda 1998, p. 282. Makinda's definition is not necessarily limited to states as understood in international law, but the definition is applicable to this context.
[47] See e.g., Wolfers 1952.

2.1.2 Cyber operations violating state sovereignty and security

Like discussed in the previous sub-section, the principle of sovereignty entails that a sovereign state's internal affairs are free of any external interference. Similarly, the general concept of national security is based on an aspiration of preserving national values, norms, institutions, and rules. These concepts give context to evaluating why cyber operations pose a significant security threat. Cyber operations that cause information manipulation or political propaganda easily surpass the threshold for what can be seen as external interference. In recent years, many political elections have been under the effect of foreign influence either through disinformation or interference with voting.[48]

Similarly, the Estonia cyberattack in 2007 may be viewed as a cyberattack that violated state sovereignty. The effects of the cyberattack included state information channels and systems being out of operation for a considerable amount of time, hindering how the government could interact with the citizens and provide services normally. Cyberattacks that immobilize critical infrastructure may be categorized as acts of aggression or threats to the peace based on their potential of creating detrimental consequences.[49] Such cyberattacks are to be considered as international crimes.[50] The Colonial Pipeline attack could be categorized as a violation of state sovereignty regardless of it being targeted to a private company, since it affected critical infrastructure. The same conclusion applies to the Stuxnet attack, since it affected Iran's internal matters by at least temporarily hindering operations possibly related to their military capabilities.

The previous sub-section introduces the preservation of common norms, rules, institutions, and values as one definition of national security. The definition seems to be at least partly overlapping with sovereignty, since interference with a sovereign state's internal matters most likely entails disregarding the national identity and institutions related to it. Again, all the three examples of cyberattacks reach the threshold of the criteria. The Estonia attack targeted national institutions and temporarily deteriorated national values, such as the freedom of press. The Stuxnet attack was targeted to a national institution and arguably disregarded Iran's national values and norms. Finally, the Colonial Pipeline attack interfered with the operations of a critical institution, also hindering the state's ability to preserve its normal operations. These

[48] For more information on interference with the 2016 U.S. presidential election, see e.g., Inkster 2016.
[49] Tallinn Manual 2.0 rule 76. The Security Council has the authority to label cyber operations directed to critical infrastructure as a threat to the peace or act of aggression.
[50] Article 8 *bis* of the Rome Statute.

observations demonstrate why reacting to harmful cyber operations is of utmost importance. The effects of cyber operations range from practical nuisance, such as network unavailability, to essential political and legal matters, such as interference with state independence. After the importance of controlling security-threatening operations in cyberspace has been described, the next issue is evaluating how can cyberspace be controlled.

2.1.3 Security concerns in trade policy

Cyber goods are not the only tradeable objects that cause security concerns. In the globalized economy, the increased trade of sensitive goods with potential security-threatening capabilities requires attention.[51] Goods that have both military and civil uses are categorized as dual-use goods.[52] For example, certain chemicals, satellite technology, drones, biological tools, and positioning technology have legitimate use purposes in the hands of civilians. However, in a military context such items are capable of causing vast harm and damage. Since dual-use goods have legitimate purposes, prohibiting the production, trade or possession of the goods or technologies is not reasonable. One of the ways these risks are managed are trade policy regimes, that aim to target the harmful aspects without halting the legitimate trade. Trade restrictions are widely used as a measure to ensure international peace and security.[53] Dual-use regimes recognize that prohibiting the global trade of dual-use goods would unintentionally ban a lot of legitimate and necessary goods from being used. Thus, the legal issue represented in dual-use regimes is how the objectives of free global trade and controlling security threats are balanced.

As a comparison to cyber goods, nuclear goods and technologies have for long been controlled to avoid the risk of nuclear conflict. Legitimate uses for nuclear goods include the production of nuclear energy, water desalination, pest control, scientific research, among other matters.[54] However, the security risk of nuclear weapon production justifies setting strict restrictions to the trade of nuclear goods and technologies. The trade policy approach entails that legitimate trade of the controlled items continuous with potential monitoring or supervising measures, but illegitimate use is prevented with trade restrictions. Similarly, trade restrictions can be imposed to avoid security risks caused by the use and trade of certain cyber goods. Decreasing the availability of security-threatening goods aims to decrease the frequency and impact of security

[51] See e.g., Aubin – Idiart 2016, chapter 1.
[52] See e.g., definition in European Council Regulation 428/2009 chapter 1, article 2.
[53] See e.g., Aubin – Idiart 2016, chapter 1.
[54] For more examples, see e.g., World Nuclear Association, 5/2021.

threats.[55] Recognizing the similarity between the potential adverse consequences caused by certain cyber goods and those of other dual-use goods leads to the question of whether the matters can also be governed with a similar trade policy approach.

2.2 National security in free trade

2.2.1 Free trade approach in international trade

To establish basis for evaluating the use of trade policy as a control measure for security threats, this section briefly explores how security interests are viewed under international trade law. International trade law is largely based on the free trade doctrine, pursuing to be as frictionless as possible to enable innovation, competitive market conditions and steady access to various different goods.[56] Principally, free trade doctrine encourages a *laissez-faire*[57] policy model, meaning that keeping policy intervention at its minimum level provides for the best economic results.[58] The *laissez-faire* approach entails that the market reacts and forms according to supply and demand without the need of guidance by trade policy intervention. In practice, the free trade doctrine does not necessarily entail that policy intervention is explicitly off-limits.[59] However, the pursuing for liberal market conditions implies minimising any policy obstacles, like quality requirements or trade prohibitions. Since the *laissez-faire* approach is based on minimal policy intervention, it generally entails steering away from governing trade with regulatory controls. However, as economic and political uncertainty in the 1930s prompted the U.S. and the European Community, waves of protectionist policies followed the golden era of the free trade doctrine to ensure that free trade does not hamper national interests.[60]

Especially during political conflicts or wars, free trade policies may suffer as national security is prioritized as an interest.[61] Trade restrictions may be established either to prevent others from getting access to certain strategic goods or to maintain national surplus on those goods to ensure security. As the society has developed and international security is not defined merely by the lack of war, trade restrictions have gotten a new meaning. In the post-9/11 era, the nature of national security has evolved as critical industries are protected from foreign threats. Modern

[55] See e.g., foreword on European Council Regulation 2021/821.
[56] Shaikh 2006, p. 53.
[57] Literal meaning in French "allow to do", originated as an economic term in the 1800s by French economists. Defined in the Merriam-Webster Dictionary.
[58] Chang 2003, p. 24.
[59] The absoluteness of the free trade doctrine was critiqued already in the beginning of the 20th century, see e.g., Ashley 1924, p. 501.
[60] See e.g. Nayyar 2006, p. 74-75 on the Great Depression and Second World War as catalysts for protectionist policies.
[61] See e.g., Zeiler 1998.

protectionist policies go beyond tariffs or quantitative restrictions by controlling foreign investments and offshore outsourcing to maintain strategic value nationally.[62] Nowadays, the choice is not between liberal or protectionist trade policies, but how each aspect is achieved simultaneously. The need to balance conflicting interests is inherited to complex trade issues, like the governance of dual-use goods. The analysis on international policy supports the constructivist evaluation of security interests as a legal concept. These findings set the grounds for the following section which elaborates on how the General Agreement on Tariffs and Trade addresses security interests in trade policy.

2.2.2 Free trade approach applied in GATT

As central as international co-operation is for international trade law, exceptions to liberal trade rules are an essential part of the legal regimes. The General Agreement on Tariffs and Trade was created in the 1940s, right after the Great Depression and the Second World War. The GATT was established on the idea of mutually advantageous arrangements among member states to reduce tariffs and other obstacles of trade and to eliminate discrimination from international trade relations.[63] Even though the GATT is based on non-discrimination between states and it channels ideas of the free trade doctrine, the societal circumstances of the time required steering away from totally universal free trade.[64] After the Second World War, many states were at different baselines for re-starting economic growth, since resources were required to repair what the war had demolished. Thus, to protect national economies the GATT included tariffs, which were to be reduced as economic stability increased. Offering flexibility for implementing some protectionist measures to guard national interests ensured that trade liberalization continued, nevertheless.

Along with the free-trade-focused primary rules, the GATT includes exception clauses, which enable deviating from the primary rule based on an important legitimate interest. The exception clauses cover, for example, national interests that relate to moral reasons or common good. The possibility to deviate from the primary rule based on the established exceptions can be seen as a safety measure for avoiding non-compliance or termination of the regime in a situation where a state participating in the regime faces a conflict of national interest and a primary rule of the international regime.[65] The intention to remove obstacles of trade and to promote free

[62] See more on the modern global protectionism, Enderwick 2011.
[63] GATT 1994, foreword.
[64] Nayyar 2006, p. 75.
[65] Henckels 2020, p. 558.

movement of goods reflects the ideology of trade liberalization, whereas the option of diverging from the default regime based on a national interest reflects a protectionist ideology. Thus, aspects from both free trade doctrine and protectionism have been considered in the making of the current legal regime.

The flexible approach to global trade adapted in the GATT enables setting specific rules for special cases such as dual-use goods. The objective of maximizing freedom in global trade fits poorly to goods that have potentially harmful purposes, which is why the exceptions in GATT are needed to set carefully targeted restrictions. Dual-use goods, such as certain chemical or biological technologies, nuclear technology, and cyber goods, demand a more complex approach than applying either fully unrestrained free trade or a blatant protectionist approach. Since various potentially harmful goods and technologies can be used also for legitimate purposes, prohibiting all trade is not fitting. The modern global trade system requires that free trade and trade restrictions are implemented contiguously. The exceptions included in GATT enable exactly that: maintaining liberal trade relations internationally, while still allowing specified regimes for dual-use goods.

2.2.3 The non-discrimination principle

The concept of trade liberalization and minimal policy intervention with international trade is built into the GATT's non-discrimination principle. The principle of non-discrimination is composed of two inter-linked principles: the principles of most-favoured-nation treatment and national treatment.[66] Together these principles pursue a levelled trading environment where all states can accomplish reciprocal and mutually beneficial trading arrangements without facing discriminatory treatment from the opposite party.[67] Reduced tariff rates and other restrictions allegedly promote international commerce which ought to benefit all parties.[68] The paragraph 1 of the article I of the GATT lays down the principle of most-favoured-nation treatment with the following phrasing:

> *With respect to customs duties and charges of any kind imposed on or in connection with importation or exportation or imposed on the international transfer of payments for imports or exports, and with respect to the method of levying such duties and charges, and with respect to all rules and formalities in connection with importation and exportation, and with respect to all matters referred to in paragraphs 2 and 4 of Article III, any advantage, favour, privilege or immunity granted by any contracting party to any product originating in or destined for any*

[66] GATT 1994 part I, article I.
[67] Ibid.
[68] Ibid.

> *other country shall be accorded immediately and unconditionally to the like product originating in or destined for the territories of all other contracting parties.*

Respectively, the paragraph 1 of the article III establishing the principle of National Treatment reads the following:

> *The contracting parties recognize that internal taxes and other internal charges, and laws, regulations and requirements affecting the internal sale, offering for sale, purchase, transportation, distribution or use of products, and internal quantitative regulations requiring the mixture, processing or use of products in specified amounts or proportions, should not be applied to imported or domestic products so as to afford protection to domestic production.*

Together, these principles form the principle of non-discrimination that constitutes the basis for the trade-liberalizing framework of GATT. To compliment the aforementioned principles, the paragraph 1 of article XI of the GATT governs quantitative restrictions:

> *No prohibitions or restrictions other than duties, taxes or other charges, whether made effective through quotas, import or export licences or other measures, shall be instituted or maintained by any contracting party on the importation of any product of the territory of any other contracting party or on the exportation or sale for export of any product destined for the territory of any other contracting party.*

These principles oppose favouring domestic products at the loss of imported ones by setting various controls over national measures that could potentially distort international trade. If the non-discriminatory approach were to be applied without exceptions, dual-use goods, such as nuclear technology or cyber goods, would have to be traded just as any other goods. Setting export license requirements, quantitative restrictions, or technical barriers to trade[69] based on the nature of dual-use goods could be seen as discriminatory measures regardless of the potential security implications. However, as much as the GATT promotes free trade with the non-discriminatory principle, it also sets exceptions and reservations to the main principle. The exceptions form a legal basis for setting specified regimes to govern dual-use goods. The following sub-section elaborates on how non-discriminatory principle is partially waived to enable accounting for vital interests that conflict with free trade.

[69] World Trade Organization's (WTO) Agreement on Technical Barriers to Trade 1995. The agreement's objective is to ensure that technical regulations, standards, and assessment procedures are non-discriminatory.

2.3 National security interests as exceptions to the free trade approach

2.3.1 Clause XXI

The GATT's roots in the era after the Second World War may explain why national security interests are regarded so strongly in the framework. National security interests are balanced with the objective of free trade by reserving exceptions from the agreement's provisions for protecting national security interests. Initially, the security aspect was included in the general exceptions clause.[70] However, in the current Agreement text national security is covered separately in clause XXI.[71] The clause XXI establishes basis for enacting trade restrictions based on national security interests with the following phrasing:

> *Nothing in this Agreement shall be construed*
>
> *(a) to require any contracting party to furnish any information the disclosure of which it considers contrary to its essential security interests; or*
>
> *(b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests*
>
> > *(i) relating to fissionable materials or the materials from which they are derived;*
> >
> > *(ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment;*
> >
> > *(iii) taken in time of war or other emergency in international relations;*
>
> *Or (c) to prevent any contracting party from taking any action in pursuance to its obligations under the United Nations Charter for the maintenance of international peace and security*

In practice, the article XXI ensures that parties of the GATT are not prohibited from taking action to protect their security interests. Allowing members to secure 'essential security interests', sections (a) and (b) cover different sides of the coin. Section (a) allows *opting out* of actions that would infringe the member's essential security interests, whereas section (b) allows the member *engaging* in action that is required for protecting an essential security interest, regardless of the action otherwise infringing GATT. Section (c) prevents any conflict between GATT and the UN Charter, giving priority to the latter. Based on section (b) allowing active measures, the clause provides an essential premise for establishing trade policy measures to

[70] GATT 1947 (pre-WTO).
[71] The separate security clause was added based on a proposal made by the U.S. Department of State. See U.S. Department of State 1945.

protect national security interests. For the governance of dual-use goods, applying the article XXI(b) entails that action taken to control the trade of dual-use goods is not prohibited by the GATT, given that the action is necessary for the protection of an essential security interest.

2.3.2 Applying clause XXI(b) to dual-use goods

The article XXI(b) permits a member of the GATT engaging in activities that it considers necessary for protecting essential security interests, regardless of other clauses in GATT. The section offers leeway for undertaking trade policy measures to control a national security threat. The phrasing of the exception clause includes two vague concepts: "any action which it considers necessary" and "essential security interest". These aspects may be interpreted in varying ways, enabling a broad variety of measures and threat scenarios to fall under the scope of the exception.[72] Controlling the trade of dual-use goods, such as nuclear and cyber goods, can easily be seen as an essential security interest due to the harm-potential related to the goods.

The clause XXI(b)(i) relates to fissionable materials and has been written to control the threat of nuclear proliferation. The clause allows establishing regional and international agreements to control the trade of nuclear technologies with a non-proliferation approach. The wording of the clause covers fissionable materials or the materials from which they are derived from, enabling a minimalist or a maximalist approach. Trade controlling regimes may either be targeted to nuclear arms or merely nuclear fission technology, that may enable producing nuclear arms. Again, the clause leaves much room for establishing arguably broad trade restrictions to nuclear technologies, since the security threat attached to nuclear weapons is so crucial.

The clause XXI(b)(ii) relates to a much broader set of items and technologies. It covers "military goods", entailing that trade controls on goods that may be used for military purposes are allowed. The article has been invoked to justify imposing export bans of a group of goods to a certain country[73] based on a national security concern. Consequently, the national security clause may also be invoked for enacting import bans on goods relevant to military purposes to protect vital industries.[74] The scope of the point (b)(ii) is much broader and more vague than

[72] See e.g., WTO 2019 "Traffic in Transit", regarding trade restrictions Russia imposed to Ukraine between 2014 and 2018. The trade restrictions were invoked based on the XX(b)(iii), circumstances to which Russia considered to be self-judging.
[73] See e.g., GATT 1949, "Article XXI – United States Export Restrictions", where the U.S. invoked the security clause to impose export bans on certain "military goods" 1949.
[74] See e.g., GATT 1975. The report discusses import restrictions imposed by Sweden on certain footwear based on the security clause to protect national production for emergency planning and security policy reasons.

previous point concerning fissionable materials, since military goods potentially include any goods that by nature may contribute to a potential military conflict.[75] Like mentioned in the definition of dual-use goods, one criterion for distinguishing dual-use goods is that the items or technologies may be used for a military purpose. Thereby, the clause XXI(b)(ii) is applicable to almost any dual-use goods, as long as the items can be used directly or indirectly for the purpose of supplying a military establishment and their use has security implications. Cyber goods also fall under the scope of this clause since cyber operations are an intrinsic part of modern military operations. Imposing trade restrictions targeted to cyber goods may be deemed justified based on the article XXI(b)(ii), if the cyber goods are used in a military context and the trade restrictions are imposed to protect an essential national security interest. Regardless, the section (b)(ii) does not seem to create as steady of a foundation for trade restrictions imposed to cyber goods as the point (b)(i) does for nuclear goods.

The first two sections of the article XXI(b) cover *categories of goods* in relation to which the actions are taken. The third point (iii) has a different approach: it allows trade-restricting security actions *based on the circumstances*. Point (iii) establishes a base for trade restrictions that are imposed in the name of an essential security interest during a time of war or other emergency in international relations. A national emergency creates an exception to obligations deriving from GATT, thus allowing actions that would otherwise infringe GATT obligations. The clause leaves the determination of war or other emergency in international relations up to the state's self-judgment.[76] However, the inclusion of non-war emergencies in international relations caters to obscure security threats like cyber conflict. Regardless of cyber operations not qualifying as armed aggression, they can be recognized as emergencies in international relations. The security exception of the article XXI(b)(iii) could be invoked, for example, if the means of information warfare would be utilized in an international conflict, creating a security threat. Trade restrictions imposed on certain cyber goods based on the article XXI(b)(iii) could help control the additional security threat caused by information manipulation or propaganda. Arguably, this interpretation is more applicable if the emergency in international relations lasts for a prolonged period of time, since reacting with trade policy does not necessarily yield immediate results.

Regardless of the GATT's fundamental purpose of promoting free trade, it includes a steady base for protecting national security in situations where the two interests collide. Security

[75] GATT 1949, Summary record of the Twenty-Second Meeting.
[76] See e.g., WTO 2019, "Traffic in Transit".

mechanisms, such as the clause XXI, allow including national security interests into the free trade system. The security exceptions in GATT entail that dual-use goods may be controlled with specified trade restrictions despite the general objective of maintaining a liberal approach to global trade. In a nutshell, invoking the security exception of GATT article XXI(b) allows for imposing trade restrictions on dual-use goods, if free trade of the goods contributes to a national security threat. A basis for imposing trade restrictions on nuclear goods can be easily found from the section (b)(iii), whereas control measures targeted to cyber goods may be enacted based on the exceptions in sections (b)(ii) and (b)(iii). While nuclear and cyber goods differ from each other vastly when evaluated as objects for trade, the GATT article XXI(b) creates a basis for controlling both nuclear and cyber goods with trade restrictions due to the possible security implications of the goods.

The GATT's broad scope enables perceiving cyber and nuclear dual-use goods as similar concepts. It seems like the GATT does not actively pursue to make the choice of including cyber goods under the same legal regime as conventional dual-use goods, since the clause does not exclusively mention cyber-related threats. Rather, the initially broad spectrum of security threats bound to fall under the scope of the security exception enables applying the exception also to cyber goods. Regardless, the security exception in GATT applies to cyber-related threat scenarios, thus creating a basis for trade restrictions on cyber goods. The security exception clause creates a foundation for applying similar trade policy measures to both nuclear and cyber goods based on their potential security implications. Different trade restricting regimes that are based on the national security exception are explored in the next section.

3 Non-proliferation of dual-use goods

3.1 Dual-use regimes

3.1.1 Governing dual use-goods based on the national security exception

As discussed in the previous section, the liberal approach in international trade law does not prevent addressing legitimate interests, such as security threats. The *laissez-faire* approach to international trade is not explicit since security-conscious trade policy is allowed to interfere with free global trade due to the crucial significance security has for states. International trade agreements, like the GATT, leave room for participating states to enact measures needed for promoting national security. Thus, dual-use goods can be controlled with various trade restrictions because of the potential security threats the nature of dual-use goods entail. Without the security exceptions, security-related trade restrictions could be considered as discriminatory measures and thereby be prohibited by international trade law.

The logic of controlling security threats with trade policy measures is based on the assumption that *less risky goods in circulation* results in *less national security threats*. This idea is put into effect by applying a non-proliferation approach to how dual-use goods are governed. Non-proliferation entails decreasing the amount of certain goods in circulation by requiring export licenses or limiting production. As the term dual-use goods partly overlaps with weapons, non-proliferation is also intertwined with the objective of disarmament. Thereby, the ultimate goal of non-proliferation regimes is to abolish all accumulations of certain destructive weapons to limit the damage potential of future conflicts.[77] For example, the article VI of the Nuclear Non-Proliferation Treaty entails all states participating in negotiations to end the nuclear arms race and to ultimately implement nuclear disarmament.

Aiming to completely diminish the trade of certain goods channels a maximalist take on non-proliferation, since the idea of non-proliferation may be implemented with less disruptive measures. Besides complete disarmament, arms control is another measure for avoiding highly destructive conflicts. Arms control regimes typically include limitations on the type or quantity of determined arms, procedures for crisis management and information sharing protocols.[78] The objective of enacting arms control measures is maintaining an understanding of the weapon accumulations to determine the threat landscape and to support establishing targeted measures.

[77] Egeland 2022, p. 109-111.
[78] See e.g., the Arms Control Association, 2/2022.

In this section, the background and purpose of non-proliferation policies is explored to evaluate how they apply to dual-use cyber goods.

3.1.2 Roots and target of non-proliferation

The Cold War era provides an example of using trade policy as a measure to control national security threats. After the Second World War, fears of nuclear arms race increased as the rapid progress in nuclear technology enabled states to increase their nuclear capabilities.[79] To stabilize the volatile state of international relations, the International Atomic Energy Agency (IAEA) was established for creating common rules on how nuclear weapons may be acquired.[80] To prevent states from engaging in an arms race, the non-proliferation approach was endorsed as a trade policy for nuclear weapons. Treaty on the Non-Proliferation of Nuclear Weapons followed IAEA's initiative of controlling the trade of nuclear weapons. Nuclear non-proliferation regimes are one essential application of the non-proliferation approach. However, as reflected in the broad scope of the GATT article XXI(b), national security threats originate in a wide spectrum of causes. Nuclear non-proliferation regimes are permitted by the article's section (i), which establishes a national security exception for enacting trade policies to control fissionable materials. Arguably, the governance of nuclear goods has paved the way for non-proliferation trade policies targeted to other dual-use goods that fall under the "military goods" category in the section (ii) of the GATT article XXI.

The bottom line of non-proliferation and arms control policies is to avoid arms race and to strictly limit the trade of the weapons. The less available harmful goods are, the less harm they are allegedly bound to do. Describing non-proliferation regimes often involves the terms "weapon" and "destructive". In the context of nuclear weapons, the strict limitations of trade are justifiable and logical because using nuclear weapons is inevitably destructive. However, the underlying logic of the non-proliferation approach needs to be re-evaluated as prominent national security threats have partly moved from land, air, and sea to cyberspace. To evaluate the applicability of non-proliferation regimes to cyberspace, the connection between non-proliferation and weapons of mass destruction ought to be discussed first.

[79] The idea of complete disarmament proposed in the Russell-Einstein Manifesto issued in 1955, cited in Russell 2012.
[80] IAEA 1956, article II.

3.1.3 Are cyber goods weapons of mass destruction?

Goods initially categorized as dual-use goods covered mainly components and technologies related to the production of nuclear, chemical, radiological, and biological weapons. These items are often also categorized as weapons of mass destruction (WMD) since they can cause catastrophic consequences for the mankind. The following definition of WMDs is included in U.S. Code Title 18, Section 2332a:

> *Any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors; any weapon involving a biological agent, toxin, or vector; any weapon that is designed to release radiation or radioactivity at a level dangerous to human life*

The definition focuses on weapons that are capable of causing potentially fatal consequences to humans. The definition of WMDs is partially overlapping with what was initially comprehended as dual-use goods, since dual-use trade restrictions mainly targeted destructive weapons and technologies that were used for military purposes.[81] Non-proliferation policies applicable to WMDs have initially aimed for the renunciation of the most harmful weapons. Non-proliferation treaties governing WMDs include the Treaty on the Non-Proliferation of Nuclear Weapons, the Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, 10 April 1972 (the Biological Weapons Convention), and the Convention on the Prohibition of the Development, Production, Stockpiling, and use of Chemical Weapons and on their Destruction, 13 January 1993 (the Chemical Weapons Convention). The non-proliferation approach is justifiable for effectively controlling the high security risk caused by WMDs. However, the non-proliferation approach has been analogically applied to other dual-use goods that may not qualify as WMDs. To critically examine the analogical application of the non-proliferation approach, the definition of cyber goods needs to be compared with the definition of WMDs.

As the international threat landscape has progressed from conventional military threats, such as nuclear weapons, to threats in cyberspace, a demand for effective control measures for new threats has emerged. Similar to WMDs, cyber goods can be used for military purposes to create vast damage to the society, civilians included. Yet, a clear answer as to whether cyber goods

[81] See e.g., European Council 2.3.2018.

can be considered as *destructive weapons* is hard to determine. The Tallinn Manual 2.0 defines cyber weapons in the following way:

> *For the purposes of [the Tallinn Manual], cyber weapons are cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack. The term 'means of cyber warfare' encompasses both cyber weapons and cyber weapon systems. A weapon is generally understood as that aspect of the system used to cause damage or destruction to objects or injury or death to persons. Cyber means of warfare therefore include any cyber device, materiel, instrument, mechanism, equipment, or software used, designed, or intended to be used to conduct a cyberattack.* [82]

The definition juxtaposes cyber weapons to conventional weapons in the extent of damage caused. Referring to the example made in the beginning of this paper, the Stuxnet attack resulted in nuclear centrifuges being physically damaged, which contributes to the interpretation that the Stuxnet virus was a cyber weapon, and the attack constituted an armed attack.[83] However, causing physical damage does not yet reach the threshold set for WMDs of causing destructive effects to human life.

Proposals for extending the term WMD have been set forth to support the analogical application of the non-proliferation approach to cyber goods. The terms electronic weapons of mass destruction (eWMD)[84] or weapons of mass destruction or effect (WMD/E)[85] regard the corollary effects of cyberattacks as destructive as the effects of conventional WMDs. Thereby, certain cyber goods could be assimilated to conventional WMDs if the corollary effect of a cyber operation would have a similar impact as what the direct effects of WMDs are. According to this interpretation, a cyberweapon would constitute a weapon of mass destruction if the direct impact of the cyberattack would be followed by a highly destructive effect that impacts human lives. For example, a cyberattack causing a nuclear reactor meltdown could reach the definition of a WMD, if the corollary effect would impact human beings in a destructive way. However, this interpretation of cyber goods being categorized as WMDs is currently not widely accepted.[86]

---

[82] Tallinn Manual 2.0, rule 103.
[83] Tallinn Manual 2.0, rule 82, paragraph 15.
[84] Barbieri – Darnis – Polito 2018, p. 20.
[85] The term WMD/E and its application for cyberweapons discussed in U.S. Joint Chiefs of Staff 2004, p. 1. The term WMD/E is not affiliated solely with cyberweapons, but it may apply to certain cyberweapons among other weapon categories.
[86] Mauroni 2016, p. 29.

The interpretation of even the most destructive cyberweapons being comparable to WMDs is still a minority view lacking strong academic or legal support. Furthermore, the scope of this paper concerns *cyber goods* instead of *cyber weapons*, since trade restrictions are imposed to a wide range of cyber goods that do not all qualify as weapons. Thus, even the most security-threatening cyber goods do not usually reach the threshold for being considered as WMDs, which is what the non-proliferation approach has been tailored for. As the prevalent non-proliferation approach to governing dual-use goods is analogically applied to cyber goods, it is important to emphasize that 1. non-proliferation trade policies have been tailored for governing WMDs, and 2. according to the current understanding, neither cyberweapons nor cyber goods at large reach the threshold for being categorized as WMDs. Without a doubt, cyberattacks create an increasingly crucial threat to national and international security, but analogical application of WMD-tailored non-proliferation policies may not be a justifiable solution.

3.2 Characteristics of nuclear and cyber goods

3.2.1 From WMDs to "military technologies": the extending scope of dual-use regimes

Initially the concept of dual-use goods was specifically catered towards items with a direct military application, such as biological, chemical, or nuclear technologies or components. Chemical and biological weapons were prohibited after the First World War by the Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare (1925, Geneva Protocol). Consequently, the substances and technologies used for the weapons have received the label of being dual-use goods to maintain control over the components used for producing harmful chemical and biological weapons. During the Cold War era, the international threat landscape was dominated by the fear of nuclear conflict. Thus, the trade controls over nuclear technologies have remained as a central measure to maintain a strict approach to the potential production of nuclear weapons.[87] Now in the 21st century, cyberattacks have stepped in as the new sphere of security threats. From WMDs to cyberweapons, trade policy has been considered as a peace-maintaining measure. The non-proliferation approach has been a solution for cutting the problem at its root in the prevention of conflict or security threats. As a basis for the restricting trade policy, the GATT article XXI(b) enables establishing trade restrictions to a wide variety of dual-use goods.

[87] See e.g., European Council 2017 on the non-proliferation of weapons of mass destruction and their means of delivery.

Based on the discussed remarks, the trade policy approach being *adaptable* to many different threat landscapes does not necessarily mean it is *suitable* for each of them.

The peace-maintaining trade regimes have adapted as the society has continued to develop, and little by little new possibly harmful items have been added under the realm of trade restrictions. Microchips, semi-conductors, and other computer hardware alongside with software are considered as dual-use goods due to their potential military applications besides the conventional civil uses. As cyberattacks have become a feasible threat to all states and private organizations alike, the dual-use nature of software has become clear. Cyberattacks may result in serious national security threats, just like nuclear attacks, yet the nature of the threat is very different. To accommodate the non-proliferation regime to new threat scenarios, the term "military technologies" has been presented.[88] Besides conventional weapons and WMDs, disrupting technologies have taken conflict to cyberspace.

The new terminology attached to the concept of non-proliferation reflects the move from land, sea, air, and space conflict to the fifth dimension, cyberspace. The mere fact that various types of software can be used for military purposes, thus qualifying as military technology, brings cyber goods under the umbrella of dual-use goods. Consequently, non-proliferation regimes are applied as a controlling measure to dual-use cyber goods. Even though cyberattacks can be seen as parallel from conventional attacks as violations of state sovereignty and national security, applying the non-proliferation approach analogically entails that the justification for the measures needs to be re-evaluated. Whereas WMDs cause destructing consequences to national security solely if they are used, cyber goods cause consequences to national security if they are used in a destructing manner. The differences of nuclear and cyber goods as objects of trade are explored covering two aspects: the nature of the industry and the nature of the goods.

3.2.2 The nature of the industry

Nuclear warfare is highly characterized by the threat's inter-state nature and division between nuclear and non-nuclear states. The threat of nuclear conflict is attached to those states, who maintain nuclear offence capabilities. In the NPT, this bilateral power dynamic is reflected in the categorization of states to non-nuclear-weapon states (NNWS) and nuclear-weapon states (NWS). The core of the non-proliferation principle is stated in the article I of the NPT by prohibiting NWS from transferring nuclear weapon technology to NNWS. NWS are also

[88] See e.g., Grimmett 2006.

prohibited from co-operating with NNWS to contribute to producing nuclear weapons. The monitoring and information sharing protocols of NPT enable determining, in which countries the security threat posed by nuclear weapons originates from. Naturally, nuclear conflict has devastating effects for all states, yet the actors related to the threat of nuclear conflict are namely those states, who obtain nuclear weapon capabilities. Regardless of the state-centric perception of the nuclear threat power dynamic, concerns of non-state actors acquiring nuclear capabilities have arisen. However, the probability of non-state actors participating in nuclear warfare currently remains low.[89]

The ability to distinct where the national security threat originates from reflects the either-or nature of nuclear related threats.[90] The nuclear capabilities of states are generally well known because of the information-sharing obligations and the difficulty of keeping such resources in secret. The development of nuclear weapons entails operating nuclear tests, which usually invoke interest by neighbouring states. Currently, the United States, Russia, the United Kingdom, France and China are certainly known to have nuclear weapons. In addition, India, Pakistan and North Korea have been known of conducting nuclear weapons tests and Israel is believed to acquire nuclear weapons, regardless of having not done any nuclear tests or confirmed the assumption.[91] The power dynamic in nuclear threats is usually distinguished and the origin of the threat or attack is known. Since the players of a cyber conflict are distinct, deterrence, or a balance of fear, may be relied upon as a control measure. It works if each side has enough nuclear capabilities to maintain a belief that a nuclear attack would lead to retaliation, so the possessors of nuclear capabilities are encouraged to not use them to secure their own safety.[92] Deterrence works when the nature of the threat is defined, and the power dynamic is bilateral. On the other hand, actors behind cyber threats may be impossible to determine, especially when the threat itself may be programmed to conceal any evidence.[93] Deterrence was and still is an important aspect of managing the threat of nuclear conflict. It describes well, how distinguished the power dynamic is in nuclear-related security threats.

The state-centric threat landscape describes the nature of the nuclear technology industry. Nuclear assets and resources are centralized to governmental companies and tightly monitored private companies within, for example, the nuclear energy industry. Nuclear goods and

[89] See e.g., Sokova 2017.
[90] Nye Jr. 2016, p. 50.
[91] See e.g., Stockholm International Peace Research Institute 2021.
[92] Miller 2017, p. 169-170.
[93] Nye Jr. 2016, p. 50.

technologies do not have commercial value in the same sense as some cyber goods, meaning that the trade controls on nuclear goods and technologies are targeted to a defined group of entities. Civilian individuals or non-state actors are not likely to acquire nuclear goods or technologies in an extent that would cause a threat to international security.[94]

In contrast with nuclear threats, the realm of cyberspace is characterized by obscurity. Since actions in cyberspace have only a limited attachment to physical places or resources, the actors behind cyberattacks may remain unknown.[95] The cyber goods industry covers various different items, which may be obtained by states, civilians, military entities, and non-state actors alike. Where is the line between a personal computer and a military weapon, if both resources can participate in or conduct a cyber operation that results in an international security threat? The role of non-state actors and even civilian individuals in cyberattacks is increasingly significant.[96] National security threats originating in cyberspace cannot be placed to the same power dynamic as nuclear threats, since security threats caused by cyber operations vary significantly in nature.

The origins, incentives, and effects of cyber operations were discussed briefly in the introduction of this paper when three examples of security-threatening cyber operations were presented. Those examples showed that the variety in the nature of cyber operations goes beyond what has previously been considered as international security threats. Controlling measures relying on the bilateral power dynamic, such as deterrence, do not apply when the nature and origin of the threat is unknown. In addition, the cyber goods industry[97] is powered by private companies. Generally, the market for software and other cyber goods is geared towards private entities and not just governmental entities or strictly controlled industries. Because of the global and consumer-centred market, wide-spread distribution of cyber goods among civilians, and the strong role of private companies in the production, distribution, and research, the nature of the cyber goods industry is highly de-centralized in comparison to that of the nuclear goods industry. In addition, a lot of research and development takes place in the cyber goods industry. The nature of common research and development practices can be

[94] In recent years, the threat of non-state actors like terrorist groups obtaining nuclear weapons has been on the rise. Regardless, the production and acquisition of nuclear weapons still remain in the hands of individual states. See e.g., Black-Branch 2017.
[95] The complexity of some cyber actors is visible in, for example, the hacker collective Anonymous, which is non-centralized, loosely organized, and yet has had a significant part in various cyber operations affecting states. See e.g., Olson 2013.
[96] See e.g., Stevens 2020.
[97] Cyber goods industry is used here as a broad term to cover, e.g., the software, hardware, and information security industries within which dual-use cyber goods may be produced, possessed, and traded.

described as a double-edged sword: in order to produce a secure system, it needs to be tested by hacking it.[98] Common practices include reverse engineering and vulnerability testing, which require that the system can be tested in ways used by potential malicious actors.[99]

Another core difference between nuclear and cyber capabilities is the ownership of the assets that can be used for security-threatening attacks. Nuclear weapons are possessed mainly by states, namely the five nuclear-weapon states determined by the NPT.[100] In comparison, the ownership of cyber resources is more distributed among different entities. A significant part of critical cyber infrastructure is in the hands of private companies, exceeding state borders.[101] The difference in asset distribution affects the available control measures, requiring that an active connection is maintained between the public and private sector. Control measures that have proved to work for nuclear non-proliferation, such as information sharing protocols, may suffer from the lack of centralization in cyberspace. Due to the decentralized nature of cyberspace, a single entity cannot have control over the resources used for cyberattacks. Thus, there is a gap between decision-making national and international entities and the mainly private entities having control over cyber resources.[102] To conclude, resources used for cyberattacks cover various categories and are distributed to multiple entities, mainly within the private sector. The ambiguity in the definition of cyber goods or cyber weapons reflects the complexity of determining, which entities have cyber capabilities and what those capabilities are.

3.2.3 The nature of the goods

Like stated in the previous sub-section, the nuclear threat landscape is characterized by the assets and resources being centralized mainly to governmental entities and monitored industry companies. The centralization of nuclear goods and technologies stems from the lack of a consumer market within the industry.[103] The scope of security-threatening nuclear goods and technologies can be determined relatively comprehensively due to the clear definition of the goods and technologies. Referring back to the previous sub-section, the evaluation of states' nuclear capabilities is possible because the nature of nuclear goods is well defined, and the

[98] See e.g., Stevens 2020.
[99] See e.g., Sommer 2006.
[100] Nuclear-weapon-states include the United States, Russia, China, the United Kingdom, and France.
[101] Baker – Filipiak – Timlin 2011, p. 29.
[102] The gap between public and private entities in cyberspace has been recognized by, e.g., NATO Industry Cyber Partnership, which aims to include industry representatives in cyber defense.
[103] See e.g., Black-Branch 2017.

definitions used have stabilized throughout the years. The destructiveness of nuclear goods and technologies can be evaluated with objective criteria, such as simply evaluating the quantity of the assets acquired by different states or other entities. Whereas the nuclear capabilities of states can be compared based on quantity[104], there is no reliable way of evaluating the cyber capabilities of states. Measuring cyber capabilities by quantity may be misleading, since the damage caused by using certain cyber goods is not tied to brute force. Security-threatening outcome of cyber operations oftentimes depends vastly on the skill and knowledge of using the resources in a destructive way. Because of the uncountable nature of cyber goods, determining the cyber capabilities of states is troublesome compared to conventional military capabilities. Ranking states by their potential of creating cyber security threats is a complex task since resources used for cyberattacks may include software, hardware, network infrastructure as well as human skills and knowledge. In recent years, various states have amped their cyber military capabilities, yet the increase in resources may also be allocated merely for cyber defence.[105] Thus, the complexity of determining what are the relevant countable assets complicate encompassing the cyber threat landscape and possible security-threatening cyber operations.

In addition to cyber goods largely being uncountable, their partially virtual nature also creates additional complications. Cyber goods may be traded globally without the transaction depending on a physical medium. The distribution of cyber goods is also practically unlimited.[106] Since the spread of non-physical software is nearly impossible to control, limiting the trade with centralized trade restrictions is an ambitious task. Another crucial feature in cyber goods is how they are produced. For example, malware is generally a piece of malicious code that is designed to infiltrate a computer system and execute pre-determined commands, like encrypting all the system's data. In principle, anyone can code a piece of malware and distribute it to an unlimited number of computer systems globally, since the main resource required in malware production is skill and knowledge.[107] Despite targeting the commercial production and trade of cyber goods with trade policy, stopping private actors from producing and distributing malicious cyber goods may not be done with the same measures.

[104] See e.g., the Arms Control Association 1/2022. It should be noted that comparison based on quantity alone may be misleading. Due to technological development and the modernization of nuclear weapons, there are significant quality differences between warheads. However, assessing quality features of nuclear weapons falls outside the scope of this paper. See e.g., Kluth 18.6.2020.
[105] See e.g., Sabillon – Cavaller – Cano 2016.
[106] See e.g., Macdonald – Frank 2017.
[107] Ibid.

The vague definition of cyber goods and their uncountable virtual nature complicate adapting trade policies as a control measure. While the category of dual-use goods and technologies is clearly distinguished and the items are centrally acquired by governmental entities, practically any civilian, malicious actor, state leader, or criminal may accumulate the goods for launching a security-threatening cyber operation. This is not to say that launching a cyber operation or an attack would be realistic or feasible, but as far as cyber goods are considered, they are available for anyone. These remarks reflect the crucial differences between the nature of cyber and nuclear dual-use goods.

4 Applying non-proliferation principles to cyber goods

4.1 The Wassenaar Arrangement

4.1.1 Overview of the Wassenaar Arrangement

The Wassenaar Arrangement is a voluntary framework established in 1996 after a preceding framework known as the Coordinating Committee for Multilateral Export Controls (CoCom) was terminated in 1994. After the Cold War era had ended, the demands for trade policies on dual-use goods changed. The core of the CoCom regime, the non-proliferation approach, was continued in the Wassenaar Arrangement alongside new trade control measures. The main objective in the Wassenaar Arrangement was determined to be transparency and co-operation in the trade of dual-use goods and technologies.[108] For example, members of the Wassenaar Arrangement may contribute to voluntary information exchanges relating to completed exports of some of the goods included in the Arrangement's control list.[109] These measures were set to avoid "destabilizing accumulations" of dual-use goods or technologies that would threaten national security of the participating states.[110] The Wassenaar Arrangement's intention is to "stop the threat at its root" by decreasing the amount of security-threatening goods in trade.[111] The additions made to Wassenaar Arrangement aimed to address the change in the international political environment and threat landscape after the Cold War. By nature, the Wassenaar Arrangement is a political document and not legally binding. Instead, the efficiency of the regime is based on a consensus between the participating states to uphold restrictions on the transfer of goods listed on the control lists.[112]

Nuclear and cyber threats are characterized by crucially different features. While there is a relatively clear understanding of what kind of goods are used in nuclear conflict, cyber conflicts can be created by the malicious use of various different cyber goods, such as malware or espionage software. Nuclear weapon assets are centralized to nuclear-weapon states, whereas cyber assets are distributed globally within civilians[113], private companies, militaries, and non-governmental organizations. The nature of nuclear threats has been defined and the consequences are known, whereas the nature of cyber threats ranges widely, and the effects

[108] Wassenaar Arrangement Public Documents Vol. 1, Initial Elements.
[109] Arms Control Association 2/2022.
[110] Wassenaar Arrangement Public Documents Vol. 1, Initial Elements.
[111] Ibid.
[112] Wassenaar Arrangement Public Documents Vol. 1, Initial Elements, section III.
[113] The distribution of cyber assets is not equal, but in principle cyberspace can be accessed from anywhere in the world. See e.g., Statista 26.4.2022.

may remain unidentified even after the attack has been launched. These differences affect what control measures are efficient and suitable for avoiding or minimising potential national security threats caused by the goods. The nature and features of nuclear threats shaped the non-proliferation approach, which has continued to be applied to other goods as trade policy is chosen as a controlling measure.

Since the legal status of cyber goods is still forming, there is no specific trade regime for controlling the trade of cyber goods. Thereby, existing regimes controlling other potentially harmful items are extended to include cyber goods. Wassenaar Arrangement governs the trade of conventional weapons as well as dual-use goods and technologies, including certain cyber goods. Regardless of the differences between different types of dual-use goods, Wassenaar Arrangement applies a relatively similar non-proliferation approach to all goods. All member states of the regime are required to set the required measures for preventing unauthorized transfers of the controlled goods.[114] The measures included in the Wassenaar Arrangement cover export licenses and information exchanging protocols to promote international co-operation between the participating states. Under the Wassenaar Arrangement control lists, member states exchange information on deliveries made and licenses granted to non-Wassenaar states, with the aim of maintaining an understanding of the total amount of arms and dual-use goods in circulation.[115] The objective of implementing the trade measures is to avoid destabilizing accumulations of dual-use goods.

4.1.2 Non-proliferation approach in the Wassenaar Arrangement

Initially, the Wassenaar Arrangement applied to WMDs as a complementary measure alongside the specified non-proliferation treaties. Besides the non-proliferation frameworks that focus strictly on a certain group of WMDs, like the NPT or Chemical Weapons Convention, the Wassenaar Arrangement has extended the non-proliferation regime to apply to various other goods. In practice, the scope of the Arrangement has been widened as new national security threats have emerged. The regime has been analogically applied to new goods that are considered to share the dual-use nature of the goods that the Wassenaar Arrangement initially governed. The extension of the Arrangement's scope has been done by adding new sections to

[114] Wassenaar Arrangement Public Documents Vol. 1, Initial Elements.
[115] Ibid.

the export control list. Thus, the initial elements or the mechanisms of the Arrangement have not changed much during the development.[116]

The Wassenaar Arrangement reflects the non-proliferation approach to potentially harmful goods by assuming that the root cause of security threats is the availability of dual-use goods. In the core of the Wassenaar Arrangement is the concept of "destabilizing accumulations of conventional arms and dual-use goods and technologies"[117]. The concept is arguably based on the assumption that minimizing the number of sensitive goods in circulation correlates to minimizing security risks caused by those sensitive goods. To some extent,[118] accumulations of conventional and nuclear weapons can be measured by the quantity of the goods.[119] Despite monitoring compliance with nuclear non-proliferation is not necessarily a straightforward task[120], setting effective monitoring frameworks is allegedly feasible in the context of nuclear dual-use goods. Measuring the attacking power and damage potential of cyber goods is not as straightforward. The technological development of cyber goods is rapid, which is why establishing frameworks for evaluating cyber capabilities or monitoring compliance seems like an inconvenient approach. The cyber goods controlled by the Wassenaar Arrangement cannot be categorized under a uniform group, further complicating how accumulations of the controlled cyber goods can effectively be evaluated. The destabilizing nature of cyber goods is not tied to the quantity of the goods but the quality and way they are utilized. The concept of destabilizing accumulations is at the core of applying trade policy as a security measure. Regardless, the nature of cyber goods does not adapt to the concept well. The incompatibility of the concept of destabilizing accumulations and the nature of cyber goods expresses the broader issue of applying trade policy as a controlling measure to cyber goods.

A general comparison of nuclear and cyber goods as objects of trade indicates that there are some similarities based on which a similar control regime may be suggested. Both goods can be traded, share the dual-use nature and are capable of creating threats for international safety. Additionally, international trade law allows setting trade restrictions for both types of goods based on their security implications. Regardless, when evaluating the nature of cyber goods and cyber threats in detail, the analogical application of an existing control regime seems to have

[116] Guidelines and other supplementary documents have been issued, but the fundamental structures of the WA remain the same. See e.g., Wassenaar Arrangement Public Documents Vol. IV.
[117] Wassenaar Arrangement Public Documents Vol. IV.
[118] See e.g., footnote 104.
[119] Wassenaar Arrangement Explanatory Note 1998.
[120] U.S. Department of State 2021, p. 2.

some deficiencies. For the trade restrictions to be effective and purposeful, they need to correspond to the nature of the goods. Based on the identified differences, analogical application of a nuclear-oriented trade policy may not adapt to the nature of cyberspace.

4.2 Cyber goods governed as intrusion software

4.2.1 Intrusion software addition

The scope of Wassenaar Arrangement covers various items and technologies that can be described as cyber goods. The control list for dual-use goods and technologies is divided to nine different categories and separate lists for sensitive and very sensitive items. The categories are divided as follows:

Category 1 – Special Materials and Related Equipment

Category 2 – Materials Processing

Category 3 – Electronics

Category 4 – Computers

Category 5 – Part 1 – Telecommunications

Category 5 – Part 2 – Information Security

Category 6 – Sensors and Lasers

Category 7 – Navigation and Avionics

Category 8 – Marine

Category 9 – Aerospace and Propulsion

Items or technologies considered as cyber goods may fall at least under category 4 covering dual-use items and technologies related to computers, and category 5 covering those related to telecommunications and information security. This section of the paper discusses the category 4 and its definition of “intrusion software” in more detail.

In 2013, the scope of the category 4 was extended to cover so called “intrusion software”. The extension of the Wassenaar Arrangement was done by adding new criteria under the pre-existing category 4 to extend the applicability of the regime. The intrusion software addition responses to concerns related to military use of certain surveillance technologies in countries

such as Bahrain[121] and Libya[122], where surveillance technologies have been used to violate human rights of representatives of the press, political figures, and citizens living in the country or abroad. The intrusion software addition meant creating a new category of goods trade of which ought to be controlled. The inclusion of intrusion software pursues to reduce the trade done through illicit malware markets. The objective of the addition is to respond to the increasing issue of certain governments and non-state actors acquiring malware for illegitimate purposes, such as cyber espionage or political interference.[123]

The Wassenaar Arrangement defines intrusion software as follows:[124]

> *'Software' specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a computer or network-capable device, and performing any of the following:*
>
> *[a] The extraction of data or information, from a computer or network capable device, or the modification of system or user data; or*
>
> *[b] The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions*

The phrasing is intentionally left vague to apply to a variety of software.[125] Any resources used to build, implement, or communicate with intrusion software are covered by the definition. The definition could cover, for example, cyber goods that enable controlling or receiving data from another device remotely, such as keylogger or remote-control software. However, fulfilling the intrusion software definition does not yet entail that trade restrictions are applied. The term intrusion software is defined as a pre-requisite for the control list, which determines the specific categories of items that are controlled. The Wassenaar Arrangement's export controls apply, if the item maintains the quality and relationship of being any of the following[126]:

> *4. A. 5. Systems, equipment, and components therefor, specially designed or modified for the generation, command and control, or delivery of "intrusion software".*
>
> *4. D. 4. "Software" specially designed or modified for the generation, command and control, or delivery of, "intrusion software".*
>
> *4. E. 1. c "Technology" for the "development" of "intrusion software".*

[121] See e.g., Marquis-Boire 10.10.2012 on the use of surveillance tools in Bahrain.
[122] See e.g., EDRi 23.5.2021 on the use of surveillance tools in Libya.
[123] Herr 2016, p. 176.
[124] Wassenaar Arrangement Public Documents Vol. II p. 224.
[125] Herr 2016, p. 182.
[126] Wassenaar Arrangement Public Documents Vol. II.

4. D. 1. a "Software" specially designed or modified for the "development" or "production" of equipment or "software" specified by 4.A. or 4.D.

4. E. 1. a "Technology" according to the General Technology Note, for the "development", "production" or "use" of equipment or "software" specified by 4.A. or 4.D. --- c "Technology" for the "development" of "intrusion software"

The intrusion software addition includes exceptions that aim to narrow the scope of the export controls from being overly extensive. The "General Software" and "General Technology" notes of the 2013 addition determine that publicly available commercial software or other technology does not fall under the scope of the trade restrictions.

The Wassenaar Arrangement includes some general exclusions that apply to all categories on the control list, thus, also to cyber goods such as intrusion software. The General Technologies Note excludes the following technologies from the trade restrictions[127]:

The export of "technology" which is "required" for the "development", "production" or "use" of items controlled in the Dual-Use List is controlled according to the provisions in each Category. This "technology" remains under control even when applicable to any uncontrolled item.

Controls do not apply to that "technology" which is the minimum necessary for the installation, operation, maintenance (checking) or repair of those items which are not controlled or whose export has been authorised.

Controls do not apply to "technology" "in the public domain", to "basic scientific research" or to the minimum necessary information for patent applications.

In addition to the General Technology Note, the Wassenaar Arrangement also includes the General Software Note, which further limits the scope of the trade restrictions:

The Lists do not control "software" which is any of the following:

1. Generally available to the public by being:

a. Sold from stock at retail selling points without restriction, by means of:

1. Over-the-counter transactions;

2. Mail order transactions;

3. Electronic transactions; or

4. Telephone call transactions; and

[127] Wassenaar Arrangement Public Documents Vol. II, p. 3.

b. Designed for installation by the user without further substantial support by the supplier; Note Entry 1 of the General Software Note does not release "software" controlled by Category 5 - Part 2 ("Information Security").

2. "In the public domain"; or

3. The minimum necessary "object code" for the installation, operation, maintenance (checking) or repair of those items whose export has been authorised.

The General Software and General Technology Notes aim to limit the scope of the control lists to ensure that the legitimate trade of any commonly used items is not interfered with. Especially the "public domain" and "basic scientific research" exceptions are beneficial for ensuring that the intrusion software addition does not limit the trade of cyber goods in an unnecessary manner. The corollary effects caused by the trade controls are discussed in more detail in section 4.3.

4.2.2 Industry critique

The intrusion software clause was added to the Wassenaar Arrangement in 2013, following which each participating state ought to implement the new addition in their national trade legislation. In the United States, Bureau of Industry and Security (BIS) under the Department of Commerce issued a proposal of how the software addition would be implemented in 2015. The proposal included a set of controlling measures that would implement trade restrictions on intrusion software in practice. The software industry voiced their concerns on the initiative, drawing attention on the proposed controls not being compatible with the industry practices. The proposal made by BIS was broader than what was required by the Wassenaar Arrangement text. Exceeding the intrusion software definition in the Wassenaar Arrangement, the BIS proposal included the following definition:

> *Systems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, intrusion software include network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices.*[128]

The scope of the definition exceeded even the Wassenaar Arrangement's definition of intrusion software, causing concerns of negative impacts on research and development. The extensive

[128] U.S. Department of Commerce's Bureau of Industry and Security 2015, p. 4.

definition of intrusion software would have entailed that export licenses for various software used in cybersecurity research would have been presumptively denied.[129]

After BIS published the implementation proposal to request comments, the proposal was amended based on the feedback given by industry stakeholders. The BIS clarified that the Wassenaar Arrangement's exceptions for technology in the public domain or used for basic scientific research will be included in the implementation of the trade restrictions.[130] Regardless of the clarifications, some concerns remained on the proposal not adapting to how research is conducted in the industry.[131] After industry stakeholders voicing their concerns on the intrusion software addition's unintentional consequences, United States proposed an amendment to the intrusion software definition in the 2016 Wassenaar Arrangement plenary. Following the proposal, the category covering intrusion software was amended.[132] Also, the license requirement exceptions were revised to better determine the technologies that fall outside the scope of the restrictions.[133] The changes can be considered successful in the extent of enabling vulnerability disclosure for research purposes and incident response. The concept of intrusion software still remains in the Wassenaar Arrangement, despite many industry lobbyists hoping for its complete removal.[134]

The discussion surrounding the Wassenaar Arrangement's intrusion software addition reflects some of the general issues of applying trade policy as a control measure for cyber goods. The intrusion software addition faced backlash for potentially causing corollary damage to research and other legitimate activities. Regardless of industry stakeholders actively voicing their stance on why the intrusion software controls should not be implemented, even the revised version of the Wassenaar Arrangement failed to repair the inconsistency and ambiguity in the scope of the determined controls. The changes made in the 2016 Plenary Session did not remove the legal uncertainty caused to industry stakeholders.[135] The issues discussed in this sub-section reflect the broader issue of extending a pre-existing legal regime to cover operations in cyberspace. The following sub-section will elaborate on the possible reasons for the issues in the intrusion

[129] According to a statement by a BIS director, software having or supporting rootkit or zero-day capabilities would have received a presumptive denial based on the proposal. Such software is used in cybersecurity research to demonstrate the validity of any found software vulnerabilities. The statement is cited in Galperin 28.5.2015.
[130] Frequently asked questions regarding the BIS proposal discussed in Galperin 12.6.2015.
[131] Some unclarity remained on researchers' conduct on reporting vulnerabilities to vendors without making them public, see e.g., Galperin 12.6.2015.
[132] Wassenaar Arrangement Summary of Changes 2017, Category 4.
[133] Wassenaar Arrangement Plenary Session 2016.
[134] Cardozo – Galperin 29.2.2016.
[135] Ibid.

software addition by highlighting remarks regarding the nature of cyber goods and the cyber goods industry. The problems with the intrusion software addition seem to be a part of the larger picture of how trade policy measures designed for conventional goods do not fit the characteristics of cyber goods.

4.3 Issues with applying the Wassenaar arrangement to cyber goods

4.3.1 Nature of the industry

The differences between nuclear and cyber goods were observed previously in the sub-section 3.2 by discussing two aspects: nature of the industry and nature of the goods. These aspects were evaluated in order to determine the differences between nuclear and cyber dual-use items which may affect how they can be effectively governed. The distinguished differences support the argument that trade policies are neither suitable nor effective for controlling security threats created by cyber goods. Observations on the nature of cyber goods and the cyber goods industry are evaluated in this section in the context of the Wassenaar Arrangement's intrusion software addition. The socio-legal method is applied to observe the surrounding societal context and contradictory interests of stakeholders, mainly states and private companies. The issues recognized in the software intrusion addition seem to reflect the broader issues of applying trade policy as a control measure to cyber goods. The critique given by industry stakeholders is examined in the context of the characteristics recognized in section 3.2.

Based on the remarks made in section 3.2, the relevant characteristics of the cyber goods industry include the strong role of the private sector, consumer-centred market and industry-specific research and development practices. Generally, many of the issues in the intrusion software addition seem to relate to the cyber goods industry being an industry driven by private companies. Observing industry practices inadequately resulted in the offered solution being unsuitable for the demands of the private sector. Since the vague phrasing of the intrusion software addition may unintentionally cover a lot of less harmful cyber goods, private sector stakeholders bear the consequences. The production, distribution and possession of cyber goods is dominated by private actors, such as private companies and civilian individuals. The cyber goods industry is largely a consumer-centred sector, unlike the nuclear industry. In the governance of cyber goods, the co-operation between governmental and private actors seems to have failed at least when the intrusion software addition was prepared.

The Wassenaar Arrangement did not sufficiently include the opinions and views of industry stakeholders, including researchers and developers, while preparing the intrusion software

addition. Going beyond the Wassenaar Arrangement, achieving active co-operation between essential stakeholders does not seem impossible. To acknowledge the nature of the cyber goods industry, the preparation of any trade policy that governs cyberspace should highlight the views and opinions of private actors as an essential input for the trade policy. Defining the scope of the trade restrictions with common terminology used in the software industry would possibly remove some of the ambiguity. Applying trade policy analogically to control cyber goods cannot succeed unless the industry practices are addressed accordingly. The issues highlighted in this section demonstrate that the trade policy approach has not yet adapted to the demands of cyberspace.

The non-tangible nature of software poses a challenge for legal governance. The trade of cyber goods does not entail the transfer of physical goods, which affects how it can be controlled. Since hackers, activist groups and other non-state actors have a vital role in cyberspace, limiting the trade of cyber goods with a state-centric approach may not bring great results for ensuring international security. The export license requirement mostly affects private companies that pursue to make a profit by producing and selling certain cyber goods. Since private companies seeking commercial profit may not have the same motivation to ensure security interests as states have, the security interests behind the trade restrictions and the business interests at stake create a troubling balance of interests. In combination with the inadequately defined scope of the intrusion software addition, private companies may not be incentivised to comply with the requirement.[136] The trade policy restrictions cause disadvantages to commercial profitability and innovation by incorrectly assessing the nature of the industry and cyber goods in general. As a consequence, private actors following market incentives may be encouraged to either operate illegally or move their business to a jurisdiction lacking similar restrictions.

4.3.2 Nature of the goods

The second aspect, nature of the goods, reflects how dual-use cyber goods vary as objects for trade from other dual-use goods. Characteristics of cyber goods highlighted in the section 3.2 include uncountable nature of the goods, obscure definition and virtual nature. As already discussed above, defining the cyber goods that ought to be controlled with trade restrictions is a demanding task. The issues of the intrusion software addition were mainly caused by the definition and scope of what was meant by intrusion software. The intrusion software definition

[136] For more information on what compliance with trade restrictions entails for private companies, see e.g., Catrain – Peters – Boyette – Lock 2016, section 5.

establishes a base for the control list that includes the specific items to which the trade restrictions apply in practice. It was acknowledged that the definition should not be too specific, or otherwise it would not adapt to the development of technology. However, the definition chosen in the Wassenaar Arrangement and the implementation proposal drafted by the BIS was inevitably too broad and vague to effectively scope the items that ought to be controlled. Hence, the overly broad definition and insufficient exception clauses resulted in the information security and software industries to bear the corollary consequence of legitimate practices being affected by the trade restrictions.[137] These issues with composing a comprehensive yet adaptable description to define the scope of the controlled goods seem to reflect the obscure nature of cyber goods. Due to the rapid technological development and broad selection of different types of cyber goods, achieving a sufficient description of what is meant by cyber goods may be an invincible dilemma.

When looking more in detail to the nature of the goods, the focus shifts from the issues in the Wassenaar Arrangement to the broader issues of governing cyber goods with trade policy altogether. In the section 3.2, the uncountable nature of cyber goods was introduced as one main difference between nuclear and cyber dual-use goods. The question remains, whether security threats in the cyber space should even be governed as trade policy matters. The intrusion software addition originated in concerns of the use of surveillance technologies by certain government entities for illegitimate tracking purposes. This issue relates to the uncountable nature of cyber goods; the harm potential caused by using dual-use cyber goods for malicious purposes is not tied to the quantity of the items. Even one malicious actor downloading a dual-use software can create security-threatening consequences. Thereby, to effectively control security-related issues in cyberspace, the trade controls would need to reach all illegitimate trade to truly control the issue. Otherwise, the malicious actors will just find another source for the technologies and tools needed for the cyber operations. Trade controls in cyberspace have already proven to be ineffective in controlling trade in a sufficient manner.[138] This aspect relates to the virtual nature of cyber goods. Controlling the trade of dual-use cyber goods is extremely hard due to the lack of physical presence or transaction. Like demonstrated in cases related to

[137] See e.g. Galperin 28.5.2015.
[138] Software company Hacking Team has provided spyware to Sudan regardless of UN's embargo on the trade of arms to the country. See e.g., U.S. Bureau of Democracy, Human Rights and Labor 2015.

illegitimate trade of spyware, virtual nature of the transactions enables evading trade policy restrictions.[139]

The uncountable and virtual nature of cyber goods enables unlimited global distribution. Since dual-use cyber goods may be traded over the internet in a matter of seconds, the means of distribution are very different from those of conventional dual-use goods or technologies. Additionally, items categorized as dual-use cyber goods may be acquired by civilian individuals or non-state actors more easily than other dual-use goods. Based on these remarks, aspiring to "cut the problem at its root" as stated in the Wassenaar Arrangement is simply not possible given the nature of cyberspace.

4.3.3 The general issues of governing cyber goods with trade policy

The backlash that followed the Wassenaar Arrangement's intrusion software addition and its implementation, especially by the U.S., draws attention to the aspects where trade policy fails to adapt to cyberspace. Perceiving dual-use cyber goods as contiguous to conventional dual-use goods may stem from the similar terminology used to categorize operations, or from the national security exception in GATT applying to cyber-related security threats as to any conventional security-threatening scenarios. As demonstrated by the examples of different cyber operations, conflict in cyberspace may lead to severe consequences just like conflicts on land, sea, or air. However, the non-proliferation focused trade policy seems to rely on the analogy between dual-use cyber and nuclear goods without questioning its grounds. When taking a closer look on trade policy as a control measure in dual-use goods governance, the prominent approach does not seem to adapt to cyberspace regardless of the initial similarities. Simply adding new items to the Wassenaar Arrangement control list does not effectively decrease the likelihood or severity of cyber threats. Arguably, each model for legal governance requires compromises. However, observing the nature of cyber goods and the cyber goods industry, the disadvantages of the non-proliferation approach seem to exceed the benefits.

The objective of evaluating the private sector's denial of the intrusion software addition through the characteristics of cyber goods and the cyber goods industry is to reach a conclusion on the broader question of whether trade policy is a suitable measure for controlling cyber-related security threats. The issues that arose with the intrusion software addition reflect a deeper incompatibility between trade policy and dual-use cyber goods in general. The trade policy

[139] Ibid.

approach has not adapted to the cyber goods industry, which is largely driven by private companies. Controlling dual-use cyber goods with trade restrictions is not a suitable approach since the damage potential of cyber goods is not tied to the quantity of the goods in circulation. The virtual nature of the goods enables unlimited possibilities for trade over the internet, further deteriorating any aspirations of an effective trade control regime. Beyond the nature of the goods, the governing mechanisms also inherit stubborn blind spots. Regimes established by inter-governmental organisations, like the WTO, regulate operations among states, further reinforcing a state-centric perception.[140] The trade of cyber goods encompasses various non-governmental stakeholders, which the inter-governmental approach fails to incorporate in an adequate extent. Additionally, the inherit obscurity in the nature of cyber goods seems to deteriorate part of the benefit created by trade policy regimes. The vagueness of the definitions of "intrusion software" and cyber goods in general makes it harder to upkeep purposeful registers or information sharing regimes. The problem of including cyber goods under the Wassenaar Arrangement is that the scope of the goods is poorly determined, and the measures of the Arrangement do not seem to adapt to the nature of the cyberspace. The analogical extension of existing trade policy frameworks cannot effectively control security threats in cyberspace before the legal status of cyberspace has fully developed. The chosen approach for legal governance of cyber threats lacks common consensus of what the issue precisely is. Defining the cyber threat landscape requires participation from all stakeholders, including states, non-state actors, private companies, and individuals.

Regardless of the problems cyber goods governance has faced, it is of utmost importance that governmental entities, private companies, and individuals understand the severity of cyber-related threats. Trade policy being an unfit approach for security governance in cyberspace does not entail that the threats should not be controlled at all. One issue with the analogical extension of a trade policy approach is that other solutions for security governance may not be explored in full. The ineffectiveness of trade controls in cyberspace should prove that other control measures need to be reviewed instead. In cyberspace, defence may be the best offense. As technology progresses and new exploits, methods and hacks become prevalent, governmental entities and private organisations need to have adequate cyber defence capabilities. By improving the level of cyber defence, information systems are less likely to be affected by cyber operations that are conducted potentially using dual-use cyber goods. Various states and intergovernmental organizations have already established comprehensive cyber defence

[140] See e.g., Pearson 2004.

strategies to assess and control risks in cyberspace.[141] Efforts to increase cybersecurity capabilities on national and international levels may address cyber threats in a broader manner than trade policy. Promoting cyber resilience could be a more effective and sustainable solution than attempting to control the trade of dual-use cyber goods. Cooperation between the public and private sector to increase cyber resilience has proven to be an effective model for preventing and handling cyber incidents.[142] Another solution for managing cyber threats is shifting resources to the investigation and prosecution on cybercrimes.[143] Instead of the Wassenaar Arrangement's idea of cutting the problem at its root (ineffectively), cyber threats need to be governed with a comprehensive approach to truly avoid the worst-case scenarios such as full-blown cyber warfare. Cybercrime causes significant economic loss and has grave consequences globally.[144] Including security-threatening operations as cybercrimes under national cybercrime legislation may target those operations more effectively than widely applicable trade restrictions. Criminalising security-threatening operations instead of specific tools may also lead to less corollary consequences for the legitimate use of those tools. One issue in applying trade policy to cyber goods is the idea of using the same approach for very different situations just based on the domain being cyberspace. By defining specific crimes, criminal law adapts better to the differences between human rights violations, information theft, ransomware attacks, and so on. Another solution for governing the legal aspects of cyberspace comprehensively would be to establish a cyber convention as a base for any further regulation.[145] Establishing a multi-lateral cyber convention could support observing the complex relation between cyberspace and conventional domains. Cyber operations should not be governed as a separate phenomenon, yet the measures taken for legal governance ought to cater to the specific characteristics of cyberspace. Having a cyber convention as a starting point for regulation could provide a broader perception of cyberspace, which the current trade policy approach seems to lack. Trade restrictions may be used as a supplementary measure, but the governance of cyber-related security threats cannot be fully based on them.

[141] See e.g., Sabillon – Cavaller – Cano 2016.
[142] European Commission 2013, section 2.1.
[143] Regardless of cybercrime legislation offering an alternative model for legal governance, is inherits its own issues. See e.g., Sommer 2006.
[144] European Commission 2012, section 1.
[145] See e.g., Roche – Blaine, 2014.

5 Conclusions

5.1 Findings regarding the legal framework for trade restrictions and cyber goods in international trade law

During the 21st century, much of our lives has shifted to the fifth domain, cyberspace. Cyberspace is characterized by its virtual nature, which reflects the broader theme of globalization. As business, trade, government operations and society at large transfer to the borderless and global cyberspace, new security concerns arise. Since the significance of cyberspace is increasingly crucial, it is a tempting environment for interfering, attacking and destabilizing targets that otherwise would be hard to affect. Cyber operations have already created massive damage and negative consequences globally. Regardless of cyberspace vastly differing from other domains, the potential similarities in the motivation, actors, and outcome of cyber operations and conventional military operations lay grounds for a broader comparison. In the beginning of the paper, similarities are distinguished between cyberspace and conventional domains. The terms cyberattack, cyber weapon and cyber conflict partly follow the same elements represented in the corresponding terms without the "cyber" prefix. The shared elements encourage applying pre-existing legal concepts and approaches to phenomena in cyberspace, regardless of the crucial differences between the domains. The approach of applying a commonly embraced legal regime analogically to new phenomena based on some shared similarities can be recognized in the discussion and narratives on the legal governance of cyber goods. Following the legal realist theory approach, the choice of defining the legal status of cyberspace by seeking parallels from pre-existing legal concepts rather than evaluating cyberspace as a fully separate domain may affect how cyberspace is construed at large. The complexity of grasping new concepts in cyberspace may be eased by utilizing existing legal frameworks, such as the security exception in GATT. However, this choice affects the reality forming around cyberspace. Despite the analogous perception of cyberspace being seemingly rational, the disrupting nature of cyberspace as a domain is observed in this paper as an essential factor in exploring for the most suitable and effective model for legal governance.

To determine how international law applies to cyberspace, the legal concepts of sovereignty and security are explored in this paper with a constructivist method. Regardless of cyberspace being described as a virtual domain free of a physical presence, many aspects of the principle of sovereignty apply in cyberspace. Sovereignty is based on the prohibition of use of force on a sovereign state's territory and interference in a sovereign state's internal matters. As a closer look to cyber operations shows, operations in cyberspace may reach the threshold of a violation

against the prohibition of the use of force and interference. In addition to the principle of sovereignty, national security is a significant aspect in cyberspace. Cyber operations are often capable of interfering with the norms, values, and institutions of a sovereign nation. This kind of a destabilizing effect creates a threat to national security. Yet the terminology and legal concepts applicable to cyber operations are still forming, it is undisputed that cyber operations can threaten global security. Thereby, finding an effective model for legal governance is an urgent issue. In this paper, cyberspace is not discussed as a separate subject matter but as a part of society and the legal system at large. The fundamental principles of sovereignty and territoriality applying in cyberspace indicates that cyberspace is not a separate dimension of society, but a whole new layer which requires legal governance.

The discussion on the concepts of sovereignty and security sets a basis for evaluating trade policy as a model for legal governance. Cyber operations are characterized by the use of cyber goods, which cover a range of different offensive and defensive items used in cyberspace capable of operating or contributing to a cyber operation. The term "cyber goods" is used as an umbrella term to cover cyber weapons as well as civil cyber goods. Various cyber goods can also be categorized as dual-use goods based on their potential military applications. Since dual-use goods have legitimate and illegitimate purposes, a complete ban on the trade of the goods would not be purposeful. Balancing between restricting legitimate use of the goods the least possible amount as simultaneously halting the potentially harmful use cases is a challenging task for trade policy. The paper compares the governance of cyber goods to how nuclear goods have been governed. Regardless of many cyber goods being intangible, such as software, the trade of cyber goods can be subject to trade policy as various nuclear goods and technologies are. The threat of nuclear conflict has been a central focus of dual-use legislation, and the trade policy approach can be used as a good measure for evaluating legal governance of cyber goods.

To define international trade law's framework for applying trade policy as a control measure, the basis for regarding security interests is examined. Free trade is an essential principle in international trade law and a starting point in international relations. However, it is not without exceptions. To evaluate the core legal framework of international trade law, this paper observes the General Agreement on Tariffs and Trade as *de lege lata*. The GATT focuses on establishing non-discriminatory terms for international trade. Regardless of the strong free trade approach in GATT, the agreement includes mechanisms to account for other vital interests. The article XXI sets a security exception, that can be invoked in order to take measures for security reasons despite them otherwise infringing other GATT articles. Article XXI(b) allows active measures

to protect security interests, creating a legal basis for setting trade restrictions on dual-use goods. The scope of the article XXI(b) is broad, allowing measures specific to various dual-use goods, such as nuclear or cyber goods. The conclusion of the legal review conducted in this paper is that international trade law allows trade restrictions on dual-use goods based on security interests.

Assimilating cyberspace with other domains affects how broadly its disrupting characteristics are regarded in the chosen model for legal governance. The answer to the first research question on whether the legal basis for establishing trade restrictions as a security measure applies to cyber goods is affirmative based on the broad scope of the GATT article XXI(b) and analogical extension of existing legal terminology. However, the choice of applying existing legal concepts to cyberspace instead of comprehensively defining its legal status has implications beyond the legal governance of cyber goods. The applicability of the chosen governance model is further evaluated while answering the second research question.

5.2 Findings regarding the application of trade policy as a control measure on cyber goods

The research conducted in this paper demonstrates that international trade law allows trade restrictions to be set in place based on security interests regardless of the measures otherwise being discriminatory. In addition, the broad scope of the security exception provided by the GATT article XXI(b) applies to cyber goods, among many other types of dual-use goods. Thereby, there is a legal basis for controlling threats in cyberspace using trade policy. Restricting trade of potentially harmful goods is based on the assumption that less risky goods in the market equals less threats for security. The model for dual-use goods governance has originated in controlling military goods, such as weapons of mass destruction. For those goods, the non-proliferation approach is justified based on the potentially detrimental effects of the goods. However, as the threat landscape has evolved from conventional military settings to more obscure threats in cyberspace, the non-proliferation approach may not be justified. In addition to the initial scope, the concept of dual-use goods is applicable also to military technologies, such as spying malware or other software. According to the current interpretation, even cyber weapons do not fulfil the criteria to be considered as weapons of mass destruction, let alone other cyber goods. Based on these reasons, the analogical extension of the non-proliferation focused trade policy is evaluated critically in this paper.

The differences between cyber and nuclear goods are evaluated in detail to determine, whether a non-proliferation approach is suitable for controlling cyber threats. The comparison is conducted with a socio-legal method to recognize the societal context surrounding cyber and nuclear dual-use goods. The distinct features of both cyber and nuclear goods are examined with two aspects: nature of the industry and nature of the goods. The threat of nuclear conflict is often perceived as a power dynamic between states. Since nuclear weapons are mainly possessed by states, facilitating multilateral co-operation on the international level offers a sufficient forum for establishing governance frameworks. However, the power dynamic of the cyber goods industry is much more de-centralized. Private organisations have a central role in the production, possession, and trade of cyber goods. The remarks made regarding the nature of the cyber goods industry relate to the strong role of the private sector, consumer-centred market and industry-specific research and development practices. The findings on the nature of cyber goods relate mainly to the inherit obscurity of the goods as well as their virtual and uncountable nature. Due to the rapid development and varying technologies used in cyberspace, it is challenging to comprehensively define the scope of harmful cyber goods. The damage-potential of cyber goods is not tied to quantity, but more to the quality of the goods and knowledge of using the goods in a harmful way. Since cyber goods can be distributed across the globe, centralized controlling measures fail to address the root of the problem. As a personal computer or a legitimate software can be used to contribute to a harmful cyber operation that results in a security threat, achieving complete control over the trade of cyber goods is arguably an impossible task. These remarks reflect the aspect that regardless of trade restrictions being adaptable to threats in cyberspace, they may not be the most suitable solution for legal governance.

After the evaluation of differences between nuclear and cyber goods, the paper observes Wassenaar Arrangement using the legal dogmatic method. The Wassenaar Arrangement governs the trade of dual-use goods by setting export license requirements and protocols for cooperation among the participating states. It applies to various dual-use goods since the export control list has been continuously extended to cover new categories of goods. The Arrangement is not specified to one category of goods like other non-proliferation regimes, such as the NPT. Regardless of the export control list being extended, the fundamental logic and mechanisms of the Wassenaar Arrangement have not changed much during its development. The concept of “destabilizing accumulations of dual-use goods and technologies” is included as a core aspect in the WA’s Initial Elements, reflecting the idea that there is a certain quantity of dual-use goods

which creates a destabilizing security threat. Based on the findings on the nature of cyber goods, the quantity-focused approach does adapt to the specific characteristics of cyber goods.

Cyber goods were included under the scope of the Wassenaar Arrangement by adding "intrusion software" as a category on the export control list. The addition mainly focused on tackling software used for information warfare, but it applies to a wide variety of other software as well. The addition caused controversy amidst scholars and industry stakeholders up to the point that it was updated in 2016. The findings made regarding the nature of the cyber goods industry and the nature of cyber goods reflect the issues in the intrusion software addition. Especially the inadequate inclusion of the private sector in the preparation of the intrusion software addition seems to have caused most of the issues. Due to the obscure nature of cyber goods, the definition of the controlled goods was neither specific nor concise enough. Software companies and the technology industry in general bear the consequences of the issues in the Wassenaar Arrangement's intrusion software addition, since the overly broad definition of intrusion software causes unnecessary corollary consequences. The disadvantages caused to actors in the private sector may exceed the benefit created by the trade policy approach, thus making it an unfavourable compromise. Thus, the trade restrictions on cyber goods may result in unintentional industry effects, such as companies trying to avoid the restrictions with unethical practices. If the trade restrictions are poorly prepared and do not seem justified, non-compliance may arise as an issue. The vague scope of the intrusion software addition leaves room for legal uncertainty even after the 2016 updates creating corollary damage to legitimate activities within the cyber goods industry. In addition, the non-tangible and virtual nature of cyber goods creates a challenge for implementing trade restrictions in practice. Based on the findings of this paper, the Wassenaar Arrangement's attempt of addressing cyber threats is not an effective way of controlling cyber threats. The remarks made regarding the intrusion software addition reflect the broader misfit between trade policy and cyber goods.

Description of the framework for setting trade restrictions, the non-proliferation nature of dual-use goods governance, and the nature of cyber goods support answering the second research question. Since the nature of cyberspace differs vastly from other domains, the pre-existing trade policy approach seems to fail at providing suitable and effective measures for governing dual-use cyber goods. The critique on the Wassenaar Arrangement's take on cyber goods governance goes beyond the specific regime, since the same issues likely remain in any regime that pursues to effectively control security threats in cyberspace with a non-proliferation trade policy approach. To conclude, the answer to the second research question of whether trade

policy is a suitable model for governing threats in the cyberspace is in the negative. Based on the nature of cyber goods and the cyber goods industry, the non-proliferation approach is not an effective model for governing dual-use cyber goods. Applying trade policy analogically to cyber goods disregards the characteristics of cyberspace, possibly resulting in more corollary damage to the cyber goods industry than benefit in controlling cyber threats. Like discussed in the beginning of this paper, analogously extending the scope of existing legal concepts and terminology may provide a rational way for defining the legal status of cyberspace. However, disregarding the disruptive nature and special characteristics of cyberspace will not support establishing an effective model for governing its legal aspects in a long-term perspective. Possible solutions for improving security governance in cyberspace include facilitating cooperation with private sector stakeholders, comprehensively defining the legal status of cyberspace with a cyber convention, and promoting initiatives for increasing global cyber resilience. To achieve a sustainable model for legal governance of cyberspace, forgetting prior assumptions of the proper approach may be a more suitable option than building on the grounds of a previous system.