Chapter 20
Cyberspace as Military Domain: Monitoring Cyberweapons

Thomas Reinhold

Introduction

Over the last several years, a growing number of military forces worldwide have started to recognize cyberspace as the next military domain whereas the questions of how to regulate this development with measures of arms control and if this works at all for this domain have yet to answered. The strategies that military forces have been prepared (UNIDIR 2013) often involve the establishment of offensive capabilities, sometimes for deterrence reasons or seen as the appropriate measure to react to cyberattacks by actively disturbing or even destroying the attackers IT systems which is described in terms like "active defense" or "hack back" (see exemplary NATO 2010). The necessary "cyberweapons capabilities" of software or hardware with disruptive or destructive effects are actively developed (see exemplary DARPA 2012) and had already been used (US-ICS-CERT 2016; US-DOD 2016), although the cases of cyber incidents so far all happened outside of officially declared wars, and the attribution of cyberattacks to state actors is hard to prove. Nevertheless, many incidents are supposed to be performed by state actors like the so called "BlackEnergy" malware that affected the Ukrainian electric power industry (US-ICS-CERT 2016). A few cases exist where military strategies explicitly include cyber warfare capabilities, such as in the U.S. fight against the ISIS terror group (see US-DOD 2016). On the other hand, the international community currently struggles to come to an agreement on binding norms of state behavior and how established rules of international law can apply to this new domain (Tikk and Kerttunen 2017). The debates include the challenge of determining an appropriate response to the ongoing militarization of cyberspace, the question of how to slow down the armament and the prevention of an arms race in this domain. Furthermore, the attempt to apply established measures of arms control or non-proliferation, as well as lessons learned from

T. Reinhold (✉)
Institute for Peace Research and Security Policy (IFSH), Hamburg, Germany
e-mail: info@cyber-peace.org

D. Feldner (ed.), *Redesigning Organizations*,
https://doi.org/10.1007/978-3-030-27957-8_20

other military technological developments, quickly comes to a stop due to specific technical features in cyberspace. Against this background, the following article will look at the core principles of arms control and the problems when applying these to the cyberspace domain. It will use as examples the lessons learned from nuclear disarmament as the most assessed arms control and arms monitoring area from the recent decades. The comparison will be used to develop concepts and approaches for applicable cyber arms control measures and to formulate the outlook for necessary treaties and international institutions.

The Roots and Core Principles of Arms Monitoring

The concept of arms monitoring is a general term that is often used in the context of arms control and non-proliferation. The overall function of arms control is the prevention of conflicts and the stabilization of international state relations by reducing the motivation of adversaries for preventative or pre-emptive military operations to destroy military capacities, as well as for the reduction of the probability of the application of specific military weapon systems (Müller and Schörning 2006). These goals are tackled on different levels and by different measures. Neuneck and his fellow authors give an overview (Mölling and Neuneck 2001) that differentiates using the following categories and correlating measures:

- Geographic measures: demilitarized regions, security zones
- Structural measures: defensive orientation of force structures
- Operative measures: limitation of maneuvers, omission of provocative actions
- Verification measures: data exchange, inspections
- Declaratory measures: abandon the first use of nuclear weapons
- Technology-related measures: limitation, reduction or destruction of certain weapons or technologies
- Proliferative measures: prohibition or restriction on the export of militarily relevant technologies
- Selective measures: prohibition or restriction of the use of certain weapons and methods of war
- Actor-related measures: prohibition, restriction or permitting of specific groups of actors
- Goal-related measures: safeguard clauses, prohibition of attack on particular, especially civil, targets.

These specific measures are embedded in treaties or agreements where parties bilaterally or multilaterally declare their intent for specific actions or their omission and the dedicated procedures and actions. A popular example is the “Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction”, often abbreviated as CWC, that had been negotiated by the UN, entered into force in 1997 and established the Organization for the Prohibition of Chemical Weapons (OPCW) to control the implementation of

the treaty (United Nations 1992). Such treaties and binding agreements as well as the customary international law create the international law that defines the rules for state behavior and interactions. One of the main principles of these rules is the convention "pacta sunt servanda" (Wehberg 1959). This centuries-old principle, that translates to "agreements must be kept", had been explicitly formulated 1969 in the "Vienna Convention on the Law of Treaties" (United Nations 1969) and entered into force in 1980. The convention describes that "every treaty in force is binding upon the parties to it and must be performed by them in good faith". This general rule brought to light the question of how treaty members are able to surveil and control the mutual compliance of agreed terms and how this should be performed. This task, which is described as verification, is an important measure for international security politics and mostly integrated in verification regimes, a concept that is based on the regime theory of Robert O. Keohane (Robert and Martin 2009). Verification regimes are either integrated to existing treaties or stand for themselves and consist of the following different parts:

- The treaty agreement itself.
- The rules that the treaty members agree to follow in combination with specific thresholds, binding instructions or forbidden activities.
- The practical measures that treaty members or specifically entrusted authorities are allowed to perform in order to control the compliance of the other treaty members.
- The definition of the authority that is allowed to make decisions regarding the compliance and consequences that states agree to perform and bear when the agreed rules are not followed.

In other terms, verification and the task of controlling and monitoring weapons is always a very context specific definition of what is getting controlled, how, by whom and for what purpose.

Principles of Nuclear Weapons Monitoring

One of the most intense verification debates of the last fifty decades concerns the risks and threats of nuclear armament. The most commonly known institution in the context of these debates is the International Atomic Energy Agency (IAEA), an international independent organization that had originally been founded in 1957 for the promotion and development of the peaceful usage of nuclear energy (IAEA 1961). It directly reports to the United Nations General Assembly and the United Nations Security Council. Since its foundation, its tasks have fundamentally changed. With the international adoption of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT 1968), the IAEA had been put in charge of different treaties (Neuneck 2017) "*to establish and administer safeguards designed to ensure that special fissionable and other materials, services, equipment, facilities, and information made available by the Agency or at its request or under its supervision or control are not used in such a way as to further any military purpose; and to apply safeguards, at the request of*

the parties, to any bilateral or multilateral arrangement, or at the request of a State, to any of that State's activities in the field of atomic energy" (IAEA 2018a; IAEA 1961). These safeguards (IAEA 1968) are practical measures that reflect the core of nuclear weapons monitoring and address two different dimensions: "horizontal" and "vertical" non-proliferation. Horizontal non-proliferation is the challenge of preventing and regulating the spread of nuclear weapons to new state and non-state actors by banning the trade of nuclear arms, as well as stopping capabilities for the production of nuclear weapons or feasible material. The term vertical non-proliferation, on the other hand, describes measures to control the technological advancement and stockpiling of nuclear weapons by nuclear powers (Goldansky 1988). One of the most recent tasks of the IAEA, which should be used as a demonstrative example for the different levels of nuclear arms control, is the supervision of the JCPOA nuclear treaty agreement (Joint Comprehensive Plan of Action) (IAEA 2016), which had been negotiated with the Islamic Republic of Iran by the five permanent members of the United Nations Security Council, Germany (P5+1) and the European Union over thirteen years, came into force in January 2016 and is still active despite the one-sided termination of the agreement by the United States under US President.

Iran's compliance is controlled by verification measures that are integrated into this treaty as safeguards. They enable IAEA staff members to get access to nuclear and research facilities, shut down and seal critical industrial hardware, install surveillance cameras, control industrial plants, count the equipment in nuclear facilities, take samples from nuclear material, as well as measure the radiation level of devices and places. As already pointed out, these verification measures are always practical steps that tightly concentrate on specific aspects of the controlled technology, the outcomes of which can be compared against threshold values, "do's and don'ts" or lists of forbidden technological procedures. Such monitoring measures always need to be very specifically tailored to the controlled technology and the monitoring context and can therefore strongly differ for different kinds of situations. From a broader and more generalized perspective, they can be categorized into four areas of restrictions that directly relate to applicable monitoring principles (Neuneck 2012):

- Geographical restrictions that regulate the allowed or prohibited location of specific goods, which are controlled by locating and visually monitoring (like ultra violet and x-ray imaging or aerial and satellite photography) these goods. An example for such monitoring measures is the Treaty on Open Skies (OSCE 1992), which came into force in 2002 and is currently ratified by 34 states. It allows unarmed aerial surveillance flights over the entire territory of the treaty members.
- Limitations in terms of the amount or even the complete prohibition of the possession of goods are controlled by counting and cataloging the goods. This can include the reduction of existing capacities. An example is the "Strategic Arms Reduction Treaty—New START" (NTI 2010) as the successor to former treaties (START I from 1991 and START II from 1993) between the United States and the Russian Federation. The treaty entered into force in 2011 and is valid until 2020, and it regulates the further nuclear arms reduction of both countries. The treaty

establishes a commission and dedicated rules and deadlines for inspections and its bilateral organization.

- Definitions of threshold values for specific properties of physical, chemical or biological states of goods are controlled by measuring or scientifically estimating these properties. An example is the already mentioned JCPOA treaty with the Islamic Republic of Iran (IAEA 2016). Among other things, the treaty contains agreements to reduce the enrichment level of uranium to a degree that enables medical treatments and research but prevents the fast weaponization of the uranium for nuclear bombs (IAEA 2018b).
- Restricting the proliferation of goods is controlled by tracing the goods, regulating or prohibiting their trade. An example of a non-proliferation treaty is the Treaty on the Non-Proliferation of Nuclear Weapons (NPT 1968), which 191 states currently adhere to. This treaty directly shaped the role and responsibilities of the IAEA that, among other things, enables the organization to inspect nuclear facilities. An additional protocol of the treaty extends these rights to include unannounced inspections and is currently signed by 139 states.

Established Measures and Their Applicability in Cyberspace?

This chapter will assess the questions about how these measures, the experiences and lessons learned can be applied to cyberspace and the challenges of an ongoing cyber armament:

In contrast to all other domains, cyberspace has some specific technical features that differ strongly from all other domains and have an important impact on the application of monitoring approaches. Often these technical features render established measures useless, because they are designed for physical domains like sea, air, land or space and rely on features of these domains that cyberspace does not provide. Therefore, the technical specifics of cyberspace have to be taken into account when thinking about monitoring and arms control in this domain.

Virtuality

First of all, cyberspace is by design a "virtual" domain. In theory, data is stored and processed by a specific IT system that has a geographical location and falls under a legislatively responsible jurisdiction. On the other hand, data can be seamlessly copied and—especially in the cloud computing age—is often transferred and stored on other IT systems for availability issues or split up into multiple parts to be processed on different and sometimes even geographically distributed IT systems. This means that even if hardware itself always has a physical representation, in practical

terms, the data itself, its storage and processing cannot be reasonably attributed to a specific geographical location and a specific nation states sovereignty.

Distribution

Another relevant aspect of software, like any other digital information, is that every piece of such data is stored physically in different ways, such as magnetic fields on classic hard drives or electromagnetic states on solid state drives, but that this storage takes place distributed within other data fragments. The handling of data as logical entities, like files, is a mere abstraction of operating systems and the physical storage most likely isn't carried out in a cohesive manner. This means that data itself has no specific coherent physical representation, and digital information cannot be handled as a unique and autonomous self-contained entity like a missile, a tank or a test cube. Furthermore, it also does not produce any kind of reliable "traces" when moved or copied, traces that could be used for monitoring. Any way of "counting" and limiting software is rendered meaningless by these aspects.

Attribution

A third technical feature of cyberspace is commonly known as the attribution problem. This term describes the problem and the ambiguity of assigning any kind of activity within cyberspace to its origin and the presumed actor that intentionally performed this activity. The necessity for attributing an attack to its origin and therefore identifying the attacking party is a key element to the states right for self-defense under the UN Charta. Attribution of cyberattacks is currently considered to be the main problem when applying international law and its rules of state behavior to cyberspace (see example Guerrero-Saade and Raiu 2017) because digital data transfer happens over multiple steps of involved IT system and cyberattackers use this feature to create a complex path from the system that controls an attack to its target. Recreating this path potentially involves the necessary cooperation of each of these "hubs". This technical feature provides multiple possibilities for adversaries to cover their tracks and use IT systems of uninvolved third parties. It also means that even if the source system of any data access is identified, it is unclear if the system itself had been hacked and misused. This principle also affects the question of how goods can be assigned to their owners, as well as the task of regulating their proliferation.

Dual Use

The last feature of cyberspace specifically concerns the technical equipment that is necessary for its infrastructure—the networking and computing devices, from servers to home electronics, or even embedded controlling devices and the software they are running—the 'Internet of Things'. All of this technology can be used for military as well as civilian purposes without being able to draw a distinct line between these usage scenarios. Therefore, it cannot be generically prohibited or allowed for arms control reasons. Furthermore, the dual use character of goods means that it's not the good itself but its precise usage that determines whether or not it falls under the negotiated agreements of arms control and disarmament. The task of defining lists of such goods and the necessary special control and monitoring has been performed for several decades for nuclear, chemical and biological goods. Its most popular example is the Wassenaar Arrangement (Wassenaar 1996), a treaty between 42 currently participating states that have agreed upon dedicated arms and export control, as well as sharing trade data for such sensitive goods as a measure of trust and confidence building. The treaty had been broadened in 2013 to include "intrusion software" (Wassenaar 2017) that can be used either for surveillance or to break and undermine IT security measures or otherwise manipulate IT systems.

In comparison with former dual-use approaches—where a relevant factor for the regulation of chemical, biological or nuclear goods was either the sheer amount of specific materials, the necessary equipment or specific military delivery systems that can be monitored and verified—the dual-use character of IT hardware and software is even more distinct. This means that, for cyberspace and its necessary technological infrastructure, it is not possible to differentiate between goods, because both the hard- and software are the same for civil, economic and military purposes. This also affects any approach towards differentiation between legitimate goods that distinctively serve military defensive measures and those whose primary purpose is for offensive measures. Even malware or software exploits that can be used offensively are also necessary to test and increase the cyber security of IT systems. A popular example for this case are penetration testing tools: software that is specifically designed to attack and penetrate IT systems and networks to detect flaws, weaknesses and security problems. These tools are an important instrument for IT security practitioners and its regulation can affect the protection of IT systems. On the other hand, its detection during theoretical inspections doesn't necessarily prove any non-compliance to a treaty. Therefore, only the usage of tools is decisive regarding the offensive or defensive application of goods. Any verification regime rules that declare certain behaviors forbidden need to implement measures for controlling the specific application of IT goods, which is not practically implementable as argued before.

Concepts for Cyber Arms Monitoring and Control

An important step for arms control and monitoring is the definition of the subject that needs to be regulated. Aside from the mentioned Wassenaar Agreement, this step has not yet been performed in internationally binding treaties. The presented specifics of cyberspace showed that such a definition has to consider more than the aspects of the usage, the intention of use and the effects of a tool over the specific technical features. A fitting definition that comprehensively reflects these is given by Stefano Mele:

> [a cyberweapon is] A part of equipment, a device or any set of computer instructions used in a conflict among actors, both National and non-National, with the purpose of causing, even indirectly, a physical damage to equipment or people, or rather of sabotaging or damaging in a direct way the information systems of a sensitive target of the attacked subject (Mele 2013).

Based on this definition, and in the light of the technical specifics of cyberspace, the core questions of monitoring and arms control—"*what to control, how to control it, by whom and for what purpose*"—raise the concerns about what aspects can actually be monitored in this domain. An assessment of suitable and measurable parameters also needs to evaluate the degree of explanatory power that a specific parameter can provide, as well as the question how the measurement can be performed. On the other hand, the extent of necessary alteration of hardware or software for monitoring purposes will affect the applicability and the political acceptance of possible monitoring regimes. With regard to this consideration, the paper takes the establishment of any first steps for cyber arms monitoring as a starting point and concentrates on parameters and measures that "look from the outside" on IT systems and the networks and do not require a modification of existing IT hardware or software infrastructures.

Physically Obvious Parameters

The first set of measurable parameters can be defined as these parameters that are physically obvious, hard to disguise or manipulate and obvious to monitor. They are applicable to monitor the tendency of technological developments, the establishment of new cyber capacities and will reveal significant changes. The drawback of these parameters is that they will not be applicable to monitoring the real time activities of actors like clandestine cyber operations. The parameters are:

- The overall power supply and the current power consumption of IT infrastructures
- The available cooling power and current thermal power production of IT infrastructures
- The network bandwidth and transmission capacities and current flow rates of data transmissions
- The number of interconnections to other external civil or commercial networks and their maximum and current transmission performance

- The required maintenance staff for the IT infrastructure
- The available computing processing and network processing power, as well as storage capacities. Measurement of these parameters requires direct access to the controlled systems.

Parameters of the Extent of Usage and Adaptation of Existing Tools

The other set of parameters applies to the usage of IT systems and aims to measure or monitor their specific application. They qualify for the real time control of cyber operations and activities but can still be gathered "from the outside". The drawback of these parameters is that they are capable of monitoring cyber activities in such detail that they can potentially reveal unwanted or even secret information. Their application will therefore be limited to situations that justify such intrusiveness. This could be either high risk contexts with a strong potential for military misconceptions and escalations or as a strong political signal of transparency and trustworthiness by unilateral declarations of a state. The applicable parameters are:

- The meta data of incoming and outbound network connections like senders and receivers, as well as the type and amount of transferred data
- The amount of usage of anonymization services or network encryption services
- The acquisition, possession and stock piling as well as the usage of software and hardware vulnerabilities like exploits for known security problems. Such vulnerabilities and code that uses these flaws are the "weapons material" for intrusive cyber tools ("cyber weapons") and necessary to overbear IT security measures, get access to IT systems, transfer the payload and perform the intended operations.

The above differentiation demonstrates that the question of the purpose of each monitoring measure needs to address specific situations and political agreements, either to provide oversight for the technological advancements or to restrict and control the deployment of specific offensive cyber operations. With regard to the task of applying established verification principles in cyberspace, the principle that seems to be most applicable is the definition of any kind of thresholds. It paradigmatically reflects that not the presence but the extent of the usage of goods in cyberspace defines compliance or noncompliance with an agreement. Approaches like restricting possession and/or proliferation of goods currently fail, as shown, due to the technical nature of the domain. On the other hand, the analysis of the necessary monitoring procedures reveals that there are already existing methods in computer science that have been developed for comparable protection and control claims, but that have not yet been used in the context of arms control and disarmament. For example, the question of how to control and restrict the usage of IT goods to allowed clients has been a challenge for the IT economy since the early days of software development and marketing. Over the last decades, a lot of effort has been put into digital rights and

intellectual property protection systems and digital usage restrictions like the digital rights management technologies (DRM) with hardware dongles or online software authentication. A similar situation exists for the question of uniquely identifying IT systems in networks. The new internet addressing system—IPv6—provides technologies and capacities to provide unique addresses for all IT devices, which can help to overcome the attribution problem when applied to relevant networks like those that are used by military forces or intelligence services. Such mechanisms can, for example, provide a way of marking military cyber forces and their activities. The examples show that arms control and disarmament are merely new ways of looking at the challenges of interconnected global IT systems from a political and international security standpoint that don't necessarily require the development of new technologies, but rather apply and adapt existing tools and concepts in the light of different goals. It's not the perfect solution to technological problems, but it raises the question of how current systems can be shaped for a technical restriction of states and military forces to apply military pressure over cyberspace, as well as the question of how to control these restrictions.

Conclusion and Outlook

The previous explanations showed the necessity of—as well as the different problems with—the task of arms monitoring in cyberspace. They also demonstrated that many of the lessons learned from former technological developments steps cannot be applied or projected on this new artificial domain, which fundamentally differs in important technical aspects. In comparison to nuclear arms control and disarmament, the challenge of cyber armament monitoring has one strong advantage. The relevant domain is—in contrast to air, space, sea and land—completely man made, and all its rules are based code (see exemplary the "Code is Law" argumentation, Lessig 2006). Every functional principle is defined and created by people or, rather, international committees like the standardization-focused Internet Engineering Task Force (Bradner 1999) or the more research-focused Internet Research Task Force (IRTF 2018). These committees develop new technologies for cyberspace and decide about their deployment. This provides a strong point for legislation and means that principles can be further established to support the peaceful development of this domain, to create transparency where it's necessary and to support measures for international political stability. On a national level, recent political debates on the implementation and institutionalization of processes—such as a vulnerabilities equities process that makes decisions about the disclosure of computer security vulnerabilities that are used or held secret by state institutions—will provide important experience for how the assessment of hazardousness and the possible impact of malicious cyber tools can be used for future arms control institutions.

Bibliography

Bradner, S. (1999). *Internet Engineering Task Force (IETF)* (p. 1). Open Sources: Voices from the Open Source Revolution.

DARPA. (2012). Broad Agency Announcement—Foundational Cyberwarfare (Plan X), DARPA-BAA-13–02. Arlington, USA. Retrieved from https://govtribe.com/project/darpa-baa-13-02-foundational-cyberwarfare-plan-x.

Guerrero-Saade, J. A., & Raiu, C. (2017). Walking in your enemy's shadow: When fourth-party collection becomes attribution hell. In *Virus Bulletin Conference*.

Goldansky, V. (1988). Connection between horizontal and vertical proliferation of nuclear weapons. In J. Rotblat & L. Valki (Eds.), *Coexistence, cooperation and common security*. London: Palgrave Macmillan.

IAEA. (1961). *The agency's safeguards. The International Atomic Energy Agency*, Geneva, Switzerland. Retrieved from https://www.iaea.org/sites/default/files/publications/documents/infcircs/1961/infcirc26.pdf.

IAEA. (1968). *The agency's safeguard systems. The International Atomic Energy Agency*, Geneva, Switzerland. Retrieved from https://www.iaea.org/sites/default/files/publications/documents/infcircs/1965/infcirc66r2.pdf.

IAEA. (2016). *Iran and the IAEA: Verification and monitoring under the JCPOA. The International Atomic Energy Agency*, Geneva, Switzerland. Retrieved from https://www.iaea.org/sites/default/files/5722627.pdf.

IAEA. (2018a). *The statute of the IAEA. The International Atomic Energy Agency*, Geneva, Switzerland. Retrieved from https://www.iaea.org/about/statute.

IAEA. (2018b). *Statement on Iran by the IAEA Spokesperson on May 1, 2018*, Geneva, Switzerland. Retrieved from https://www.iaea.org/newscenter/pressreleases/statement-on-iran-by-the-iaea-spokesperson.

IRTF. (2018). Internet Research Task Force. Retrieved from https://irtf.org/.

Lessig, L. (2006). *Code: And other laws of cyberspace, Version 2.0*. Center for Internet and Society Standford.

NPT. (1968). *Treaty on the non-proliferation of nuclear weapons*. Retrieved from https://www.state.gov/documents/organization/141503.pdf.

Mele, S. (2013). *Cyber-weapons: Legal and strategic aspects*.

Mölling, C., & Neuneck, G. (2001). Präventive Rüstungskontrolle und Information Warfare. In Rüstungskontrolle im Cyberspace. Perspektiven der Friedenspolitik im Zeitalter von Computerattacken, in: Dokumentation einer Internationalen Konferenz der Heinrich-Böll-Stiftung am 29./30. Juni 2001 in Berlin, S. 47–53.

Müller, H., & Schörning, N. (2006). Rüstungsdynamik und Rüstungskontrolle: Eine exemplarische Einführung in die internationalen Beziehungen Nomos, 2006, Aussenpolitik und Internationale Ordnung.

NATO. (2010). *Cyber war and cyber power. Issues for NATO doctrine*. Rome: NATO Defense College.

Neuneck, G. (2012). Confidence building measures—Application to the cyber domain. In *Cyber Security Conference*, Berlin.

Neuneck, G. (2017). 60 Jahre nuklearer - Prometheus oder Sisyphos? Vereinte Nationen Magazin, 2017.

NTI. (2010). Treaty between the United States of America and the Russian Federation on measures for the further reduction and limitation of strategic offensive arms (New START). *Nuclear Threat Initiative*. Retrieved from http://www.nti.org/media/documents/new_start.pdf.

OSCE. (1992). *Treaty on Open Skies. Organization for Security and Cooperation in Europe*, Vienna, Austria. Retrieved from https://www.osce.org/library/14127.

Robert, K., & Martin, L. (2009). The promise of institutionalist theory. *International Security, 20*(1), 39–51. http://www.jstor.org/stable/2539214. (Published by : The MIT Press Stable Robert O. Keohane and Lisa L. Martin).

Tikk, E., & Kerttunen, M. (2017). *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*. New York, The Hague, Tartu, Jyvaskyla: Published by the Cyber Policy Institute.

United Nations. (1969). *Vienna Convention on the law of treaties*. United Nations. Geneva, Switzerland. Retrieved from https://treaties.un.org/doc/publication/unts/volume%201155/volume-1155-i-18232-english.pdf.

United Nations. (1992). *Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction*. Retrieved from https://treaties.un.org/doc/Treaties/1997/04/19970429%2007-52%20PM/CTC-XXVI_03_ocred.pdf.

US-DOD. (2016). *Department of Defense press briefing by Secretary Carter and Gen. Dunford in the Pentagon briefing room from February 29, 2016*. Washington, USA. Retrieved from https://www.defence.gov/News/Transcripts/Transcript-View/Article/682341/department-of-defence-press-briefing-by-secretary-carter-and-gen-dunford-in-the/.

US-ICS-CERT. (2016). Alert (IR-ALERT-H-16-056-01) *Cyber-attack against Ukrainian critical infrastructure*. The U.S. Industrial Control System Computer Emergency Response Team. Retrieved from https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

UNIDIR. (2013). *The cyber index—International security trends and realities*, Geneva, Switzerland. Retrieved from www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

Wassenaar. (1996). *The Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies, Initial Elements*. Retrieved from https://www.wassenaar.org/docs/IE96.html.

Wassenaar. (2017). *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*. Wassenaar Arrangement Secretariat.

Wehberg, H. (1959). Pacta sunt servanda. *The American Journal of International Law, 53*(4), 529–551.

Dipl.-Inf. Thomas Reinhold is a peace and security researcher and an expert for the challenges of the militarization of the cyberspace. As a graduated computer scientist, he works on technical measures for trust and security building for this domain like verification, arms control and non-proliferation. He is a Non-Resident Fellow at the Institute for Peace Research and Security Policy (IFSH) and a Ph.D. candidate at the research group Science and Technology for Peace and Security (PEASEC) at TU Darmstadt. He is also a member of the Transatlantic Cyber Forum and the Research Advisory Group of the Global Commission on the Stability of Cyberspace.