ICT for peace foundation

Can arms control and disarmament contribute to a secure cyberspace?

By Martin Dahinden, ICT4Peace

Abstract

The ongoing 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. Experience from arms control is highly relevant to the cyber domain, both for understanding the policy process and as an inspiration for solutions. Existing arms control arrangements 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 hazardous technologies, cooperation for peaceful purposes, regional arrangements, verification, or enforcement. 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. Switzerland with its international credibility, experience and technical know-how is particularly well suited to play an active role, including during the forthcoming two years as a non-permanent member of the UN Security Council

Introduction

Cyberweapons exist and are spreading rapidly (The world is witnessing a rapid proliferation of cyberweapons and a real arms race is taking place in cyberspace. The risks to international stability are considerable, but also difficult to fully grasp. This should not be obscured by the war in Ukraine, which is largely fought with conventional means.

Arms control and disarmament in the cyber domain have so far played a subordinate role in the discussion. This is remarkable because arms control was of enormous importance for global stability during the Cold War. This experience is important for the cyber domain, both to understand the political process and as a source of inspiration for concrete solutions.

Like cyber technology today, nuclear technology was once completely novel and difficult to assess in terms of its impact. Comprehensive agreements failed at first. In contrast, limited and pragmatic measures led over time to a comprehensive arms control regime. Today, this approach is also promising for the cyber domain.

Progress will depend primarily on whether the key political actors (USA, China, Russia) can agree on common goals. At first glance, the political climate is unfavourable. However, arms control during the Cold War came into being precisely at the height of international tensions after the Cuban Missile Crisis.

Switzerland is well placed to play a useful and active role in arms control and disarmament initiatives in cyberspace. It does not belong to one of the political blocs and has a worldwide network of foreign policy relations. In addition, it has extensive experience in confidence building, arms control and disarmament. Switzerland has the indispensable technical expertise, for example in the National Cyber Security Centre (NCSC), in the army and in the federal intelligence service.

The Swiss Federal Department for Foreign Affairs (FDFA) has expertise in the area of international security policy and in the special Ambassador for digitalisation. If necessary, expertise from universities, such as ETH, and the private sector can also be mobilised within the framework of a negotiation process. With the Conference on Disarmament and a large number of institutions in the field of information and communication technologies, Geneva is a global hub that is a natural fit. Political initiatives in this area are also aligned with the broader objectives of Swiss foreign and security policy. The upcoming two years as a non-permanent member of the UN Security Council offer a variety of opportunities and a good starting point to launch ideas, to identify and exploit promising avenues.

Cyberspace and cyber weapons

Most states have recognised the dangers of offensive cyber capabilities for their national security, although cyber attacks cannot cause the same damage as kinetic attacks. The Swiss Federal Council'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 armament goods".1

Cyber weapons are more complex than anything arms control and disarmament have ever dealt with. Cyberspace as a sphere is already elusive. It is the virtual space created by the global interconnection of ICT infrastructure that allows information flows to circulate without geographical distance or other traditional physical constraints.2 As a virtual sphere, cyberspace is largely operated and used by the private sector.

Cyberweapons are computer codes that can threaten and cause physical, functional or psychological damage to systems, structures or living beings.3 The spectrum is broad. At the more benign end is malicious software (malware) that affects systems from the outside but does not technically penetrate, for example software that generates massive data traffic to overload servers. At the other end of the danger spectrum is malware that penetrates even protected and physically isolated systems and inflicts direct damage, not only to data, but possibly also with major physical effects, for example by destroying military installations, weapons systems or infrastructure (Computer Network Attacks CNA).

Armament in cyberspace takes place as a build-up of offensive (and defensive) capabilities. No tangible, countable and controllable objects are created, as is the case with conventional armed forces and kinetic weapons (tanks, missiles, submarines, etc.). Accordingly, it is extremely difficult to quantify military strength in the cyber domain with any degree of reliability.4 These are clear indications that the experience gained from disarmament and arms control cannot be transferred to the cyber domain without in-depth examination. This important aspect is also pointed out in the Swiss Federal Council's Arms Control and Disarmament Strategy 2022 - 2025.5.

Possibilities and limits for arms control and disarmament in cyberspace

Nevertheless, cyber weapons and military capacities in the cyber domain have characteristics that make them predestined for arms control and disarmament. Armament with offensive cyber capabilities can endanger political balances and can - intentionally or unintentionally - lead to an escalation that is not limited to the cyber domain but can also include kinetic means of combat. The geopolitical context plays an important role, for example the rivalry between the USA and China. The use of cyber weapons can cause great damage. Less clear (and transparent) are the costs of the arms race in cyberspace, which has often been an incentive to agree on limitations for military capabilities.

Also evident are the difficulties and obstacles to reaching viable agreements. Verification in particular is difficult to imagine in the cyber domain. It could expose one's cyber capabilities and sensitive technical information, and make gaps in defensive capabilities visible to a potential adversary.

The technology of cyber warfare is only in its infancy. In the past, it was hardly possible to ban or restrict weapons systems while they were still in the development phase.

For offensive cyber operations, not only states (armed forces) come into question, but also private, i.e. non-state, actors. This is relevant because it goes beyond the logic of traditional arms control agreements.6

This complicated situation explains why disarmament and arms control have been neglected so far and why international efforts have focused on international humanitarian law and norms of good governance, which are much less intrusive and mandatory.

Despite these factual obstacles, the main problem for the slow progress is not primarily conceptual, legal and technical difficulties. It is the lack of interest of the main actors to tie their hands with mandatory agreements.

It is precisely for this reason that the political process that once led to successful arms control is instructive. The most important lesson is that ambitious and comprehensive approaches are not a good starting point. Pragmatic and limited steps, on the other hand, promise good progress even in the long run. It is advisable to reach for achievable results, the low hanging fruits, and to prepare for a long process in the same time.7

What concepts and building blocks from the fields of disarmament and arms control measures can we draw inspiration from?8

A general ban on cyber weapons is not realistic in the foreseeable future. Even a general ban on the use of cyber weapons is unrealistic because in the event of a cyber attack, the attacked state will want to be able to retaliate in cyberspace, which might reduce the risk that a state attacked with cyber weapons will quickly switch to using kinetic means to exercise its right to self-defence under Article 51 of the UN Charter. Moreover, it is difficult to imagine that effective protective measures against cyber attacks can be developed without mastering offensive cyber capabilities.

Under these conditions, the ban on the first use of cyber weapons appears to be a realistic and at the same time significant goal in terms of security policy. In this logic the possession of cyber weapons can does not weaken but can thus deter first use.

An arms control agreement can define objects that are exempt from cyber attacks (de-targeting) - not only civilian targets, as required by international humanitarian law anyway, but also military targets with great potential for escalation, for example, nuclear weapons infrastructure, military warning systems, etc. The bilateral U.S.-China Cyber Agreement follows this logic.9

Many disarmament and arms control measures contain provisions on the non-proliferation of weapons and technology. In principle, this is also conceivable for cyber technology that can be used for military purposes. However, this is a difficult undertaking because of the strong dual-use character and the large role of the private sector. Little is known about international agreements or arrangements on the non-proliferation of sensitive digital technology.10 Everything indicates that intelligence services are increasingly active in this area and that states individually or jointly intervene against the proliferation of undesirable technology.

Confidence-building measures (CBMs) are important to strengthen the functioning of agreements. They are low-threshold instruments that need not be legally binding. The novelty and unpredictability of cyber technology suggests that great importance should be given to confidence-building measures, drawing on the extensive experience from previous disarmament and arms control agreements. There are a lot of studies on this including by ICT4Peace Foundation.11

Would it be possible to prohibit the development of particularly dangerous cyber technology in an agreement? Because the specific technologies are not yet known (and therefore cannot be specified), the starting point would have to be the prohibition of certain harmful effects. A precedent for this is the environmental warfare convention ENMOD, which prohibits the use of environment-changing technologies as weapons of warfare (artificially generated earthquakes, volcanic eruptions, hurricanes, tsunamis, etc.).12 Similarly, a preventive ban on particularly dangerous cyber technologies is worth examining and could contribute to the stigmatisation of cyber weapons in the longer term.

Disarmament and arms control agreements often have provisions for cooperation among states for peaceful purposes, for example for the peaceful use of nuclear technology or chemical substances. The aim is not to discourage states from joining an agreement out of fear to hamper legitimate activities. In the cyber domain, there is much room for innovative solutions. It would be worth examining, for example, the support of attacked states, which not only contributes to the attractiveness of an agreement, but also increases the risk for possible attackers.13

Regional agreements have always been important for arms control and disarmament. Prominent examples are nuclear weapon-free or demilitarised zones. Have regional agreements lost their importance because cyberspace is everywhere and can hardly be clearly assigned geographically? That would be a false conclusion. Regional agreements have great potential in the cyber domain as well. Cyber arms race can emerge from a regional dynamic, and existing forms of regional cooperation (ASEAN, OAS, OSCE, etc.) are good formats for pragmatic progress. Discussions on cyber threats are already taking place in many regional organisations.

In hardly any other area the verification of treaty provisions is as central as in arms control and disarmament. If a state takes on far-reaching obligations, it wants certainty in return that the other parties will also fulfil the obligations. Effective verification is probably the most difficult element of an arms control agreement in the cyber domain. But there is a large pool of solutions and room for innovative approaches as well.

Political resistance and technical difficulties are no reason to refrain from verification. The absence of effective verification measures reduces the attractiveness of an agreement and can later become a stumbling block if disagreements and accusations cannot be verified.

Parties to an agreement have a common interest in ensuring that violations are excluded as far as possible and that, in the event of violations, the lawful state is restored. This means sanctions. They are a difficult area and can quickly lead into extensive political disputes. For the cyber area, it makes sense to design innovative forms of sanctions.

Outlook

Arms control and disarmament in cyberspace are possible. They can make a decisive contribution to stability, reduce the risk of war breaking out and limit the impact of conflicts. There is extensive experience from arms control and disarmament to date, both on the political process and on specific solutions. But it has not yet been tapped and discussed in depth.

It is crucial that the US, China, Russia and others assume their responsibilities and play a leading role. But this in no way means that other states, multilateral organisations, think tanks, academia and non-governmental organisations should be inactive. On the contrary: it is important that a broad discussion takes place and political pressure is created. It is also important to have novel and forward-looking models and approaches - knowing that the most brilliant ideas will not achieve a breakthrough if the political will and the willingness to negotiate on the part of key actors are lacking.

Endnotes

1 EDA 2022: 28.
2 Definition vgl.: Ning et al. 2018; Starodubtsev et al. 2020: 1–3.
3 Rid & McBurney2012.
4 Borghard & Lonergan 2018.
5 a.a.O.
6 Wicki-Birchler, D. 2020.
7 vgl. Futter 2020.
8 Dahinden 2022.
9 Rollins et al. 2015.
10 Buzatu 2022
11 Stauffacher D. & Kavanagh C. 2013.

12 United Nations. Office for Disarmament Affairs. *Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD).*
13 Nye 2013.

Bibliography

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). *Nonproliferation 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)

Buzatu, Anne-Marie (2022). *From Boots on the Ground to Bytes in Cyberspace.* ICT4Peace Foundation.

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, expected 2021), 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. and Eberli, L.: *From Confrontation to Consensus: Taking Stock of the OEWG Process*. In Klimburg 2021: 31–39.

Meier, 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.microsoft.com/cms/api/am/binaryREVmed)

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. *Treaty on the Nonproliferation of Nuclear Weapons (NPT).* (https://www.un.org/disarmament/wmd/nuclear/npt/)

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.

****

Dr. Martin Dahinden is Vice-Chairman of ICT4Peace, a former Swiss Ambassador to the US, former Head of the Swiss Development Agency (SDC) and a lecturer at the University of Zurich.

This Text has been published first in German language on 16 December 2022 by stratos - Military Science Journal of the Swiss Armed Forces (2-22) https://www.vtg.admin.ch/de/organisation/kdo-ausb/hka/milak/mehr-zur-milak/stratos/zeitschriften.html

A comprehensive policy brief in English by Martin Dahinden was published by ICT4Peace on 13 April 2022 under the title How can Arms Control and Disarmament Contribute to a Secure Cyberspace? https://ict4peace.org/activities/how-can-arms-control-and-disarmament-contribute-to-a-secure-cyberspace/