ICT for peace foundation

POLICY
BRIEF

# HOW CAN ARMS CONTROL AND DISARMAMENT CONTRIBUTE TO A SECURE CYBERSPACE?

**Martin Dahinden**

**GENEVA 2022**
ICT4Peace Foundation

ICT4Peace Publishing, Geneva. April 2022
Copies available from www.ict4peace.org

# HOW CAN ARMS CONTROL AND DISARMAMENT CONTRIBUTE TO A SECURE CYBERSPACE?

**Martin Dahinden**

ICT for **peace** foundation

# Table of Contents

# HOW CAN ARMS CONTROL AND DISARMAMENT CONTRIBUTE TO A SECURE CYBERSPACE?

**Martin Dahinden**[1]

## Abstract

The arms race in cyberspace poses risks to international stability and security. Arms control and disarmament have thus far played almost no role in international discussions on cybersecurity, even though arms control has been importance to global stability for more than half a century. This article shows that experience from arms control is relevant to the cyber domain, both for understanding the policy process and as a source of inspiration for concrete solutions. Like cybertechnology, nuclear technology was once entirely novel and difficult to assess. Comprehensive agreements were initially unattainable; in contrast, limited and pragmatic steps led over time to a comprehensive arms control regime. This approach is also promising for the cyber domain. The concrete experiences and solutions from arms control cannot simply be transferred to the cyber domain, but they do draw attention to promising approaches in areas such as no-first-use policy, de-targeting, non-proliferation, confidence building, prohibition to develop certain dangerous technologies, cooperation, regional arrangements, verification, enforcement, and sanctions. Progress will depend primarily on whether key political actors (US, China, Russia) can agree on common objectives. This in no way implies that other states, multilateral organizations, think tanks, academia, and civil society organizations have no role. What is needed is broad discussion and political pressure, but also innovative approaches to solutions.

[1] Martin Dahinden is Vice-Chairman of the Think Tank ICT4Peace. He was Swiss Ambassador to the USA and teaches security policy at the University of Zurich. He thanks Daniel Stauffacher, Founder and President of ICT4Peace for his inputs and critical review.

# 1. Introduction

Cyberweapons exist and are spreading rapidly. A real arms race is taking place in cyberspace today. The risks to international stability are significant, but difficult to assess. Most states have recognized the dangers of offensive cyber capabilities to their national security, although cyber-attacks cannot inflict the same damage as kinetic attacks.

There is broad international consensus that existing international law applies in cyberspace. However, there is no consensus on how to apply it, what constitutes an armed attack, etc. Extensive deliberations have taken place on international humanitarian law in cyberspace, on norms of responsible state behavior, and on confidence-building measures, among others, within the United Nations.[2]

By contrast, arms control, disarmament, and non-proliferation have not been the focus of international discussions. The Swiss government's Arms Control and Disarmament Strategy 2022-2025 rightly states that "consideration should be given to the extent to which arms control approaches could be used to address certain cyber challenges, notwithstanding the fact that digital technologies do not per se correspond to traditional armaments." [3]

Arms control and disarmament have a fundamentally different purpose than international humanitarian law. It is not about the rules to apply during armed conflict. It is about the prohibition, reduction or limitation of weapons and military capabilities with the aim of achieving stability, preventing the outbreak of conflict, and limiting the impact of armed conflict.

For more than half a century, arms control and disarmament were the key element of bilateral relations between the United States and the Soviet Union. During the Cold War, arms control played a prominent role in managing the arms race and in global stability. It was instrumental in keeping nuclear weapons from being used and limiting their proliferation. Arms control has also regulated the buildup of other military potential and banned entire categories of weapons.

What lessons can be learned from these experiences and from the concepts of arms control and disarmament for the cyber domain?

[2] Lauber & Eberli 2021. Tiirma-Klaar 2021. Meyer & Stauffacher 2021. United Nations Office for Disarmament Affairs (2017).

[3] EDA 2022: 28.

## 2. Cyberspace and Cyberweapons

Cyberweapons are more complex than anything arms control and disarmament have ever dealt with. The *Cyberspace* as a sphere is extraordinary complex. It is the virtual space created by the global interconnection of ICT infrastructure that allows information flows to circulate unlimited by geographic distances or other common physical constraints.[4] As a virtual sphere, cyberspace is largely operated and used by the private sector.

The point of departure for arms control and disarmament is weapons and military capabilities. A *cyberweapon* is a computer code that can threaten and inflict physical, functional, or psychological damage on systems, structures, or living beings.[5] The spectrum of cyberweapons is wide. At the more benign end is malicious software (malware) that affects systems from the outside but cannot technically penetrate and cause immediate damage, for instance software that generates massive traffic to overload servers. At the other end of the threat spectrum is malware that penetrates even protected and physically isolated systems and inflicts direct damage, not only to data, but potentially with major physical impact, for example by destroying weapons systems, other military capabilities, or infrastructure (Computer Network Attacks CNA).

*Arms race in cyberspace* takes place as a buildup of offensive (and defensive) capabilities. There is no tangible, countable, controllable objects, as with conventional forces or kinetic weapons (tanks, missiles, submarines, etc.). It is extremely difficult to quantify military strength (balance of forces) in the cyber domain with some reliability. These are all clear signs that the experience gained from disarmament and arms control thus far cannot be transferred to the cyber domain without further scrutiny.[6]

## 3. Arms Control, Disarmament and Non-proliferation

*Disarmament* is the unilateral, bilaterally, or multilaterally agreed elimination or reduction of weapons and military capabilities. The long-term political goal is complete

[4] Definitions: Ning et al. 2018. Starodubtsev et al. 2020: 1-3.

[5] Rid & McBurney 2012.

[6] Borghard & Lonergan 2018.

disarmament to eliminate, as far as possible, the use of force between states, as required by the UN Charter and consistent with the UN's political vision.[7]

*Arms control* goes less far. It assumes that rivalry between states will continue to exist, as will military potential. Therefore, arms control is not about total elimination, but about monitoring the number, the production, the development, the storage of weapons or the deployment of troops. [8]

Experience with arms control and disarmament goes back to ancient times. In contrast to the mostly very general provisions of international humanitarian law, arms control and disarmament agreements are very specific and precise. They concern well defined weapons and capabilities, for example chemical or biological weapons; they often refer to clearly defined geographical perimeters, for example in the case of demilitarized zones. For some arms control and disarmament agreements, universal adherence is sought, as for the Treaty on the Non-proliferation of Nuclear Weapons NPT. But there are other agreements that have been concluded among a few contracting parties, such as the New Start Treaty between Russia and the USA.

In addition to the core provisions, arms control and disarmament agreements usually contain substantial provisions on verification and compliance. There may also be provisions for the enforcement of the agreement, on sanctions, confidence-building measures, on procedures for peaceful dispute settlement, or on cooperation among the parties regarding activities for peaceful purposes (in the NPT for instance on cooperation for the civilian use of nuclear energy).

*Non-proliferation measures* have the purpose of preventing the spread of weapons and technologies. The focus has traditionally been and still is on weapons of mass destruction (NBC weapons) and on their delivery systems. Non-proliferation measures can be regulated in an agreement (as in the Chemical Weapons Convention, or the NPT). Important for non-proliferation are the so-called dual-use goods, which means goods that have a civilian use but can also be used to produce weapons, such as industrial chemicals that are at the same time precursors for chemical weapons or solid-fuel missiles. Dual-use goods are to a large extent controlled by informal control regimes. Within these control regimes states exchange information on (hidden) procurement activities and coordinate their control measures (Australia Group, Missile Technology

[7] Burroughs 2016.

[8] Croft 1996. Rumer 2018.

Control Regime, Nuclear Suppliers Group, Wassenaar Arrangement).[9] The UN Security Council, individual states or groups of states can also decide on measures against proliferation. Regarding cyber technology there is currently no such specific control regime. The prospects for strategic export controls of cyber technology are difficult to assess, the assessments and opinions on this are widely divergent.[10]

# 4. Opportunities and Limitations for Disarmament and Arms Control in the Cyber Domain

At a first security policy glance, cyber weapons have many characteristics that make them suitable for arms control and disarmament. Offensive cyber capabilities can challenge balances of power. They can - intentionally or unintentionally - lead to escalation even beyond the cyberspace and including kinetic means of warfare. The geopolitical context matters, for example great power competition or regional tensions. Cyberattacks can cause great damage. Less clear are the costs of the arms race in cyberspace; therefore, it is also difficult to assess whether there is an incentive to limit cyber arms race for financial reasons.

## Challenges for Arms Control

The difficulties and obstacles for arms control and disarmament in cyberspace are obvious. The intricate characteristics of cyberweapons have been mentioned. Cyberweapons are even more complex than biological weapons with their rapidly changing technological environment (biotechnology, genetic engineering, etc.).

*Verification* in the cyber domain is difficult to imagine. Notifications and inspections would require the disclosure of sensitive information. States are extremely reluctant to take such commitments. Regarding cyber capabilities disclosure would not only expose a state's own cyber capabilities, but also reveal gaps in its defense.

*Means of cyber warfare are in the development phase*, possibly even at an early stage. Experience has shown that it is almost impossible to ban or restrict weapons while they are still in a developmental phase.

[9] Joyner 2020.

[10] Barbieri et al. 2018.

Not only state actors or armed forces are capable for offensive cyber operations, but also *private entities*, i.e., non-state actors or even individuals. While it is possible that international agreements impose obligations on states to establish criminal law norms, to exercise controls, etc. within their jurisdiction, these are outside the logic of arms control and disarmament and belong to the area of law enforcement.[11]

Such complex issues are a major reason why disarmament and arms control have been neglected so far and efforts were on international humanitarian law, norms of responsible state behavior, confidence building measures, capacity building etc. These are also less intrusive. Hence it is difficult to imagine states committing to far-reaching obligations without legally binding commitments among each other. Non-binding norms, interpretation of existing rules, codes of conduct etc. are certainly useful steps on the way to legally binding agreements, but no replacement.

However, the main problem for the slow progress, is not the conceptual, legal, and technical difficulties. The paramount problem is that *main players are not interested in constraining themselves with commitments.* If lessons and experiences are to be drawn from arms control and disarmament, it is less about the technical design and the practical implementation of agreements, but primarily on the political process that preceded them. The lessons to learn from nuclear disarmament are particularly instructive. Not only are they enormously vast, but they also had (at the outset) to deal with the complexity of a new type of technology, with impacts, further developments, and geopolitical significance unknown before.

## Comprehensive Approaches vs. Pragmatic Steps

One of the most important lessons from nuclear arms control is that very comprehensive and ambitious approaches are no promising starting point. Pragmatic and limited steps, on the other hand, can achieve significant progress in the long run.

In June 1946, when the U.S. was still the only state with nuclear weapons, it presented the *Baruch Plan* at the United Nations. It was a uniquely ambitious proposal of nuclear disarmament. The U.S. agreed to decommission all their nuclear weapons and to hand over nuclear technology for civilian use if all other nations also renounce to nuclear weapons and agreed to a strict system of inspection and sanctions.[12] In

[11] Wicki-Birchler, D. 2020.

[12] Gerber 1982.

other words, the U.S. proposed the multilateralization of the entire nuclear sector and a comprehensive ban on nuclear weapons, as it was proposed under completely different conditions and modalities more than half a century later with the Treaty on the Prohibition of Nuclear Weapons.[13] The 1946 Baruch Plan failed because of opposition from the Soviet Union, which shortly thereafter put into service its own first nuclear weapons. A decade of intensive nuclear armament followed and then decades of small steps in arms control.

In 1962, the Cuban Missile Crisis brought the world to the brink of nuclear war. One positive outcome was the *Hot Line Agreement* between the United States and the Soviet Union (1963), which established direct communications between Moscow and Washington to avoid in future misperceptions and undesirable escalations (1963). In the same year, the *Treaty on the Prohibition of Nuclear Weapons Tests in the Atmosphere, in Outer Space, and Underwater* came into being. It was followed by the ban on deploying nuclear weapons in space (1967), the *Nuclear Weapons Free Zone in Latin America* (1967), the *Nuclear Non-Proliferation Treaty* limiting the possession of nuclear weapons to the then five nuclear-weapon states and other provisions (1968), the *Soviet-U.S. Strategic Arms Limitation Talks SALT* began in 1969 (until 1979), the *Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Sea-Bed and the Ocean Floor*... (1971), etc.[14]

The point is not to retell the story of nuclear disarmament, but to highlight the many steps that did not follow a preconceived blueprint but over time led to a global regime that limited and outlawed nuclear weapons. The history of arms control also shows that a wide variety of actors played a role and that setbacks were by no means rare.[15]

For the cyber domain it is arguably more promising to reach out for achievable results, to seek the low hanging fruits, and to prepare for a long process. Working on a comprehensive convention banning the use, possession, development, etc. of cyberweapons, equipped with a strict verification system, appears to be an unpromising endeavor or starting point at least.[16]

Pragmatic steps are not easy. They require concrete, politically achievable and substantive content, and much analytical acuity regarding the geopolitical

[13] Borrie et al. 2018. Ruff 2018.

[14] Meyer, P. 2011: 25.

[15] Nye 2013.

[16] Futter 2020.

environment. Out-of-the-box thinking coupled with solid pragmatism is required. Studying the history of arms control and disarmament does not allow to discover replicable solutions. It will, however, help to identify promising tracks. Reference to precedents have in political processes the important advantage of credibility because they have been agreed to before and because there is an observable practice.

What disarmament and arms control measures could be tested and discussed?

## No-first-use Policy

A general ban on the use of cyberweapons is for many reasons unrealistic. One is that an attacked state wants to be able to retaliate in cyberspace, which reduces the risk that kinetic means of warfare are used at an early stage to exercise the right to self-defense under Article 51 of the UN Charter. It is also difficult to imagine how effective protective measures against cyberattacks can be developed without mastering offensive cyber capabilities.

Under these conditions, banning the first use of cyberweapons appears to be a realistic and substantial goal. The first-use ban is not weakened if states continue to have offensive cyber-capabilities. Possession of cyberweapons can deter first use. There is an important precedent for this: the 1925 Geneva Protocol banned the use of chemical and biological weapons, but not their production and deployment.[17] The fear of retaliation, which remained possible, has certainly deterred the use of such weapons at least as much as the legal prohibition itself, including during World War II in Europe, when both sides had important chemical weapons arsenals.

A first use ban on cyberweapons is by no means easy to achieve, even if the political will were there. It will require hard negotiations to define what constitutes first use for instance. Not every use of harmful algorithms must be considered as first use for the purposes of an arms control treaty, and little would be gained by leaving this judgement to individual states.

[17] United Nations. Office for Disarmament Affairs. 1925 Geneva Protocol.

## De-targeting

International humanitarian law prohibits attacks on civilian persons and facilities. However, there may be an interest in exempting military targets from attack as well, particularly targets that carry a great risk of escalation, that may lead to dangerous reactions, or cause great damage. Such targets include nuclear weapons infrastructure, military warning systems, or military command and control facilities. The U.S.-China Cyber Agreement follows this logic.[18]

An arms control agreement could define targets to be exempt from cyberattacks. Again, this would require hard negotiations that may follow very different methodological approaches (general definition of prohibited targets, notification of specific targets to be exempted, etc.). Because geopolitical and technological developments have an impact on what constitutes a critical target, it is not very useful to regulate de-targeting once and for all. A continuous exchange could be necessary, which - if well designed - would also have a confidence-building effect. There is little experience with de-targeting, which makes innovative approaches necessary.

## Non-proliferation

To strengthen the common goals of a treaty and to make it attractive to additional parties, many disarmament and arms control agreements have provisions on the non-proliferation of weapons and technologies.

The paradigmatic model is the already mentioned Treaty on the Non-Proliferation of Nuclear Weapons NPT. The NPT contains provisions on disarmament, non-proliferation, peaceful uses of nuclear energy, etc. In other words: not only prohibitions but incentives as well. However, the NPT is not a very suitable model because it created different rights and obligations for nuclear-weapon states and non-nuclear-weapon states, which has continuously led to disagreement among the parties. Another model is the Nuclear Suppliers Group NSG, which is a strategic export control regime. The NSG also aims at nuclear non-proliferation but is based on informal cooperation and has no international treaty as its basis. One of the limitations of the NSG and other strategic export control regime is that it is a regime of technologically powerful states

[18] Rollins et al. 2015.

against others. This may work for nuclear technology, but it is certainly not suitable for cyber technology, which is difficult to control and easily accessible.

Strategic export controls would be a most difficult undertaking in the area of cybertechnology because of its strong dual-use nature and because of the predominant role of the private sector. Everything looks like intelligence agencies will continue to be very active in this field, and states will intervene individually or in ad hoc cooperation against the proliferation of harmful cyber technology.

## Confidence Building Measures

Confidence-building measures (CBMs) are parts of many arms control and disarmament agreements. They are important to strengthen the functioning of the agreements. As low-threshold instruments, CBMs do not necessarily require a legally binding form. The novelty and the many uncertainties with cybertechnology suggest that CBMs can be of great importance.[19]

Experience with CBMs is vast, ranging from early forms of cooperation between the superpowers during the Cold War, the implementation of arms control and disarmament conventions to the experience of CSCE/OSCE during the closing stages of the Cold War and beyond. There are studies on this topic by ICT4Peace, among others.[20]

With cooperative approaches such as CBMs, it is possible to create a common understanding of threats and challenges, as well as transparency about military activities and intentions. CBMs usually allow open discussion regarding fears and perceptions. Depending on their design, CBMs foster personal relationships between protagonists. Viable personal contacts have proven useful in crisis situations and for de-escalation.

## Prohibition to Develop certain Dangerous Technologies

Would it be worth examining the possibility of banning the development of particularly dangerous cybertechnologies in an agreement? Because the targeted technologies

[19] Meyer, P. 2011: 26.

[20] Stauffacher & Kavanagh 2013.

might not exist yet and could hardly be specified technically, such a ban would have to aim at specific harmful effects.

Prohibitions on weapons systems that have not even been developed are practically non-existent. The example of the Baruch Plan and the Soviet response to it demonstrate how difficult such a ban is. One precedent is the Environmental Warfare Convention ENMOD.[21] It prohibits the development and use of environment-altering techniques as weapons of warfare, such as artificially generated tsunamis, volcanic eruptions, hurricanes, earthquakes etc. Both the United States and the Soviet Union did research on such technologies until the 1970s. They never entered service as military means of combat. It is controversial what role the ENMOD convention had in this process. Was it the prohibition of the use of environment-altering techniques under ENMOD that resulted in these weapons developments not being pursued? Or are there other reasons (technical problems, difficulties to include in military strategies, lack of predictability of their effects, incompatibility with international humanitarian law, etc.)? Despite those open questions a preemptive ban on particularly dangerous cyber technologies seems well worth examining and could in the long term contribute to the stigmatization of cyber weapons.

Although a different issue, the discussions on prohibiting or restricting lethal autonomous weapon systems are worth to be studied.[22] These discussions take place under the UN Convention on Certain Conventional Weapons CCW, a convention at the intersection of international humanitarian law and disarmament.[23] Likewise of interest are the unfolding discussions on the military use of artificial intelligence.

## Cooperation

Disarmament and arms control agreements often have provisions for cooperation among states parties. In some agreements, their purpose is to prevent impeding legitimate activities, such as the civilian use of nuclear energy, access to industrial chemicals that can be precursors to chemical weapons, etc.

[21] United Nations. Office for Disarmament Affairs. *Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD).*

[22] Surber 2018.

[23] United Nations. Office of Disarmament Affairs. *The Convention on Certain Conventional Weapons*.

In the cyber domain, there is much room for innovative solutions to increase the benefits of treaty accession. In any case, a duty to assist attacked treaty states is worth examining in the context of an arms control agreement. It would not only be an incentive for states parties but would also make offensive cyber operations riskier and thus less attractive for potential attackers. Forms of cooperation against third parties (terrorists, organized crime) are also conceivable and would provide an additional incentive to join an agreement.[24]

## Regional Agreements

Regional agreements have been and are important in the field of arms control and disarmament. Prominent examples are nuclear weapon-free zones or demilitarized zones. Have regional agreements lost their importance because cyberspace is everywhere and can hardly be assigned geographically? This is not the case. Regional arrangements have great potential to counter cyber challenges as well. Although cyberspace is global, cyber arms race and the use of offensive cyber capacities can well emerge from regional dynamics. Existing forms of regional cooperation (ASEAN, AU, OAS, OSCE, etc.) are therefore an excellent basis for pragmatic progress, also because discussions on cyber risks and on CBM's are already taking place in many regional organizations.

## Verification

In no other area of international law is the verification of treaty provisions as central as in arms control and disarmament. Those who take on far-reaching obligations in this area also want to be certain that the other parties to the treaty will abide by the provisions (the core provisions of the agreements are verified, whereas the term review is used to assess the functioning of the agreements as instruments).

The range of possible verification measures is broad, ranging from analyzing open sources to notifications and inspections up to permanent monitoring. Appropriate verification is probably the most difficult element of an arms control agreement in the cyber domain.

[24] Nye 2013.

Political restraint and technical difficulties are no reason to forgo verification. It is certainly easier to reach an agreement without verification in the first place, but the absence of effective verification measures can weaken the appeal of an agreement and become a stumbling block for its proper implementation.

### Enforcement and Sanctions

Contracting parties have a common interest in ensuring that treaty violations are excluded as far as possible and that, in the event of violations, compliance is restored. Sanctions are a difficult area and can quickly lead into extensive political disputes.

For the cyber domain, it makes sense to design innovative forms of sanctions. It is not about major violations that threaten peace and international security and prompt the UN Security Council to act, but about concrete measures to take in response to violations of commitments.

## 5. Outlook

Arms control and disarmament in cyberspace is possible. They can contribute to stability, reduce the risk of war breaking out, or limit the impact of an armed conflict. There is extensive experience from arms control and disarmament, both in terms of the political process and specific solutions to individual challenges.

A comprehensive arms control agreement in the realm of cyberspace is hardly realistic in the foreseeable future. On the other hand, it is worthwhile to strive for progress with small steps, as has been successful in nuclear arms control. Innovative yet pragmatic solutions and goals are particularly important. Geopolitical factors and technical developments will always play an important role.

The Geneva Conference on Disarmament is the global forum for negotiations on arms control and disarmament and is therefore predestined to play an important role. However, the now sixty-year history of the Geneva Conference on Disarmament has shown that success is only possible if the key players are willing to negotiate solutions. In other words, the U.S., China, Russia, and others must take a leading role or at least be able to agree on core objectives.

This in no way means that other states, multilateral organizations, think tanks, academia, and non-governmental organizations should be inactive. On the contrary, it is important that a broad discussion takes place, and that political pressure is generated. It will also be important that novel and forward-looking models are developed and put up for discussion, knowing that the best knowledge and the most brilliant idea will not achieve a breakthrough without the political will and the willingness to negotiate on the part of the key players.

## Literature

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

Benjamin, J., & Haney, M. (2020). *Non-proliferation of Cyber Weapons*. In 2020 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 105-108). IEEE.

Benincasa, E. (2021). The Case for Cyber 'Disarmament'in the European Union. The International Spectator, 56(1), 39-54.

Board, D. I. (2019). *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense: Supporting Document*. United States Department of Defense.

Body, N. S. (2021). *The Evolution of the UN Group of Governmental Experts on Cyber Issues*. New Conditions and Constellations in Cyber, 15.

Bolton, M. (2016). *Time for a discursive rehabilitation: A brief history of general and complete disarmament. Rethinking General and Complete Disarmament in the Twenty-First Century.* New York: UN Office for Disarmament Affairs.

Borghard, E. D. & Lonergan, S. W. (2018). *Why Are There No Cyber Arms Control Agreements?* Council on Foreign Relations, 16. Computer Security Resource Center CSRC. (https://csrc.nist.gov/glossary)

Borrie, J., Spies, M., & Wan, W. (2018). Obstacles to understanding the emergence and significance of the treaty on the prohibition of nuclear weapons. *Global Change, Peace & Security*, *30*(2), 95-119.

Dittrich, P. J. (2017). *More Security in Cyber Space: The Case for Arms Control.* Federal Academy for Security Policy. Security Policy Working Paper, No. 9/2017.

Eidg. Departement für auswärtige Angelegenheiten EDA (2022): *Strategie Rüstungskontrolle und Abrüstung 2022-2025.* Bern.

Futter, A. (2018). *Hacking the bomb: cyber threats and nuclear weapons*. Georgetown University Press.

Futter, A. (2020). *What does cyber arms control look like? Four principles for managing cyber risk*. European Leadership Network.

Gerber, L. G. (1982). *The Baruch Plan and the origins of the Cold War*. Diplomatic History, 6(1), 69-96.

Henderson, C. (2021). *The United Nations and the Regulation of Cyber-Security.* In Research Handbook on International Law and Cyberspace. Edward Elgar Publishing.

Herzog, S. (2011). *Revisiting the Estonian cyber-attacks: Digital threats and multinational responses*. Journal of Strategic Security, 4(2), 49-60.

Joyner, D. (2020). *Strategic Trade Controls*. Research Handbook on Arms Control Law Edward Elgar Publishing, University of Alabama Legal Studies Research Paper, (3599357).

Kello, L. (2018). *Cyber Threats*. In The Oxford Handbook on the United Nations.

Klimburg, A. (Ed.) (2021). *New Conditions and Constellations in Cyber*, The Hague Centre for Strategic Studies.

Kittichaisaree, K. (2017). *Public international law of cyberspace* (Vol. 32). Cham: Springer.

Lauber, J. & Eberli, L.: *From Confrontation to Consensus: Taking Stock of the OEWG Process*. In Klimburg 2021: 31-39.

Meyer, P. (2011). Cyber-security through arms control: an approach to international co-operation. The RUSI Journal, 156(2), 22-27.

Meyer, P. & Stauffacher, D. (2021): *ICT4Peace and the United Nations Open-Ended Working Group on International Cybersecurity (UN OEWG) 2019-2021*. ICT4Peace Foundation. Geneva 2021.

Mačák, K. (2021). *Unblurring the Lines: Military Cyber Operations and International Law*. Journal of Cyber Policy, 1-18.

Microsoft International Cybersecurity Norms (https://query.prod.cms.rt.mictrosoft.com/cms/api/am/binary/REVmcd)

Milmo, D. (2022). *Anonymous: The Hacker Collective that has Declared Cyberwar on Russia*. The Guardian, 28.2.2022.

Monte, M. (2015). *Network Attacks and Exploitation: A Framework*. John Wiley & Sons.

Ning, H., Ye, X., Bouras, M. A., Wei, D. & Daneshmand, M. (2018). *General Cyberspace: Cyberspace and Cyber-enabled Spaces.* IEEE Internet of Things Journal, 5(3), 1843-1856.

Nye Jr, J. S. (2013). *From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future*? Bulletin of the Atomic Scientists, 69(5), 8-14.

Pearson J. & Landay J.: *Cyberattack on NATO Could Trigger Collective Defence Clause*. Reuters, February 28, 2022.

Rid, T. & McBurney, P. (2012). *Cyber-weapons*. The RUSI Journal, 157(1), 6-13.

Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2018). *An Introduction to Cyber Peacekeeping*. Journal of Network and Computer Applications, *114*, 70-87.

Rollins, J. W., Lawrence, S. V., Rennack, D. E., & Theohary, C. A. (2015). *US-China Cyber Agreement.* Library of Congress, Congressional Research Service.

Ruff, T. (2018). *Negotiating the UN Treaty on the Prohibition of Nuclear Weapons and the Role of ICAN*. Global Change, Peace & Security, 30(2), 233-241.

Rumer, E. (2018). *A farewell to arms… Control*. Carnegie Endowment for International Peace, 17(April), 2018.

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

Schmitt, M. N. (2012). *International Law in Cyberspace: The Koh Speech and the Tallinn Manual Justaposed.*

Starodubtsev, Y. I., Balenko, E. G., Vershennik, E. V., & Fedorov, V. H. (2020, October). *Cyberspace: Terminology, Properties, Problems of Operation*. In: 2020 International Multi-Conference on Industrial Engineering and Modern Technologies: 1-3.

Stauffacher D. & Kavanagh C. (2013): *Confidence Building Measures and International Cyber Security*. ICT4Peace Foundation: Geneva.

*Strategie Rüstungskontrolle und Abrüstung 2022-2025*, Eidgenössisches Departement für auswärtige Angelegenheiten EDA, Bern 2022.

Surber, R. (2018). *Artificial intelligence: autonomous technology (AT), lethal autonomous weapons systems (LAWS) and peace time threats*. ICT4Peace Foundation and the Zurich Hub for Ethics and Technology (ZHET) p, 1, 21.

Svenmarck, P., Luotsinen, L., Nilsson, M., & Schubert, J. (2018, May). Possibilities and Challenges for Artificial Intelligence in Military Applications. In Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision-Making Specialists' Meeting (pp. 1-16). Neuilly-sur-Seine France.

Tiirma-Klaar, H.: *The Evolution of the UN Group of Governmental Experts on Cyber Issues from a Marginal Group to a Major International Security Norm-Setting Body*. In Klimburg 2021: 15-29.

Tsagourias, N., & Buchan, R. (Eds.). (2021). *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing.

United Nations General Assembly Doc. A/66/359 *International Code of Conduct for Information Security* (2011)

United Nations General Assembly Doc A/70/174 A/70/174 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (2015)

United Nations Office for Disarmament Affairs (2017). *Civil Society and Disarmament. Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary.*

United Nations Office for Disarmament Affairs. *1925 Geneva Protocol. Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare (*https://www.un.org/disarmament/wmd/bio/1925-geneva-protocol/*)*

United Nations Office for Disarmament Affairs. *Treaty on the Non-proliferation of Nuclear Weapons (NPT)*. (https://www.un.org/disarmamaent/wmd/nuclear/npt/)

United Nations Office for Disarmament Affairs. *Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD). (https://www.un.org/disarmament/enmod/)*

United Nations Office of Disarmament Affairs. *The Convention on Certain Conventional Weapons*. (https://www.un.org/disarmament/the-convention-on-certain-conventional-weapons/)

Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime? *International Cybersecurity Law Review*, *1*(1), 63-72.

Ziolkowski, K. (2013). *Confidence Building Measures for Cyberspace*. Peacetime Regime for State Activities in Cyberspace, 533.

# About ICT4Peace Foundation

ICT4Peace is a policy and action-oriented international Foundation. The purpose is to save lives and protect human dignity through Information and Communication Technology. Since 2003 ICT4Peace explores and champions the use of ICTs and new media for peaceful purposes, including for peacebuilding, crisis management and humanitarian operations. Since 2007 ICT4Peace promotes cybersecurity and a peaceful cyberspace through inter alia international negotiations with governments, international organisations, companies and non-state actors.

The ICT4Peace project was launched with the support of the Swiss Government in 2003 with the publication of a book by the UN ICT Task Force on the practice and theory of ICT in the conflict cycle and peace building in 2005 and the approval of para 36 of the Tunis Commitment of the UN World Summit on the Information Society (WSIS) in 2005.

ICT4Peace Website: www.ict4peace.org

ICT4Peace Academy - www.academy.ict4peace.org

ICT4Peace Publications: www.ict4peace.org/publications

ICT4Peace on Twitter - www.twitter.com/ict4peace

ICT4Peace on Facebook - www.facebook.com/ict4peace

ICT for peace foundation