Refocusing Export Control Regimes to Effectively Address Cyber Security Concerns

Cindy Whang
Assistant Professor
Department of Financial and Economic Law
Fu Jen Catholic University

Abstract: Cyber security as a common security interest of NATO member states raises the question of how to promote it through different technical and policy constructs. One such aspect has been through establishing trade regulations like export controls to prevent the proliferation of military-use goods and technology for national security reasons. Since NATO's formation, member states have used export controls as a trade measure to protect their national security. As cyber security threats have become an important feature of the protection of national security, the role by which export control regulations should be used to address this new rising threat should be discussed. Export control regimes have traditionally functioned as a means to prevent the proliferation of military-use and technological goods from crossing borders. The two primary elements used to achieve that goal were the use of export control lists to determine the subject of export control and the allocation of export control liability to the violating party. While the export control regulations regulated 'technology' as an entity, before the widespread use of the internet, the control and enforcement of this intangible form of technology were predicated on the technology being installed on physical goods. In addressing cyber security concerns through export control regimes, this paper analyses the construct of export control lists and the imposition of export liability through the lenses of cyber security concerns and argues that the current construct of export controls regulations might not be effective in addressing these concerns.

Keywords: *Export control regime, export control regulations, cyber security, control lists, export liability*

1. INTRODUCTION

The North Atlantic Treaty Organisation (NATO) created a political and military alliance between European and North American countries to provide for a collective defence alliance based on shared security concerns rooted in the common determination to protect the freedom, democracy, liberty and rule of law of member countries. In 1951, internal reports to the North Atlantic Military Committee reflected the concern that NATO's conventional forces had not met the requirements outlined to protect the NATO member states from a full-scale Soviet Union attack (NATO, 1951a; NATO, 1951b; Bitzinger, 1989). During that period, the United States (US) had reached a consensus with Britain and France to coordinate domestic export controls of strategic materials and technology that would prohibit specific goods from being exported to communist states and the multilateral coordination of domestic export controls was expanded to include other European countries as the restrictions were shown to be an important element in slowing down the technological advances that the Soviet Union gained from importing strategic goods (McDaniel,1993; Office of Technology Assessment, 1979). A separate international export control entity called the Coordinating Committee for Multilateral Export Controls (COCOM) was established to function as a collective means to wage economic warfare against the Soviet Union and the Soviet bloc. By 1985, all the member countries of NATO except Iceland were participating states of COCOM (McDaniel, 1993).

The structure of a modern export control regime was established through COCOM and consisted of multilateral negotiations done on an international level that would result in export control lists that countries would then have the discretion to adopt into their domestic export control regimes. COCOM had the strategic purpose of negotiating export control lists that would restrict military-use goods and technology from reaching the Soviet bloc, but it was established through a gentleman's agreement that did not give COCOM the ability to enforce the negotiated lists. The actual enforcement and implementation of export control lists were decided through domestic export control regulations and, in COCOM's early years, the US played a strong role in promoting the adoption of COCOM's export control lists into domestic export control regimes (McDaniel, 1993; Office of Technology Assessment, 1979). International export control agreements such as COCOM provided multilaterally negotiated export control lists and the domestic export control regimes offered different utilities that structured the elements of domestic export liability. Both are important in the discussion of export control regimes. The interplay of COCOM and domestic export control regulations worked together to create an added layer of economic policy consideration that worked to facilitate the collective defence for NATO member states.

The dissolution of the Soviet Union shifted the focus of NATO's security policy and also changed the purpose of international export control regimes. NATO went from being an organisation formed to provide collective defence against a common adversary to being an organisation that worked together

to build a system of collective security and interests. International political changes also affected the international export control regimes. As the export controls in COCOM were established for the specific purpose of containing conventional arms and dual-use goods and technology from reaching the Soviet Union, they were no longer necessary. COCOM was terminated in 1994 and replaced by the Wassenaar Arrangement (WA) in 1995. Instead of targeting specific countries for export control, WA created consensus among the participating states to establish control lists of conventional arms and dual-use goods and technology that would then be implemented in domestic export control regulations (Wassenaar Arrangement, 2019). The transition from COCOM to WA denoted a policy shift of international export control regimes that promoted regional and international security instead of being country-specific in its control list-making process.

The discussion of security concerns has expanded from traditional armed military threats to include online cyber security attacks, but the export control regimes were not constructed to easily adopt and reflect cyber security concerns. There are two reasons for this. First, the national security concern that is focal in export controls allows for governments to coordinate international and domestic export control regimes in a concentrated securities effort. In contrast, the widespread need for cyber security in both the private and public sectors makes the successful strategic planning of cyber security one that would need to be done through the coordination between the various industries. The feedback from the cyber security industry early in the policy-making process to address cyber security concerns would be more effective compared with the concentrated decision powers given to the government in the pursuit of national security considerations. Second, the regulatory construct for domestic export control regimes was established to restrict the cross-border movement of physical goods rather than the transmission of data and technology through the internet. Although domestic export control regulations have been amended to address the transmission of controlled technology through the internet, the two primary elements in the construct of domestic export control regulations have remained unchanged: 1) the control lists that decide what goods and technology are subject to export controls, and 2) the allocation of liability for regulatory compliance. Both of these elements were structured when the primary subject of export control was physical goods and as domestic export control regulations seek to incorporate cyber security into their export control, it is important to analyse and recognise why the construct of these two elements might not be the best structure to address cyber security concerns.

2. Challenges of Using Export Control Regimes to Deal with Cyber Security Challenges

Cyber security concerns pose challenges to the national security of countries, but to use the policy tools formulated under the traditional military-

oriented national security considerations might not help to address extant cyber security concerns. The formation of the strategic plans for national security concerns and cyber security concerns are fundamentally different. The former are driven by national governments and address a country's national security and tactical concerns. As export control regimes are viewed as trade measures rooted in military-oriented security considerations, the government acts as the main policymaker and enforcer of legislation that would restrict the export of military and dual-use goods and technology. The coordination of multilateral export control agreements such as WA and the implementation of these measures in domestic export control regimes reflect the government-centric approach of those regimes. The strategic planning of military-oriented national security concerns is concentrated at the governmental level and flows in a top-down manner where civil stakeholders have limited ability to respond unless invited by the government. Therefore, the formation of a national security strategic plan is different from the bottom-up strategic plan needed in cyber security strategy planning.

Although cyber security could be discussed as an extension of national security concerns, the definition of cyber security dictates that the creation of the strategic plans for it would be different from those of export controls. Craigen, Diakun-Thibault and Purse define cyber security as 'the organisation and collection of resources, processes and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights' (Craigen et al., 2014: p. 17). Another definition offered by the International Telecommunications Union (ITU) is: 'the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the availability, integrity and confidentiality of assets in the connected infrastructures pertaining to government, private organisations and citizens' (ITU, 2018: p. 13). Both definitions highlight the entities involved in dealing with cyber security strategic plans to be parties working from their respective industries in both the public and private sectors that have vested interest in being protected from cyber harm (ITU, 2018; OECD, 2012). The wide-ranging elements included in the definition of cyber security make it necessary for civil stakeholders from various industries to be involved in the strategic planning of cyber security to construct a policy that would address and reflect a wide array of issues that fall under the broad definition of cyber security concerns.

Besides the different ways that the governments and civil stakeholders interact with each other in their respective strategic planning process, another challenge for addressing cyber security concerns through the construct of export control regimes stems from the original subject matter of restriction under export control. Export control regimes were established with the focus of restricting the physical movement of goods rather than intangible technologies. Even for US Export Administration Regulations (EAR) that have incorporated knowledge-based export control measures, the determination of whether or not export licenses should be obtained

for controlled technology released to a foreign person was predicated on the exposure of controlled technology to the physical presence of a foreign person. As export control seeks to incorporate cyber security concerns into its regulatory framework, some of the primary elements of export control regimes that were not originally constructed to regulate the movement of software technology in cyberspace need to be reconsidered.

A. Interaction between Government and Civil Stakeholders

Modern export control regimes were established during the Cold War as an accompanying trade measure that reflected the security concerns of NATO regarding the looming threat from the Soviet Union to Europe and the outbreak of the Korean War in 1950. As governments implemented domestic regulations of export controls based on multilateral negotiations, the national security aspect of export control took priority over the potential economic sacrifices that civil stakeholders might have to bear. However, because the export control lists made during the COCOM era stemmed from these shared strategic concerns, the controlled goods and technology were conventional military-used or dual-use items that needed to be controlled based on their military orientation. The economic detriment that civil stakeholders encounter under export control regimes would be viewed by the government as necessary for the protection of national security.

To protect a country's national security, government agencies, especially the military, have also been a primary source of research grants in the research and development of advanced technologies (Singer, 2014). The internet itself would not have been created if not for the US Department of Defense funding the Defense Advanced Research Projects Agency (DARPA) that partnered with scientists, industry and academia to build the basic framework of the internet (Goldsmith and Wu, 2008; Singer, 2014). This creates an additional layer of proprietary control that governments might have towards the export of restricted military-use goods and technology. Even if the original funding for developing advanced technologies had been granted from government entities, the private sector finessed the use of these advanced technologies for broad commercial application and adopted them for general use. To control the export of technologies that have become commercially available even with specific national security needs, such as the export control of software that could generate cyber-attacks, would require feedback from the public and private sector as its use and proprietary nature are now shared among many stakeholders.

The traditional decision-making power in export control regimes has been centralised in the government and resulted in a top-down flow of requests for regulatory compliance for civil stakeholders. As a result, the participating states of the multilaterally negotiated international export control lists from COCOM and current international export control agreements that include WA, the Missile Technology Control Regime, the Nuclear Suppliers Group and the Australia Group would be adopted into the US and EU dual-use export control lists without seeking comments or feedback from the general

public. Divergence from this general practice happened in the US when cyber security software, specifically intrusion software and surveillance items, were added to the WA export control list after the 2013 Plenary Meeting. The different methods that the US Department of Commerce and EU responded to the WA 2013 Plenary Meeting Agreement reflected the different perspectives that governments have in incorporating cyber security considerations into export control regimes.

For the EU, the use of export controls to promote security has become inclusive of protecting human rights as a human security focus. There was an amendment made to EU's dual-use list in 2014 to include WA 2013 Plenary Meeting Agreement's control of intrusion software and Internet Protocol (IP) network communications surveillance system or equipment (European Commission, 2014). The export control of intrusion software and surveillance items was deemed to be necessary as these technologies had allegedly been used by autocratic states to monitor and arrest dissidents (Kanetake, 2019). Because the construct of export controls was based on protecting the security of the exporting country defined by the government, as the EU incorporates the value of protection of human rights as a security concern.

In an administrative move usually not seen when implementing the agreed export control list, the US Department of Commerce posted the proposed rules and sought comments for implementing the WA 2013 Plenary Meeting Agreement (BIS, 2015). There was concern from the Department that the scope of export control over intrusion software would be too broad and that public feedback would be needed to make sure that the rule would not harm the US government or cyber security industry within the private sector if it was implemented. When the then Assistant Secretary of Commerce for Export Administration Kevin J. Wolf testified before the US Congress in 2016, he acknowledged that the public response was mostly negative rules (BIS, 2016). The initial inquiries for the proposed rule reflected a different understanding of the terminology used in the control list entries by the cyber security community than by the export control agencies and the WA participating states and commenters also worried that the measures could not be implemented without causing significant harm to cyber security. As a result, even though intrusion software and surveillance technology remained on WA's export control lists, the US has yet to adopt these restrictions.

Export control regimes were constructed with a policy focus on national security that allowed governments to exert control over the subject matter of the controlled items and technology, but the way that dual-use technologies have evolved to widespread public and private sector use might make future export control rule-making something that would need more private sector input. This underlying tension is seen in the way the main elements of export controls have been structured.

B. Primary Elements of Export Control

Adding classes of cyber security technology into export control lists seems

like a natural extension of the use of export control regimes since their main policy goals are to restrict the export of technologies that would result in military and/or cyber attacks to the exporting country. However, the construct of export control regimes creates friction with some of the policy concepts of cyber security and has resulted in export control being less effective in promoting cyber security. The two primary elements that construct export control regimes have remained unchanged even with the arrival of the internet: 1) the control lists that decide what goods and technology are subject to export controls; and 2) the allocation of liability for regulatory compliance.

These aspects have served to create cohesion among the domestic export control regulations between nations, but adopting them for cyber security has showcased the inherent weakness. The foundational construct of export controls is the use of bans and restrictions, but this construct is not found in the methodology for constructing cyber security strategies in most countries. Cyber security strategies require the involvement of civil stakeholders. The fundamental construct of cyber security is the co-operation between stakeholders in formulating measures to diminish cyber security risks and fend off attacks (Public Safety Canada, 2019; US Department of Homeland Security, 2018; US Department of Commerce, 2017; Klimburg, 2012). The use of export controls requires policymakers and stakeholders to narrow the focus to debating what types of information technology and what specific software and technologies should be restricted or banned for export instead of taking an overview of cyber security strategies from a cooperative approach between government and stakeholders. This creates a concentrated focus on determining what information technology should or should not be subject to export controls while being mindful of the liability that might be imposed on parties that violated export control regulations. The following sections will break down the two foundational elements in export control regulations to address the two issues: why identifying technology to add to control lists might not be effective for cyber security tactics, and why the methods used to allocate export control liability are not helpful in addressing cyber security concerns.

1) Control Lists

After World War II, international export control regimes such as COCOM and WA facilitated multilateral negotiations among participating states so that the states could adopt similar control lists and create unity in controlling the movement of goods and technologies. The lists provided a framework for the construction of domestic export control regimes. Even though countries have the ultimate decision-making power of incorporating the control lists into their domestic export control regimes, most adopted the control lists from the international regimes thus forming a cohesive international approach.

Adding technology as an intangible subject of control into control lists thus far made up only of physical goods was much debated in the early 1980s. Many COCOM member countries opposed such an addition, as it would be difficult

to enforce export controls over the intangible forms of data and technology (McDaniel, 1993). The difficulty of enforcement lies not only in the intangible nature of data and technology, but also in determining whether or not it belongs to a category on the control lists. A cargo box sitting in a port might contain export-controlled items that require an export license, but whatever physical item is in the cargo can be categorically determined. A review of the questions submitted for the United States Department of Commerce, Bureau of Industry and Security (BIS)'s proposed rule for WA plenary agreements highlights the technological complexity and actions that are taken to create a cyber security ecosystem. Policymakers need to identify specific technologies, systems or tools that are part of that ecosystem and label them as subject to export control when they bring cyber security into the construct of an export control regime. Within the vast scope of software and technologies that build the cyber security ecosystem, trying to separate particular technologies and systems for export control does ignore the interwoven connections of a cyber security strategy framework. Therefore, while it is possible to address cyber security concerns through adding specific software or technology to export control lists, the purpose of control lists and the general construct of a cyber security ecosystem would not make the use of export control lists the best method of addressing cyber security concerns.

2) Export Liability

The construct of domestic export control regimes is determined by the establishment of control lists and the allocation of export control liability. Historically speaking, the establishment of control lists was organised through multilateral efforts under international export control regimes and the allocation of liability determined through domestic regulation. Allocating export liability identifies the party responsible for ensuring that all export activities are conducted in compliance with domestic export control regulations. While there are differences between each country's regulations, two definitions are generally found that help construct the liability framework: the exporter who is liable for export control compliance and the export activity that triggers that control.

Export liability is generally allocated to exporters because they have the control and decision-making power to send items or transmit technology abroad. In some jurisdictions, exporter's liability is imposed because there is a presumption that they will receive financial gain from the export activity. In the case of US, EAR Part 772 defined exporter as '[t]he person in the United States who has the authority of a principal party in interest to determine and control the sending of items out of the United States' (Bureau of Industry and Security, 2020: p. 16). EAR Part 772 also describes the principle parties to be 'persons in a transaction that receive the primary benefit, monetary or otherwise, of the transaction. Generally, the principals in a transaction are the seller and the buyer' (ibid.) This is similar to the definition in EU Council Regulation (EC) No. 428/2009 Article 2 where an exporter is a person who:

> ‘holds the contract with the consignee in the third country and has the power for determining the sending of the item out of the customs territory of the Community ... [However] [i]f no export contract has been concluded or if the holder of the contract does not act on its own behalf, the exporter shall mean the person who has the power for determining the sending of the item out of the customs territory of the Community... [or] transmit or make available software or technology by electronic media including by fax, telephone, electronic mail or by any other electronic means to a destination outside the Community’ (European Council, 2009: p. 2).

The subtle difference in the definition of exporters could affect the allocation of export liability for actors in cyberspace, especially as it relates to the liability of platform services. For example, in an Advisory Opinion issued in 2009, BIS determined that online cloud computing storage services would not be considered to be an export under EAR because they are not considered to be a party of interest. The party of interest was the user of the service (BIS, 2009). The same issue of using online cloud computing services might result in a different interpretation under EU Council Regulation (EC) No. 428/2009 since the definition of an exporter is not tied to the entity receiving economic benefit for their actions. The exporter is the person that sends items outside of the export control jurisdiction and is responsible for export control violations, but identifying the exporter in cyberspace might not be as straightforward as it is with identifying the exporter that ship goods in the physical world.

For the exporter to be held liable, an export activity must happen to trigger export liability or a broader export liability could also be imposed on exporters that fail to secure the protected items. The general definition of export is when goods or technologies are sent or transmitted across borders and so the transmission of data and software through cyberspace is subject to export control if it is clear that it has crossed a border. However, in some countries like the US, an export activity is not restricted to the traditional cross-border movement of goods and technology. Allowing a foreign person to gain knowledge of export-controlled technology inside the US is also prohibited as an act of ‘deemed export’ which under the US EAR is defined as the release or transfer of technology to a foreign person inside the US. The concept of export activities under this definition is therefore focused on the exposure of knowledge rather than the movement of allowance of goods and technology between sovereign jurisdictions.

The liability framework was originally constructed with the idea that the person who was responsible for sending the goods intends that they cross a border. However, with the advent of the internet, the relationship between the parties involved with the transmission of technology and data might not fit the traditional definitions of exporter and export activities. Consideration

should be given to whether the framework established to regulate the movement of goods should automatically be adopted to address new national security concerns such as cyber security. Internet service providers (ISPs) and online storage companies act as agents for transmitting or storing data on the internet, but they have been mostly excluded from export control liabilities. This is because ISP users, not ISPs, are considered to be exporters as they are the 'principle party in interest' under US EAR and the entity receiving economic benefit under EU Council Regulation (EC) No. 428/2009. As ISPs are parties that could contribute most to cyber security planning, the exclusion given to ISPs might not be the best construct to protect against cyber security threats.

3. Refocusing Export Control Regimes to Address Cyber Security Concerns

As technology has advanced, export control regimes must evolve to reflect the new reality of the transfer of data rather than physical goods. Changes thus far have not shifted the foundational construct of using control lists to allocate export liability to the exporter of controlled items or technology. This creates tension between government and civil stakeholders and makes it difficult to achieve cyber security policy protection through the construct of export controls. Change is needed to decrease the friction between civil stakeholders and government entities when incorporating cyber security concerns into export controls. Like-minded NATO countries should work together to build a public-private partnership based on voluntary cooperation between government agencies and civil stakeholders in order to address cyber security concerns.

A proposed change is needed to find a way to address these issues which should see the involvement of civil stakeholders in the construct of these lists. Current export control lists identify goods and technology that could endanger national security. A control list acts as a prohibitive measure that details the goods and technologies that should not be exported, so instead of focusing the control lists on software or technology that would be harmful to national security, another type of list could also be established specifically to provide for information security, network security and operational security as they relate to the software and tools that would be helpful in building a cohesive cyber security framework among participating states. It is important in the construction of this new list that input from cyber security industry and experts be incorporated from the start and instead of creating liability for the technologies listed in cyber security items, an exemption would be given to the cross-border movement of items on this list among member states that are building a common cyber security framework. The goal is to build more cooperation between civil stakeholders and various national governments to maximise efforts to promote cyber security between different states.

4. CONCLUSION

NATO was created as a political and military alliance between European states and North American countries to provide for a collective defence alliance based on shared security concerns rooted in the common value of protecting the freedom, democracy, liberty and rule of law of member countries. It is through these shared security concerns that modern export control regimes have been established. While the use of export control regimes to resolve cyber security threats could be discussed as an extension of national security considerations, the formation of strategic plans for national security concerns and cyber security concerns is fundamentally different. There is a need to reconsider how cyber security issues could be incorporated into the export control regime framework through a list-building process that could promote closer working relationships between member states that share similar security concerns.

5. REFERENCES

Bitzinger, R.A. (1989) *Assessing the Conventional Balance in Europe*, 1945-1975, Santa Monica, the RAND Corporation.

Bromley, M., Cooper, N. & Holtom, P. (2012) The UN Arms Trade Treaty: Arms Export Controls, the Human Security Agenda and the Lessons of History. *International Affairs*. 88 (5), 1029-1048.

Bureau of Industry and Security. (2009) *Application of EAR to Grid and Cloud Computing Services*. Available from: https://www.bis.doc.gov/index.php/documents/advisory-opinions/527-application-of-ear-to-grid-and-cloud-computing-services [Accessed 14th August 2020].

Bureau of Industry and Security. (2015) Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items, *Federal Register* 80, 28853-28863. Available from: https://www.federalregister.gov/documents/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items [Accessed 14th August 2020].

Bureau of Industry and Security. (2016) *Testimony by Assistant Secretary of Commerce for Export Administration Kevin J. Wolf Before the House Committee on Oversight and Government Reform, Subcommittee on Information Technology and the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies on 'Wassenaar: Cybersecurity and Export Control'.* Available from: https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/1393-doc-testimony-for-asst-sec-kevin-wolf-1-12-16/file [Accessed 19th September 2020].

Bureau of Industry and Security. (2018) Review of Controls for Certain Emerging Technologies, *Federal Register* 83, 58201- 58202. Available from: https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies [Accessed 14th August 2020].

Bureau of Industry and Security. (2020) Export Administration Regulations Part 772: Definition of Terms. Available from: https://www.bis.doc.gov/index.php/documents/regulations-docs/2344-part-772-definitions-of-terms-2/file

[Accessed 21th November 2020].

Craigen, D., Diakun-Thibault, N. & Purse, R. (2014) Defining Cybersecurity. *Technology Innovation Management Review.* 4 (10), 13-21. Available from: doi:10.22215/timreview/835.

European Council. (2009). *Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items*. Available from: https://eur-lex.europa.eu/eli/reg/2009/428/oj [Accessed 25th November].

Goldsmith, J. & Wu, T. (2008) *Who Controls the Internet?: Illusions of a Borderless World*. New York, Oxford University Press.

International Telecommunications Union. (2018) *Guide to Developing a National Cybersecurity Strategy*. Available from: https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018 [Accessed 14th August 2020].

Kanetake, M. (2019) The EU's dual-use export control and human rights risks: the case of cyber surveillance technology, *Europe and the World: A law review*. 3 (1). Available from: doi:10.14324/111.444.ewlj.2019.14.

Klimburg, A. (Ed.) (2012) *National Cyber Security Framework Manual*, NATO. Available from: https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/ [Accessed 14th August 2020].

McDaniel, D.E. (1993) *United States Technology Export Control*. Westport, Praeger Publisher.

NATO. (1951) *Item MC 0031-Final-Readiness and Effectiveness of NATO Forces*. Available from: https://archives.nato.int/readiness-and-effectiveness-of-nato-forces-2 [Accessed 19th September 2020].

NATO. (1951) *Item MC 0033-Final-Estimate of the Relative Strength and Capabilities of NATO and Soviet Bloc Forces at Present and in the Immediate Future.* Available from: https://archives.nato.int/estimate-of-relative-strength-and-capabilities-of-nato-and-soviet-bloc-forces-at-present-and-in-immediate-future [Accessed 19th September 2020].

National Institute of Standards and Technology. (NIST) (2018) *Framework for Improving Critical Infrastructure Cybersecurity.* Available from: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11 [Accessed 14th August 2020].

Office of Technology Assessment. (1979) *Technology and East-West Trade.* Washington, D.C., Office of Technology Assessment Publications.

Organisation for Economic Co-operation and Development (OECD). (2012) *Cyber Security Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the Internet economy.* Available from: https://www.oecd.org/sti/ieconomy/comparativeanalysisofnationalcybersecuritystrategies.htm [Accessed 14th August 2020].

Public Safety Canada. (2019) *National Cyber Security Action Plan 2019-2024*. Available from: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx [Accessed 14th August 2020].

Public Safety Canada. (2018) *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*. Available from: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx [Accessed 14th August 2020].

Ruohonen, J. & Kimppa, K.K. (2019) Updating the Wassenaar Debate Once Again: Surveillance, Intrusion Software and Ambiguity. *Journal of Information*

Technology & Politics. 16 (2), 169-186.

Singer, P. (2014) *Federally Supported Innovations: 22 Examples of Major Technology Advances That Stem from Federal Research Support*. Washington, D.C., The Information Technology & Innovation Foundation.

US Department of Commerce. (2017) *International Cybersecurity Priorities: Fostering Cybersecurity Innovation Globally*. Available from: https://www.commerce.gov/news/reports/2018/06/international-cybersecurity-priorities-fostering-cybersecurity-innovation [Accessed 14th August 2020].

US Department of Homeland Security. (2018) *Cybersecurity Strategy*. Available from: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf [Accessed 14th August 2020].

Wassenaar Arrangement. (2014) *The Wassenaar Arrangement on Export Control for Conventional Arms and Dual-Use Goods and Technology: List of Dual-Use Goods and Technology and Munitions List.* Available from: https://www.wassenaar.org/app/uploads/2019/consolidated/WA-LIST-14-2.pdf [Accessed 14th August 2020].

Wassenaar Arrangement, Public Documents. (2019) *Vol. IV – Background Documents and Plenary-related and Other Statements.* Available from: https://www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-PUB-006-Public-Docs-Vol-IV-Background-Docs-and-Plenary-related-and-other-Statements-Dec.-2019.pdf [Accessed 14th August 2020].