Arms Control and Its Applicability to Cyberspace

10

Thomas Reinhold and Christian Reuter

Abstract

Arms control aims at preventing conflicts and fostering stability in inter-state relations by either reducing the probability of usage of a specific weapon or regulating its use and thus, reducing the costs of armament. Several approaches to arms control exist, limiting or reducing numbers of weapons and armed forces, disarmament ("down to zero") or prohibiting certain weapons. To illustrate these further, this chapter elaborates on the necessity of arms control and presents some historical examples, including an overview of existing measures of arms control. Extrapolating from these, the general architecture of arms control regimes and the complex issue of establishing and verifying compliance with agreements will be discussed, not least with respect to cyberspace. Building on these theoretical considerations, the chapter presents important treaties and first approaches, including the *Wassenaar Arrangement*, the recommendations of the OSCE, and the UN GGE 2015.

T. Reinhold (✉) · C. Reuter
Science and Technology for Peace and Security (PEASEC),
Technische Universität Darmstadt, Darmstadt, Germany
e-mail: reinhold@peasec.de

C. Reuter
e-mail: reuter@peasec.tu-darmstadt.de

C. Reuter (ed.), *Information Technology for Peace and Security*,
Technology, Peace and Security I Technologie, Frieden und Sicherheit,
https://doi.org/10.1007/978-3-658-44810-3_10

Objectives

- Understand the historical background of arms control and its development of the last decades for different military systems, applications or technologies.
- Learn about the diverse approaches of arms control and the stepwise progress of arms control treaties according to the political situation, the affected stakeholders and the intended goals.
- Understand the challenges of establishing arms control measures in cyberspace.
- Learn about the different proposals of states, private companies and non-governmental actors that can prepare the way towards binding international treaties for the cyberspace.

10.1 What is Arms Control and Why is It Necessary?

The concept of arms control has been developed as a political reaction to the dynamics of military armaments in the international state system (see Chapter 3 "*Natural Science/Technical Peace Research*" and Chapter 17 "*Unmanned Systems: The Robotic Revolution as a Challenge for Arms Control*"). At its core, **arms control** is a normative endeavour. It was born out of the recognition that war must be prevented, and the principle of preventing future wars guides it.

The concept can be described as

> unilateral measures, bilateral and multilateral agreements as well as informal regimes (…) between States to limit or reduce certain categories of weapons or military operations in order to achieve stable military balances and thus diminish tensions and the possibility of large-scale armed conflict. (Den Dekker, 2004)

Thus, arms control does not necessarily imply steering armed forces towards complete disarmament. Early attempts of arms control can be recorded in the pre-twentieth century, often accompanying more significant conflicts or new military technologies like the development of firearms and large-calibre guns. These early approaches, like the Hague Conventions of 1899 and 1907 and their annexes,[1] often included the non-usage of certain weapons, such as chemical weaponry. This dynamic increased with the advancements of military weapons during the First and Second World Wars as well as with the subsequent arms races of the Cold War. Especially the development of nuclear weapons,

[1] Both *Hague Conventions* from 1899 and 1907 consist of multiple treaties and additional annexes. Most relevant for the challenges of arms control is the second treaty of the first conference "Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 29 July 1899" (Hague Conference, 1899) as well as the fourth treaty of the second Hague convention (Hague Conference, 1907).

their massive destructive potential and the high risk of global annihilation underlined the necessity of political regulation.

Arms control usually takes the form of bilateral or multilateral legally binding treaties to regulate some aspects of military potential and capabilities. Still, it is also concerned with the conditions and circumstances that lead to armed conflicts. The overall goal of arms control is less a complete disarmament, which strictly speaking would mean the renunciation of all military capabilities but rather a rational planning for reducing the risk of war. This task can be divided into three different parts (Müller & Schörnig, 2006):

1. War prevention and the reduction of conflict probability, limiting the acceleration of armament dynamics and its causes, as well as reducing the likelihood of preventive or pre-emptive strikes.
2. Damage limitation in the event of armed conflicts, restricting the extent of death and destruction caused by certain weapon systems with massive destructive potential or weapons that can be used on a large scale.
3. Reduction of armament-related costs and the release of such funds.

Against the background of these overall tasks, arms control approaches generally consider the following different principles and measures specified in individual and usually legally binding treaties for specific weapons, weapon parts, weaponisable technologies, and armed forces:

- Create transparency about military capabilities, establish and maintain sustainable stability and communication in inter-state relations, so-called Confidence and Security Building Measures (Chapter 9 "*Confidence and Security Building Measures for Cyber Forces*").
- Provide quantitative and qualitative limits of permitted weapons or their specific capabilities, for instance, the payload or the range of missiles.
- Restrict or prohibit the proliferation of weapons, weapon parts or weapon technology, establish measures to control restrictions or limitations and provide information for other states about arms sales.
- Develop and establish specific measures of verification that enable states to practically verify the compliance of other treaty parties with agreements.

These approaches are not necessarily consistent or compatible. The particular focus in a concrete situation and the corresponding means always depend on the configuration and level of political, economic or (expected) military conflict. This is also important given the realistic assessment of possibilities and expected results of arms control in specific situations and its limitations. Therefore, arms control cannot be equated with **disarmament**. This may be the case, for example, when limits are set for weapons systems that are above the current stock levels of two treaty parties. The controlled armament build-up to the new limits could allow a balance of military power and reduce concerns of a later and possibly covert armament. In general, arms control stretches from measures

Fig. 10.1 Sculpture "Non-violence" showing a revolver tied in a knot, on display outside the Headquarters of the United Nations in New York City by the sculptor Carl Fredrik Reuterswärd. (Picture: C. Reuter)

with minimal requirements for commitment to establish first steps towards positive state relations to reduction measures with practical controls and monitoring of weapon sites or other relevant facilities. Figure 10.1 shows the "Non-Violence" sculpture in front of the UN headquarter – a classical tribute to non-violence and peace.

10.2 Historical Examples of Arms Control

The following examples aim to illustrate that over the last decades, each emerging military technology has raised new challenges for arms control, led to international debates and – often after its military deployment – to agreements and treaties.[2]

10.2.1 Arms Control for Nuclear Weapons Technology

Due to their major threat to humankind and the historical arms race during the Cold War era, the regulation of nuclear weapons and their carriers has a long history with many,

[2] For an insightful overview of arms control endeavours see Goldblat (2002).

sometimes unsuccessful, approaches to mutual agreements and treaties. The following examples also illustrate a specific aspect of arms control treaties. In most cases, the agreements have a specific technological or military-strategic scope and a limited period of validity. Often, they are intended to be reviewed and possibly renewed after some time or followed by subsequent treaties. Because of these expiry dates or the unilateral withdrawal of treaty signatories, some of the agreements were terminated without follow-up approaches. The list further exemplifies that arms control regulation is often a step-by-step process, starting with minimum consensus regulations and proceeding towards stricter prohibitions. This development can be seen in the first arms control agreement for nuclear weapons and weapons technology, the so-called *Partial Nuclear Test Ban Treaty* (PTBT),[3] which entered into force in 1963 (PTBT, 1963).

The treaty was initially signed by the Soviet Union, the United Kingdom, and the United States and then opened for signature by other countries. The still effective agreement prohibits all test detonations of nuclear weapons other than those conducted underground. It can be perceived as a first measure to slow down the nuclear arms race and its proliferation by limiting scientific testing capabilities. A few years later, in 1970, the *Non-Proliferation Treaty* (NPT)[4] came into force, taking arms control of nuclear weapons an important step further (NPT, 1970). The treaty is based on three pillars.

1. First, it defines a list of nuclear-weapon states that have manufactured and detonated a nuclear weapon or other nuclear explosive devices before 1. January 1967 and declares that all non-nuclear weapon states agree never to acquire nuclear weapons.
2. Its second pillar is the agreement of all treaty parties to pursue nuclear disarmament in order to ultimately eliminate nuclear arsenals (Graham, 2004).
3. Its third pillar is the right of all parties to develop nuclear energy for peaceful purposes and to benefit from international cooperation in this area.

The NPT originally had a limited duration of 25 years but was extended indefinitely in May 1995. It is now reviewed every five years in the Review Conferences of the Parties. An essential aspect of the NPT is that it authorises the International Atomic Energy Agency (IAEA) to monitor the states' compliance with NPT agreements and commits them to security measures, the so-called nuclear safeguards.

Another issue of arms control is highlighted by the 1988 Intermediate-Range Nuclear Forces Treaty[5] between the United States and the Soviet Union (INF, 1988). The treaty

[3] The full name of the treaty is *Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water*, but it is also known as *Limited Test Ban Treaty* (LTBT).

[4] The full name of the treaty is *Treaty on the Non-Proliferation of Nuclear Weapons*.

[5] The full name of the treaty is *Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Elimination of Their Intermediate-Range and Shorter-Range Missiles*.

did not focus on the nuclear explosive device itself but on its deployment tools, the missiles and the necessary launchers. It codified the elimination of all nuclear and conventional missiles and their launchers with specific ranges and ordered a deadline for their destruction. In addition, verification measures such as on-site inspections were established to check compliance with the treaty by both sides. Besides the obvious positive effect of reducing the military escalation potential of nuclear weapons, peace and security researchers value the agreed verification measures because they established specific, practical and measurable steps[6] for checking compliance while respecting and sustaining national security agendas. After many years of criticism against Russia for undermining the agreements as well as arguing that the treaty is ineffective without China, both countries withdrew from the INF treaty in 2019. A similar fate threatens the so-called New START treaty that was signed in 2010 and entered into force in 2011 (New START, 2010). START is the abbreviation for *Strategic Arms Reduction Treaty* and is used to describe three different, consecutive treaties between the Soviet Union (later Russia) and the United States on the reduction of nuclear bombers, intercontinental and submarine-launched ballistic missiles and warheads in combination with the establishment of verification measures. Although the New START treaty is formally still active, Russia suspended its participation in 2023, followed shortly after by a US revocation of the Russian nuclear inspectors' visas. This led to a standstill of any verification measures.

10.2.2 Arms Control for Biological and Chemical Weapons Technology

As mentioned, arms control treaties were also negotiated for many other technologies. Two other important weapons of mass destruction are chemical or biological weapons. Facing the challenges and risks associated with them, the member states of the United Nations adopted the *Biological and Toxin Weapons Convention* (BWC)[7] that entered into force in 1975. It prohibits the development, production, stockpiling, and distribution of biological weapons combined with a strong emphasis on restricting the application of biological and toxic material to civil purposes (BWC, 1972).[8] Since its implementation, review conferences have been held every five years. However, in the absence of specific compliance or verification stipulations in the treaty, effective compliance monitoring has

[6] Verification measures include extensive data exchange, on-site inspections at deployment sites, permanent inspections at the missile production facilities (Woof 2011).

[7] The full name of the treaty is *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction*.

[8] The military usage of chemical weapons had already been banned by the *Geneva Protocol* in 1925. The BWC reaffirms this ban and supplements the Protocol.

proved insufficient. Attempts to solve this problem by means of an additional protocol, including disclosure requirements and inspections, failed in 2001.

As for the challenge of chemical weapons, the *Chemical Weapons Convention* (CWC),[9] signed in 1993 and entered into force in 1997, provides a series of comprehensive and practical disarmament steps (CWC, 1997). The signatory states undertake to declare existing stocks and to destroy all chemical weapons under international supervision by 2012.[10] In addition to toxic chemicals, the CWC also applies to munitions or equipment specifically designed to cause death or other harm by exploiting the toxic properties of the listed chemicals. The CWC also included establishing and authorising the Organisation for the Prohibition of Chemical Weapons (OPCW), based in The Hague, which is responsible for monitoring compliance with the Convention. A so-called "verification annex" to the Convention sets out contractual obligations (i.e. a detailed description of procedures to be followed by the treaty parties) and verification measures (i.e. how inspections are to be conducted and how samples are to be collected, handled and analysed).

10.2.3 Arms Control Treaties for Conventional Weapons and the Outer Space

Other examples of the diverse field of arms control approaches are:

- The *Outer Space Treaty* 1967. It aims to prevent the occupation of celestial bodies by individual states (at that time the Soviet Union and the USA) and the temporary or permanent deployment of military forces in space, on the moon or other celestial bodies, especially weapons of mass destruction (UN, 1967). However, given the spirit of technological advancement, civil space exploration is explicitly allowed for each state.
- Regarding arms control for conventional forces and weapons, the 1990 *Treaty on Conventional Armed Forces in Europe* (CFE) sets upper limits for the number of heavy weapons systems that may be deployed in Europe (CFE, 1990). After its implementation, the treaty led to drastic reductions in stocks of weapons for offensive purposes in Europe as a stable balance of military powers between the Cold War parties was established. In view of increasing global political tension, Russia withdrew from the treaty in 2023, whereupon NATO decided to suspend its participation in the treaty.
- The *Convention on Cluster Munitions* (CCM, 2008) is a ban on the use, manufacture and transfer of certain types of conventional cluster munitions. It refers to bombs,

[9] The full name of the treaty is *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction*.

[10] This deadline had to be prolonged. During the summer of 2023, the OPCW reported the total elimination of the declared stockpiles (OPWC, 2023).

grenades or warheads that do not explode as a whole but release a variety of smaller explosive devices. In addition to the prohibition provisions, the agreement includes provisions on the destruction of existing stocks, the disposal of residues from cluster munitions and the support of victims of cluster bombs. The convention was signed in December 2008.

10.3 Arms Control Measures

The following section will explain measures for arms control, starting with the concepts of confidence building and verification, as well as preventive arms control as core elements. Following up on these, the broad range of arms control measures that have been developed over the last decades for different types of military weapons and their technologies will be presented.

10.3.1 Confidence Building and Verification as Important Parts of Arms Control Measures

The historical examples showed that arms control efforts are almost always a gradual process; their success is often temporary and depends on the political circumstances and responsible actors. In many cases, the initial situation is characterised by two or more state parties with a certain degree of mistrust or uncertainties about the current or planned military power and security policies of "the other sides". Sometimes combined with ideological differences, these situations have often been marked by little official communication. Each party depends on the "outside perception" of other parties and the interpretation of their actions without having complete knowledge about their intentions and motivations. These constellations can be described by the sociological system theory of Parsons and Luhmann and their concept of "double contingency" (Luhmann, 2021). Applied to the context of international security politics, this means that state parties are under the impression of existing or perceived threats of other state actors that will or may interfere with their national security, sovereignty, or foreign policy goals. Such threats can be aggressive territorial behaviour but also military armament, which is perceived as overpowering either in terms of sheer capacities of military power (e.g. conventional forces like tanks, infantry, military airplanes) or by the destructive military potential of specific weapons technology. Such tense situations are often exacerbated by new technologies and the inadequate or lacking understanding of their invasive or destructive capacities.

The current debates on cyber weapons illustrate this situation: It is yet unclear what **cyber weapons** are and if cyber-related offensive military acts fit the conventional term of use of "weapons". As Sommer and Brown point out, "there is an important distinction between something that causes unpleasant or even deadly effects and a weapon" (Som-

mer & Brown, 2010). The authors propose a comparison with kinetic weapons, which they define as follows:

> A [kinetic] weapon is 'directed force' – its release can be controlled, there is a reasonable forecast of the effects it will have, and it will not damage the user, his friends or innocent third parties.

Another approach for the definition of cyber weapons proposes an assessment of the strategic selection of the target, the purpose and the intended damage of specific cyber incidents and the attackers behind them. However, these approaches have the problem that they can be assessed after the use of a specific malware but not before its application. This means that they fail for the preventive approach of arms control. An effective approach is proposed by Reinhold & Reuter that assesses the technical measurable parameters of software (2021). Despite this rather terminological debate, several interruptive and sometimes damaging incidents in cyberspace have occurred and demonstrated the existence of such malicious cyber tools. International studies emphasise the increasing demand for military forces for cyber-related capacities (UNIDIR, 2013).

On the other hand, it is unclear how to measure, compare, and categorise such cyber tools and their potential military destructive effects. As a result, especially in political debates, each state expects the most dystopian scenarios and tries to prepare for them, either with cyber defence measures or sometimes by setting up its own offensive cyber capacities. The most visible parts of these concerns are the ongoing debates about a**ctive cyber defence** (in Germany known as the Hack-Back debates) or the perpetual fear that military cyber attacks could shut down critical infrastructures. In the face of these challenges, relations of mistrust, armament and the risk of conflicts by accident or misconception, the international political community has developed the concept of **confidence building measures (CBMs)**[11] (see Chapter 9 "*Confidence and Security Building Measures for Cyber Forces*").

These measures, initially introduced by the Conference on Security and Co-operation in Europe (CSCE) during the Cold War era, intend to establish cooperation between states through gradual and mutual concessions, exchanging information and reducing military threats (CSCE, 1986). The proposed actions further intend to establish active communication channels between opposing parties, facilitating communication in times of crisis before "pushing the buttons". The exchange of information and talks about national security doctrines or strategies and the underlying motivations aim at fostering an understanding of the security goals and fears of the "other side". At best, they could help the parties reach the common knowledge that weapons should be seen as "military insurance" and not be used. Such a situation emerged, for example, during the Cold War,

[11] In debates addressing military forces, the term is often extended to confidence and security building measures (CSBM).

where the capacities of nuclear weapons either reached a level that ensured a balance of power between the opposing states or provided the military tactical possibility for an immediate strike back.[12] Over the last decades, and especially during the Cold War, some trust-building approaches explicitly focused on technical-level talks about securing weapons and their facilities. Protecting one's own population from unwanted and destructive effects of weapon technologies by accidents can be seen as the least common denominator of all states.

These approaches sometimes helped circumvent the ideological differences that would otherwise overshadow or even prevent these knowledge exchanges. Such talks and conferences, specifically the establishment of mutual understanding, often became the starting point for further debates about reducing or stopping arms races. Moreover, they promoted agreements that kept a balanced level of specific weapons that sufficed for all sides in terms of their national security considerations without further armament. The fact that many of the examples mentioned above of weapons technology also contain potential risks for civil society and risks of technical accidents helped to drive debates further towards the reduction of military capacities or the abolishment of specific weapon technologies.

As mentioned, the general goal of any arms control agreement or treaty is reducing the likelihood of war by reducing military technology weapons, their development, testing, or military application. To restrict or regulate these aspects, treaties define rules for forbidden activities, thresholds for the numbers, or instructions for the handling of specific items. The stability of arms control treaties depends on the widespread acceptance and support of these rules as well as on the existence of trustworthy and effective compliance procedures (Müller & Schörnig, 2006). This underlines the importance of possibilities for treaty parties to check compliance with the agreements of other parties, especially when the mutual relationship is characterised by mistrust. This vital part of arms control treaties can be implemented in different ways, and the agreed measures are specific to the regulated technological issues and the political goals of the negotiating parties. These so-called verification measures range from methods that allow supervision without on-site assessment like aerial imaging or seismic sensors to the structured collection, submission and exchange of data between states on stockpiles and trade volumes and on-site inspections with counting and measuring stockpiles and facilities. Müller & Schörnig (2006) define four important characteristics for the states' acceptance of these measures:

- Appropriate and focused on the given context and the intended regulation of the selected items.
- Practicable and able to detect violations.

[12] The military concept of a strike back followed the deterrence idea of preventing the threat of a nuclear attack by a country's assured ability to respond with an own nuclear attack. Such a "second strike" should have destroyed the attacker too and by that minimised its intent for the first strike.

- Adequate and suitable to assess violations and their military dimension.
- Effective to recognise violations without being hindered by technical obstacles or political intentions.

10.3.2 Preventive Arms Control

One concept of arms control useful in assessing uncertain scenarios, such as the militarisation of cyberspace and its many technical difficulties, is the so-called **preventive arms control**. It complements traditional arms control by focusing on technologies that are still in the research and development stages today. Preventive arms control attempts to regulate, limit or minimise technological innovations that could negatively affect international security and peace to prevent such consequences as early as possible. The assessment of preventive arms control follows three main objectives (Mölling & Neuneck, 2001):

- Risk prevention for sustainable development and the evaluation of the consequences and potential dangers of the technology for the human, environmental, social and political systems and infrastructure complexes.
- The further development of effective arms control, disarmament and international law to place new technologies under existing arms control and disarmament contracts or existing international treaties as well as the development of new standards.
- The reduction or limitation of the extent to which technologies have destabilising and negative effects on international security, either as a result of qualitative armament or in terms of the proliferation of armament-related knowledge.

10.3.3 An Overview on Existing Measures of Arms Control

An important step towards arms control measures regarding the militarisation of cyberspace is to look at the history of similar measures of former technological developments and their military application. The specific requirements, technical constraints, and goals of these approaches, as well as the lessons learned from their success or failure, are valuable resources for their application to cyberspace. The following Table 10.1 depicts a categorised list of arms control measures (Mölling & Neuneck, 2001; Stohl & Grillot, 2012):

10.4 The Challenges of Arms Control Measures in Cyberspace

Cyberspace as a domain has some very specific characteristics that differ from other domains like land, air and sea. This includes the virtuality of this field and the information it contains, the non-physical representation of code and the seamless duplication of data. These features pose many challenges, especially for the practical side of arms

Table 10.1 Forms of arms control

Forms of Arms Control	Explanations and Examples
Geographical measure	Demilitarised regions, security zones, e.g. nuclear weapon-free zone Africa
Structural measures	Defensive orientation of force structures, e.g. the *Treaty on Conventional Armed Forces in Europe* (CFE, 1990)
Operational measures	Limitation of manoeuvres, omission of provocative actions e.g. the Vienna Document (OSCE, 2011)
Verification measures	Data exchange, inspections, etc., e.g. the *Open Skies Treaty* (US Department of State, 1992) or the IAEA Nuclear Safeguards in Iran (IAEA, 2015)
Declaratory measures	Waiver of the first use of weapons, especially nuclear weapons
Technology-/Medium-related measures	Limitation, reduction or destruction of certain weapons or technologies, e.g. ABM Treaty (ABM, 1972), INF Treaty (INF, 1988), individual marking of weapons to make the flow and illegal discharge of weapons comprehensible, e.g. *Arms Trade Treaty* (UN, 2013)
Proliferation-related measures	Prohibition or restriction on the export of militarily relevant technologies, e.g. Nuclear Suppliers Group under the NPT (1970), securing the storage and production facilities of weapons to prevent illegal diffusion
Application-related measures	Prohibition or restriction of the use of certain weapons and methods of war
Actor-related measures	Prohibition, restrictions or permissions in relation to specific groups of actors
Target-related measures	Safeguard clauses, prohibition of the attack on certain, especially civil, targets, e.g. the treaties of the *Geneva Convention* (ICRC, 1949)
Economic/Trade-related measures	Registration and licensing of arms dealers, producers, shippers as well as the regulation and approval of individual arms transfers and provision of sanctions and intervention options, licensing arrangements for import, export, transit through national territories of weapons
Interstate cooperation measures	Inter-agency coordination, cooperation, coordination between relevant governmental organisations involved in arms control and, if necessary, cooperation in law enforcement with appropriate powers of the commissioned institutions
Information exchange measures	Transparency of production, ownership, trading and control efforts and dissemination of information to international partners

control agreements; many of the established approaches will not work. In particular, this concerns all measures that rely on one of the following aspects:

- The limitation or the reduction of cyber weapons.
- The differentiation between civil and military usage and the resulting differences in authorisation.

- The differentiation between a defensive and an offensive usage of cyber tools.
- The assignment of responsibility for individual activities in this domain.
- The necessity to practically control or monitor compliance with agreements.

Chapter 11 "*Verification in Cyberspace*" will have a detailed look at the specific technical aspects of cyberspace that cause these challenges and explain how cyberspace differs from real physical domains. The chapter will further explain how to deal with these problems and what aspects and measurable parameters could be used to implement verification measures for this space.

The previous examples of arms control approaches have shown that many of the approaches are based on states' declarations of the intended use or non-use as well as the trade or exchange of information on restricted items. Nevertheless, the ongoing international political debates struggle to find a way to reach binding agreements in the cyber area. Besides the technical difficulties and the specifics of cyberspace that prevent a direct application of most established measures to cyberspace, further problems are based on the different views of states about what constitutes cyberspace and the question of state sovereignty in this area. Whereas proposals from European states or the US usually focus on the IT infrastructure and acknowledge human rights and the freedom of speech, other approaches, such as a proposal to the UN by Russia, China and other states (UN, 2011), emphasise the national right to monitor and regulate the distribution of information in this space. This potentially includes censorship. The conceptual disagreement is further complicated by the problem of transferring the idea of national borders to this area; determining a state's sovereign territory and its responsibility is complex.

Another aspect exacerbating these disagreements is the question of which international committee or institution can be entrusted with monitoring and controlling the further technological development of cyberspace, supporting its long-term peaceful orientation. This task was historically taken by different organisations like the Internet Corporation for Assigned Teams and Numbers (ICANN) and the **Internet Engineering Task Force** (IETF)), which did not represent the international state community and may have been influenced by individual state actors. So far, approaches to transferring these tasks to a UN institution such as the International Telecommunication Union (ITU) have been unsuccessful, while some countries like China are trying to gain further national influence through voluntary participation in different committees. A similar question arises regarding an internationally legitimate institution that could be assigned to investigate suspected state-actor-driven incidents that would require (in most cases) the exchange and analysis of malware samples or sensitive log data from the affected IT systems (Davis II et al., 2017).

A further problem for arms control approaches is the current lack of an internationally consistent classification of cyber weapons or any kind of malicious cyber tools such as exploits and vulnerabilities in IT products. This lack prevents a uniform risk assessment. Thus, there is no basis for any kind of definition specifying limitations or reporting obligations. This applies to the necessary analysis of possible damage and the classification

of different types, ranges, and destructive factors of cyber weapons. The lack of classification further intensifies cyber armament as unpredictability hinders a "stable balance of military cyber power" where states would agree to limit military capabilities that meet their security requirements.

Previous cyber incidents showed that cyber weapons have so far - unlike expected – mainly been used for gaining hidden access to IT systems. This resembles espionage tactics rather than the use of classic weapons with disruptive or destructive effects. In most cases, cyber weapons rely on exploiting vulnerabilities in IT products. Especially when zero-day exploits are used – attack tools based on vulnerabilities that are not yet known to the public - the malicious cyber tool must be considered a "one-shot weapon" that loses its impact once released because it reveals its attack vector and the exploited weakness. This results in a very cautious disclosure of the cyber capacities of states, which - from a military tactical perspective - work best when they are secretly implanted into the targeted systems and stay hidden until their application is needed (US Government, 2012).

10.5 Important First Approaches of Arms Control in Cyberspace

As demonstrated, there is a growing international understanding of the dangers of an uncontrolled militarisation of cyberspace and the need for cyber arms control measures. The historical examples illustrated that the first step for specific agreements on the limitation or reduction of military goods is a common understanding of the technology's problems and risks. The debates within the international community are moving in this direction, forming an essential basis for agreements on norms and rules for state behaviour in cyberspace as well as for future binding treaties on the military usage of cyberspace technology. The last part of this chapter will present some of the attempts made in recent years by various actors and at different levels of inter-state cooperation that have driven these debates forward and will hopefully help pave the way towards broader agreements. The approaches are not ordered chronologically but according to the involved stakeholders and their target groups. It is essential to mention that these examples do not always explicitly fulfil the criteria of arms control treaties following the presented historical treaties and agreements. Their selection will present state-driven initiatives, proposals from economic actors and civil society to illustrate the different aspects of the ongoing debates in cyberspace and their challenges, and the first results of these efforts.

10.5.1 The Wassenaar Export Control Arrangement and Its Extension from 2013

The ***Wassenaar Arrangement*** *on Export Controls of Conventional Weapons and Dual-Use Goods and Technologies* is a multilateral export control regime. It was established in 1996 and currently consists of 42 member states (Wassenaar, 2011). The objective of

the Convention is to increase international transparency and regulation of trade as well as to limit the distribution of conventional arms. The list of regulated items comprises so-called dual-use items that can be used for both civil and military purposes. The member states of the arrangement undertake to control the export of these critical goods, examine export inquiries and, in the event of suspicion, reject them because of the potential for security-critical or human rights-endangering application. Trade data is exchanged between the member states twice a year. In view of the increasing expansion of intelligence and military activities into cyberspace, a first step towards regulating these activities was taken at the end of 2013. The extension of the agreement comprised the inclusion of "intrusion software" in the catalogue of critical goods, regulated by the following definition (Wassenaar, 2013):

> '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.

This definition considers the functional scope of an application as a sufficient criterion for its regulation, less the possible damage or the specific application environment. One of the problems of the *Wassenaar Arrangement* is its implementation, which falls under the sovereignty and responsibility of each member state and is decided independently. The Federal Office of Economics and Export Control (BAFA) has been commissioned to examine export inquiries in Germany. The German control criteria differ with regard to the destination of planned exports. Exports to EU Member States, NATO members or states with a similar status are generally authorised unless specific political reasons exist against them. Exports to other countries are questioned and examined regarding the potential buyer, the possible open and hidden purpose of use, as well as the political situation and stability in the target country. These decisions and export controls are handled differently in other member states, and there is no obligation for standardised procedures. Control of the proliferation of such goods, an essential component of classical arms control agreements, is, therefore, only possible to a limited extent and does not achieve universal validity. The approach could, thus, be seen as a blueprint for a potentially global approach to regulating these goods and items if combined with consistent and equal national trade export laws and placed under an international control body such as a UN organisation.

10.5.2 The 2018 Proposal of the EU Parliament for a Harmonised Dual-Use Export Controls Regulation

Based on the *Wassenaar Arrangement*, the European Commission has begun to discuss further regulation of such goods within the framework of a uniform export control

system for EU countries (EU Commission, 2016a). It prepared a proposal for the European Parliament, which adopted this position and prepared negotiations with the Council of the EU for a final agreement (EU Parliament, 2018). The EU Parliament's position follows most of the principles of the *Wassenaar Arrangement* on the regulation of technologies capable of cyber surveillance and human rights violations. The definition of the proposal covers (EU Commission, 2016b):

> items specially designed to enable the covert intrusion into information and telecommunication systems with a view to monitoring, extracting, collecting and analysing data and/or incapacitating or damaging the targeted system. This includes items related to the following technology and equipment: a) mobile telecommunication interception, equipment; b) intrusion software; c) monitoring centres; d) lawful interception systems and data retention systems; e) digital forensics

When assessing the export authorisation for cyber surveillance and other affected items, member states must consider the risk of infringement of the defined rules. This regulation potentially broadens the scope of regulated goods and their assessment compared to Wassenaar because it introduces a catch-all control approach that aims to supplement the specific control categories for non-listed technology items and prepare regulation for future developments. Beyond the approach of an EU-wide common export control law, it also proposes a due diligence regime for exporting states and the exporter itself, as well as a responsibility for standardised reports on national export control measures. This exceeds the Wassenaar approach of national sovereignty concerning the specific export rules and reporting procedures. In addition, member states may prohibit or impose an authorisation requirement on the export of dual-use items not listed in the regulation for public security, human rights considerations or the prevention of acts of terrorism.

10.5.3 Recommendations of the United Nations Group of Governmental Experts from 2015

In 1999, the United Nations General Assembly passed the resolution 53/70 *Developments in the Field of Information and Telecommunications in the Context of International Security* (UN, 1999). The resolution is concerned with the increasingly relevant topic of cyberspace in terms of its potential for scientific and technological progress as well as its use for malicious purposes. A further resolution 58/32 of 2003 (UN, 2003) proposed to focus on the threats for this domain, the chances and possibilities for international cooperation in the field of information and communications technology (ICT) (including technical infrastructures) and established a **group of governmental experts (GGE)** to address these issues. Since its foundation, five groups of governmental experts have been concerned with these questions and the applicability of international law in cyberspace. Also, they prepared recommendations for international agreements. The last successful group from 2015 "examined existing and potential threats arising from the use

of ICTs by States" and recommended a set of voluntary, non-binding norms of responsible state behaviour (UN GGE, 2015). These norms have been adopted by the UN General Assembly "in a call to its member states to be guided in their use of information and communications technologies. […] G20 has also invited states to implement the GGE recommendations" (UNODA, 2017). With regard to the challenges of arms control in cyberspace, the recommendations of the 2015 report addressed the following aspects:

> [It] recommended that States cooperate to prevent harmful ICT practices and should not knowingly allow their territory to be used for internationally wrongful acts using ICT. It called for the increased exchange of information and assistance to prosecute terrorist and criminal use of ICTs. [...] A State should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure [...] States should not harm the information systems of the authorised emergency response teams of another State or use those teams to engage in malicious international activity. [...] States should take reasonable steps to ensure the integrity of the supply chain and prevent the proliferation of malicious ICT tools, techniques or harmful hidden functions. [...] The Group identified a number of voluntary confidence-building measures to increase transparency [...] and called for regular dialogue with broad participation under the auspices of the United Nations and through bilateral, regional and multilateral forums. [...] The report called for the international community to assist in improving the security of critical ICT infrastructure, help to develop technical skills and advise on appropriate legislation, strategies and regulation. (UN GGE, 2015)

The 2016/2017 follow-up group did not reach a final consensus. This can be explained (among other things) by disagreements between states about assessing cyber incidents and their impact on national security. The expert group members could not agree on how international law applies to the possibilities and limits of responses to such presumed state activities and appropriate countermeasures.

10.5.4 Proposals for Confidence Building Measures by the OSCE

Over the last years, the **Organisation for Security and Co-operation in Europe** (OSCE) has issued two decisions concerning "confidence-building measures to reduce the risks of conflict stemming from information and communication technologies". Decisions No. 1106 of 2013 (OSCE, 2013) and No. 1202 of 2016 (OSCE, 2016) are based on the organisation's belief and commitment to foster international security by promoting communication and international cooperation between states and other relevant international organisations. In this regard, the organisation developed a set of confidence building measures that should "enhance interstate co-operation, transparency, predictability, and stability, and […] reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs." The measures are voluntary, but the OSCE instructed its member states to base their political decisions, law-making and behaviour on these principals. Most measures concern interstate consultations, the definition of a common

terminology for cyberspace and its threats, the exchange of information regarding the security and use of ICTs as well as – in particular – the risks for critical national and international ICT infrastructures and their integrity:

> Participating States will nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs. Participating States will voluntarily provide contact data of existing official national structures that manage ICT-related incidents and co-ordinate responses to enable a direct dialogue and to facilitate interaction among responsible national bodies and experts. Participating States will update contact information annually and notify changes no later than thirty days after a change has occurred. Participating States will voluntarily establish measures to ensure rapid communication at policy levels of authority, to permit concerns to be raised at the national security level. (OSCE, 2016)

Furthermore, the proposal encourages the establishment of a central platform for the dialogue, exchange of best practices, awareness-raising and information on capacity-building as well as the handling of security threats and incidents and the OSCE is calling on its member states to prepare an effective national legislation for cooperation on this international, interstate level. The proposal extended these considerations, especially regarding the significance of ICT for critical infrastructures and industrial IT systems, and encouraged its member states to cooperate in the exchange of national ICT incidents and the vulnerabilities detected. Although all these proposals concern "only" the political behaviour of states (not the preparations of their armed forces) and are based on exchanging of information and the establishment of communication channels, these efforts must be considered highly valuable. This is due to the critical role of the OSCE as an international organisation that connects states by providing an important and established platform for dialogue and decision-making, potentially fostering necessary discussions and the finding of shared views and rules which could form a basis for negotiations and further agreements.

10.5.5 State-Driven Proposals for Norms and Responsibilities of State Behaviour in Cyberspace

Besides the previous multilateral approaches, various states have in recent years developed proposals for binding norms and rules of state behaviour in cyberspace that followed established rules of international law. These proposals are often driven by national foreign policy priorities or reflect national views and concerns about state sovereignty and internal security.

At the end of October 2018, both Russia and the US, together with other supporting states, submitted two different proposals to the United Nations General Assembly First Committee for the further development of norms and responsibilities of state behaviour in cyberspace. Both proposals assume that states should not use information technology to "carry out activities that are contrary to the maintenance of international peace and security" or "intervene in the internal affairs of other states". The Russian proposal

(UN, 2018a), which is supported by 26 other countries, including China, reaffirms the UN GGE's recommendations. In doing so, the proposing states endorse a comprehensive list of international rules, norms and principles of responsible behaviour. In particular, this draft resolution calls on the Secretary-General to convene an open working group to continue work on these issues, which was discontinued by the UN GGE in 2017. A special feature of this proposal is that it emphasises the state sovereignty over the national internet in terms of the state rights to examine and regulate the information that is shared, transferred, stored and distributed within national IT systems and the national part of the internet. The US-led proposal (UN, 2018b), supported by 35 nations, also confirms the UN GGE's work and calls for a further group of experts. In particular, it should focus on the question of how international law can be applied to the state's use of information and communication without defining new spaces of national sovereignty that profoundly conflict with freedom of speech and other human rights.

Two other proposals worth mentioning are the Paris Declaration and the Commonwealth Cyber Declaration, both published in 2018. The French government presented the Paris Declaration at the Internet Governance Forum (IGF) under the name of *Paris Call for Trust and Security in Cyberspace* (France-Gov, 2018). The Call is formulated as a non-binding document and does not contain any detailed measures, nor does it propose to create new institutions. Rather, it aims to promote existing institutional mechanisms to "limit hacking and destabilising activities" in cyberspace. This move intended to end the confrontations in the intergovernmental debates and the resulting stalemate. For this purpose, the call proposes that the monitoring of effective implementation be delegated to the IGF as a UN body. The text contains nine objectives that balance its priorities between states, businesses and civil society, addressing three main issues: regulation of state-based activities based on norms, state sovereignty in cyberspace and protection of citizens.

The document encourages more comprehensive and coordinated regulation of cyberspace, particularly the maintenance of international peace and security. It recognises the applicability of **international humanitarian law** to cyberspace, including human rights and customary international law. The role and responsibilities of state actors in cyber conflicts are to be strengthened, and active cyber defensive measures by companies are excluded. In the same way, "offensive operations by non-state actors" and the influence of foreign states on democratic processes, such as elections, are condemned. Another central theme of the document is protecting individuals and critical infrastructures from harm. The document calls for the "public core of the Internet" to be protected from hostile actors and demands from the industry a more substantial commitment to "security by design" in products and services. At the time of publication, the call was signed by 57 states, including the EU member states as the strongest faction. Russia, China and the US are not among the signatories.

A second declaration that promotes similar goals is the *Commonwealth Cyber Declaration* (Commonwealth, 2018) which was adopted at the 2018 meetings of the Commonwealth Heads of Government Meeting. This is relevant given the many smaller and economically weaker states of this group, which emphasise the importance of cyberspace

for their nations and express a right to co-determination in its development. Therefore, the Commonwealth Cyber Declaration is, together with the OSCE CBMs, one of the strongest intergovernmental signals for the peaceful development of cyberspace. It acknowledges cyberspace as the basis of social, economic and political development and stresses the dangers of destabilisation of cyberspace by offensive state activities:

> We, as Commonwealth Heads of Government [...] recognising the threats to stability in cyberspace and integrity of the critical infrastructureand affirming our shared commitment to fully abide by the principles and purposes of the Charter of the United Nations to mitigate these risks [...] commit to [...] limit the circumstances in which communication networks may be intentionally disrupted, consistent with applicable international and domestic law. We, as Commonwealth Heads of Government [...] recognise that without cybersecurity citizens are at risk of crime or exploitation, and commit to strengthening legislative, social and educational measures that protect the vulnerable. (Commonwealth, 2018)

In this view, the declaration recognises the importance of international cooperation in tackling cybercrime and promoting stability in cyberspace and supports the UN GGE's recommendations to develop frameworks for applying international law to and establish confidence building measures for this domain. Given the current shift in global politics and the tendency towards the establishment of new political blocks, some researchers even propose a common EU legislation for arms control as a role model that might help to foster this important topic (Bollfrass & Budjeryn, 2020).

10.6 Conclusion

The previous examples of international and national approaches to the development of binding rules and norms for state behaviour have highlighted the increasing acceptance of cyberspace's importance and the international community's growing commitment to ensuring its stability. However, assessments, such as the 2013 cyber security index (UNIDIR, 2013), can only be the first step towards binding rules that limit, reduce or even prohibit the development, proliferation and usage of offensive cyber tools for military purposes. Besides the political will of states, many technical issues need to be analysed to develop solutions to these challenges. Measures need to be developed to verify treaty parties' compliance, practical monitoring of military facilities, or tracking cyber weapon material like software vulnerability exploits. The history of arms control shows that this is a long way to go but a necessary step towards the peaceful development of a global domain. To summarise the chapter:

- Arms control aims to prevent conflicts and foster stability in interstate relations by either reducing the probability of using a specific weapon or regulating its use and thus reducing the costs of armament. Thus, the overall goal of arms control is less a complete disarmament but a rational planning for reducing the risk of war.

- The field of arms control approaches is highly diverse; weapons to be controlled include nuclear, biological, chemical and conventional weaponry.
- Arms control measures include confidence building and verification or preventive measures.
- Cyberspace as a relatively new domain poses many challenges due to its specific characteristics. These include conceptual disagreements, the determination of territory and responsibility as well as the establishment of a supervising authority. Many of the established approaches do not work.
- First approaches for a regulation of cyber weapons include the *Wassenaar Export Control Arrangement* and the 2018 *Proposal of the EU Parliament for a Harmonised Dual-Use Export Control Regulation* that could help to establish arms control measures in cyberspace.

10.7 Exercises

Exercise 10-1: Describe what is arms control and how can it be achieved?
Exercise 10-2: Illustrate the challenges of applying existing norms, regulations and validation measures to the area of cyberspace?
Exercise 10-3: Explain how the concept of disarmament is related to arms control by describing both.
Exercise 10-4: Discuss the reasons why arms control efforts are not always successful.

References

Recommended Reading

Müller, H., & Schörnig, N. (2006). Rüstungsdynamik und Rüstungskontrolle: Eine exemplarische Einführung in die internationalen Beziehungen (Außenpolitik und Internationale Ordnung). Baden-Baden: Nomos.

Meyer, P. (2011). Cyber security through arms control - An approach to international cooperation. *The RUSI Journal*, 156 (2), 22–27. doi: 10.1080/03071847.2011.576471.

UNIDIR. (2013). The Cyber Index - International Security Trends and Realities. Retrieved January 23, 2019, from http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

Bibliography

ABM. (1972). *Treaty Between the United States of America and Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems*. https://treaties.un.org/doc/Publication/UNTS/Volume%20944/volume-944-I-13446-English.pdf.

Bollfrass, A., & Budjeryn, M. (2020). *Arms Control: For and By Europe* [Application/pdf]. 4 p. https://doi.org/10.3929/ETHZ-B-000437456

BWC. (1972). *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (Btwc)*. https://www.unog.ch/80256EDD006B8954/(httpAssets)/C4048678A93B6934C1257188004848D0/$file/BWC-text-English.pdf.

CCM. (2008). *The Convention on Cluster Munitions (CCM)*. https://www.unog.ch/80256EE600585943/(httpPages)/F27A2B84309E0C5AC12574F70036F176?OpenDocument.

CFE. (1990). *Treaty on Conventional Armed Forces in Europe (CFE)*.

Commonwealth, T. (2018). *Commonwealth Cyber Declaration*. https://www.chogm2018.org.uk/sites/default/files/Commonwealth%20Cyber%20Declaration%20pdf.pdf.

CSCE. (1986). *Document of the Stockholm Conference on Confidence- and Security-Building Measures and Disarmament in Europe Convened in Accordance with the Relevant Provisions of the Concluding Document of the Madrid Meeting of the Conference on Security and Co-Operation, (2)*. https://www.osce.org/fsc/41238?download=true.

CWC. (1997). *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (CWC)*. https://www.opcw.org/chemical-weapons-convention

Davis II, J. S., Boudreaux, B., Welburn, J. W., Aguirre, J., Ogletree, C., McGovern, G., & Chase, M. S. (2017). *Stateless Attribution: Toward International Accountability in Cyberspace. RAND*. http://www.rand.org/pubs/research_reports/RR2081.html.

Den Dekker, G. (2004). The Effectiveness of International Supervision in Arms Control Law. *Journal of Conflict and Security Law*, *9*(3), 315–330. https://doi.org/10.1093/jcsl/9.3.315

EU Commission. (2016a). *Commission Proposes to Modernise and Strengthen Controls on Exports of Dual-Use Items.* http://trade.ec.europa.eu/doclib/press/index.cfm?id=1548.

EU Commission. (2016b). *Regulation Setting up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (Recast)*. http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154976.pdf.

European parliament. (1972). *Representation*, *12*(47), 13–13. https://doi.org/10.1080/00344897208656356

France Government. (2018). *Paris Call for Trust and Security in Cyberspace.* https://www.gouvernement.fr/en/cybersecurity-paris-call-for-trust-and-security.

Goldblat, J. (2002). *Arms Control: The New Guide to Negotiations and Agreements*. SAGE Publications Ltd. https://doi.org/10.4135/9781446214947

Graham, T. J. (2004). Avoiding the Tipping Point. In K. M. Campbell, R. J. Einhorn, & M. Reiss (Eds.), *The nuclear tipping point: Why states reconsider their nuclear choices*. Brookings Institution Press.

Hague Conference. (1899). *Convention (II) with Respect to the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land. The Hague, 29 July 1899 (adopted 29 July 1899, entered into force 4 September 1900) (Hague Convention 1899)*. from http://www.opbw.org/int_inst/sec_docs/1899HC-TEXT.pdf

Hague Conference. (1907). *Convention with Respect to the Laws and Customs of War on Land*. https://ihl-databases.icrc.org/ihl/INTRO/195

IAEA. (2015). *Joint Comprehensive Plan of Action*. http://eeas.europa.eu/archives/docs/statements-eeas/docs/iran_agreement/iran_joint-comprehensive-plan-of-action_en.pdf.

ICRC. (1949). *The Geneva Conventions of 12 August 1949*. https://www.icrc.org/en/doc/assets/files/publications/icrc-002-0173.pdf.

INF. (1988). *Treaty Between The United States Of America And The Union Of Soviet Socialist Republics On The Elimination Of Their Intermediate-Range And Shorter-Range Missiles (INF Treaty)*. https://www.state.gov/t/avc/trty/102360.htm#text

Luhmann, N. (2021). *Soziale Systeme: Grundriß einer allgemeinen Theorie* (18th Edition). Suhrkamp.

Mölling, C. & Neuneck, G. (2001). Rahmenprojekt: Methoden, Kriterien und Konzepte für präventive Rüstungskontrolle. In Altmann, J., Bielefeld, T., Hotz, M., Dando, M. R., Liebert, W., Mölling, C., Neuneck, G., Nixdorff, K., Pistner, C, & Schilling, D., *Präventive Rüstungskontrolle*. https://www.wissenschaft-und-frieden.de/seite.php?dossierID=008

Müller, H., Schörnig, N., Schmidt, H.-J., & Wisotzki, S. (2006). *Rüstungsdynamik und Rüstungskontrolle: Eine exemplarische Einführung in die internationalen Beziehungen* (1. Aufl). Nomos-Verl.

New START. (2010). *Treaty Between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms.* www.state.gov/documents/organization/140035.pdf.

NPT. (1970). *Treaty on the Non-Proliferation of Nuclear Weapons*. https://www.iaea.org/sites/default/files/publications/documents/infcircs/1970/infcirc140.pdf .

OPCW. (2023). OPCW confirms: All declared chemical weapons stockpiles verified as irreversibly destroyed. https://www.opcw.org/media-centre/news/2023/07/opcw-confirms-all-declared-chemical-weapons-stockpiles-verified.

OSCE. (2011). *Vienna Document*. https://www.osce.org/fsc/86597?download=true#page=1&zoom=auto,-276,842.

OSCE. (2013). *Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Ttemming from the Use of Information and Communication Technologies*. http://www.osce.org/pc/109168?download=true.

OSCE. (2016). *Decision No. 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from rhe Use of Information and Communication Technologies, (March)*. https://www.osce.org/pc/227281?download=true.

PTBT. (1963). *Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water (Partial Test Ban Treaty — Ptbt)*. https://treaties.un.org/doc/Publication/UNTS/Volume%20480/volume-480-I-6964-English.pdf.

Reinhold, T., & Reuter, C. (2021). Toward a Cyber Weapons Assessment Model—Assessment of the Technical Features of Malicious Software. *IEEE Transactions on Technology and Society*, *3*(3), 226–239. https://doi.org/10.1109/TTS.2021.3131817

Sommer, P. & Brown, I. (2010). *OECD Study—Reducing Systemic Cybersecurity Risk*. http://www.oecd.org/governance/risk/46889922.pdf.

Stohl, R. J., & Grillot, S. (2012). *The international arms trade* (repr). Polity.

UN. (1967). *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies.* http://www.unoosa.org/pdf/publications/STSPACE11E.pdf.

UN. (1999). *A/Res/53/70 Developments in the Field of Information and Telecommunications in the Context of International Security.* https://ccdcoe.org/sites/default/files/documents/UN-981204-ITIS.pdf.

UN. (2003). *Resolution adopted by the General Assembly on 8 December 2003 on Developments in the field of information and telecommunications in the context of international security*. https://ccdcoe.org/sites/default/files/documents/UN-031208-ITIS_0.pdf.

UN. (2011). *Proposal of a Convention for International Information Security by Russia, China et al.* http://archive.mid.ru//bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument

UN. (2013). *Arms Trade Treaty*. https://treaties.un.org/Pages/ViewDetails.aspxsrc=IND&mtdsg_no=XXVI-8&chapter=26&clang=_en?

UN. (2018a). *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/C.1/73/L.37)*. http://undocs.org/A/C.1/73/L.37

UN. (2018b). *Draft Resolution by Russia and Other States Concerning the Developments in the Field of Information and Telecommunications in the Context of International Security*. http://undocs.org/A/C.1/73/L.27

UN Office for Disarmament Affairs. (2017). *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary*. https://www.un.org/disarmament/wp-content/uploads/2018/04/Civil-Society-2017.pdf

UN-GGE. (2015). *Consensus Report 2015—Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security—A/70/174.* http://undocs.org/A/70/174.

UNIDIR. (2013). *The Cyber Index—International Security Trends and Realities*. http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

US Department of State. (1992). *Treaty on Open Skies*. https://www.state.gov/t/avc/cca/os/106812.htm

US Government. (2012). *Presidential Policy Directive 20.* https://www.fas.org/irp/offdocs/ppd/ppd-20.pdf.

Wassenaar. (2011). *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies—Guidelines & Procedures*. http://www.wassenaar.org/guidelines/docs/5-InitialElements.pdf.

Wassenaar. (2013). *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies—List of Dual-Use Goods and Technologies and Munitions List*. http://www.wassenaar.org/controllists/2013/WA-LIST%2813%291/WA-LIST%2813%291.pdf .

Woof, A. F. (2011). *Monitoring and Verification in Arms Control. CRS Report for Congress*. https://www.nti.org/media/pdfs/Monitoring_and_Verification_in_Arms_Control.pdf