

Appendix

Challenges for Cyber Arms Control: A Qualitative Expert Interview Study

Thomas Reinhold · Helene Pleil · Christian Reuter

1 Overview of the Challenges to Establishing an Arms Control Agreement in Cyberspace

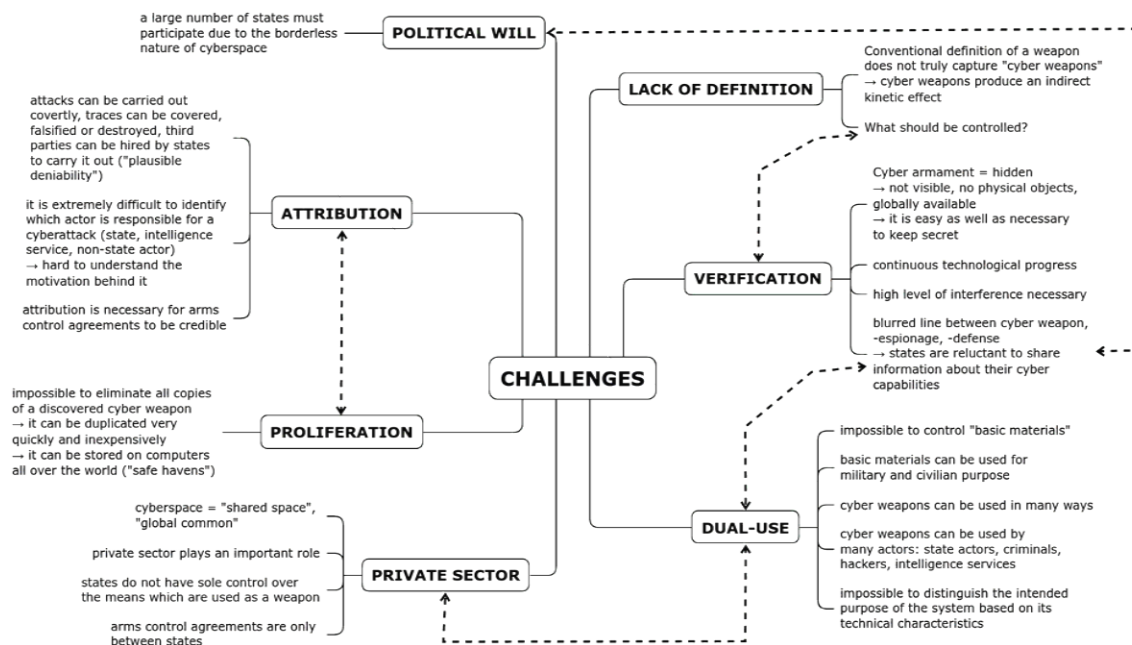


Fig. 2: Overview of the challenges to establishing an arms control agreement in cyberspace.

The dashed lines represent particularly strong connections between the respective aspects.

Source: Own illustration.

2 Interview Guidelines

Remarks: We used the conducted interviews for two different research projects. The second research project analyzes similarities and differences between arms control for chemical weapons and cyberweapons. The interview guideline scheme therefore sometimes refers to chemical weapons. The guidelines below are a shortened version, reduced to the aspects concerning this research paper.

The role of Meaningful Human Control (MHC) in autonomous military systems against the background of an actor-systematizing view.

In our work, we deal with the concept of MHC in autonomous military systems. Here, I am mainly interested in how different actors define MHC for themselves and what implications this may have for a possible implementation.

The starting point is that in the debate about MHC there are different ideas about what human control means or should mean – this is not least an obstacle to agreeing on international arms control rules. Nevertheless, numerous states are already developing weapon systems with autonomous or semi-autonomous functions – both within the EU and within NATO, systems are currently being developed that pose a challenge to human control – a prominent example here would be Future Combat Air Systems (FCAS). With this in mind, I am initially interested in:

Introductory question What does MHC imply for you and what role do you think does it play in the context of autonomous military systems? Would you say MHC and the autonomization of autonomous systems or autonomous weapon systems represents a contradiction?

The development of autonomous military systems involves a whole range of different actors from civil society, research and development, and business and industry.

Question 1 How would you describe the current 1) technical debate on the responsible and ethical use of AI-driven autonomous systems? What are core aspects that you would highlight here? How does it differ from the 2) policy debate?

Demand I How would you see the interaction of different stakeholders, for example from civil society, academia, military, or policy, in the implementation of MHC in autonomous systems

development to date? Whose role in Research and Development do you rank as the most influential and why?

Demand II How useful would you consider a multi-stakeholder approach to the development of autonomous systems? Which stakeholders should definitely be brought in?

In our research, we examine the websites of arms-producing corporations for narratives on MHC in autonomous systems. Thereby the impression is created that the defense industry promotes the use of autonomous systems in a military context with many different narratives – one example is that operating in a “contested battlefield” or “contested environment” makes it indispensable for military to deploy a “human-machine team”. Autonomous systems are thus promoted as necessary in order to be able to act efficiently and quickly and are thus seen as the future of warfare. With these narratives, one quickly gets the impression that the industry side is quickly falling into technical discussions with little consideration of political and ethical aspects.

Question 2 I would be interested in your (critical) assessment of this. Do you see an implementation of MHC in the development of autonomous weapons by the defense industry?

Inquiry What do you think would have to change in the status quo to establish a broader debate on MHC in the defense industry as well? Do you have any examples?

Question At the same time, however, companies also emphasize the need for a so-called human-machine team, in which the AI or AI-controlled autonomous system acts primarily as a support for humans. In this context, I brought a statement/slogan that crossed my way while analyzing the website of a defense company that develops autonomous systems. It says: “The Future of Autonomy Isn’t Human-Less. It’s Human More.” How would you evaluate this statement in the MHC context (critically)?

Question 3 What are technical and operational parameters that autonomous systems must meet for responsible and ethical use?

Demand II How can technical design of autonomous military systems suggest and facilitate accountability? What might this look like specifically in future systems?

Demand III Can you give concrete examples where it is possible to speak of a successful implementation of MHC?

Question 4 Keywords *human-in-the-loop*, *human-on-the-loop* and *human-out-of-the-loop*: What role will autonomous military systems play on the *battlefield of the future*? What advantages or risks do you see in this? And how many humans will still be involved in warfare in the future?

Question 5 That are all the questions I have. In your opinion, are there any important aspects that we have not yet addressed?

Question 6 Who else do you think we should ask about this?

Why this research question at all?

On the one hand: In various papers or lectures, one hears again and again about (possible) parallels between the chemical weapons domain and the cyberweapons domain.

Parallels can be observed especially in the challenges that these types of weapons pose to arms control: dual-use and proliferation play a major role in both domains, the weapon itself is difficult to define, constant technological progress is expected in the domain and, above all, the type(s) of weapon puts previous verification mechanisms of “classical” arms control to the test or shows that they are not applicable to the domain.

On the other hand: chemical weapons agreement is a great success of arms control, with (almost) worldwide agreement, independent verification regime, surviving crises for arms control (like former US President Trump).

Therefore, I came to the idea that it would be useful to analyze to what extent similarities and parallels exist between the two domains and whether and if so, to what extent lessons can be drawn from the past of the Chemical Weapons Convention for a possible cyber arms control.

Question 7 In your opinion, what are the main challenges for a cyber arms control agreement? If cyber arms control is generally not possible, why do you think so? What are in your eyes the unsolvable problems, so that cyber arms control is impossible?

In the chemical weapons domain, similar challenges (or challenges that at least appear similar) to arms control agreements could be observed as currently in the cyber domain. However, new ways of verification have been found to overcome these challenges, in the form of 1) lists of banned chemicals, 2) inspections by an independent specially created verification regime, and 3) through the General-Purpose Criterion, which focuses the agreement or definition of a chemical weapon on the purpose or intent of its use.

Question 8 To what extent could such measures of verification be effective for a cyber arms control agreement? To what extent would there be a need for adaptation here? At the heart of the Chemical Weapons Convention is the “General Purpose Criterion” – would such a focus on the purpose or intent of the use of certain means be conceivable or useful for a possible cyber arms control agreement? (Given the difficulty of defining a cyberweapon and its dual-use nature, but especially given that the Chemical Weapons Convention does not explicitly define the purposes of chemical weapons, but rather specifies many more purposes that are not prohibited by the Convention).

Question 9 By whom could a cyber arms control treaty be controlled? Would creating an independent verification regime be one approach to meeting the challenge so that states would share information related to their cyber capabilities? What functions would such a body need to handle?

Question 10 What do you see as 1) technical as well as 2) political challenges to transferring Chemical Weapons Convention measures to cyberweapons? Possible question (if more generally desired): In your estimation, what are 1) technical as well as 2) political challenges to implementing arms control measures for cyberweapons?

Bonus Question In your view, what is the factor or common denominator among states that has made and continues to make a common policy on chemical weapons possible (or arms control in the past), or what is missing or needs to change so that this is also possible regarding cyberweapons?

Final Question That would have been all the questions on my part now. In your opinion, are there still important aspects that we have not yet addressed? Who else do you think we should ask about this?

3 Coding Scheme

Remarks: We used the performed interviews for two different research projects. The second research project analyzes similarities and differences between arms control for chemical weapons and cyberweapons. The coding scheme therefore sometimes refers to chemical weapons. The coding scheme below is a shortened version, reduced to the aspects concerning this research paper.

Table 1 Coding scheme

Code	Description	to be coded when ...
<i>Arms control challenges</i>	All text passages that thematize challenges for arms control	–
Arms control challenges – cyber domain	All text passages that thematize specific arms control challenges related to the cyber domain	–
Arms control challenges – chemical weapons domain	All text passages that thematize specific arms control challenges related to the chemical weapons domain	–
Attribution – cyber domain	All text passages that thematize attribution as a challenge for arms control in the cyber domain or which elaborate to what extent it represents a challenge	“attribution has been very difficult in the cyber side for lots of reasons. So, the attribution question is important”
Attribution – chemical weapons domain	All text passages that thematize attribution as a challenge for arms control in the chemical weapons domain or which elaborate to what extent it represented a challenge	“Covert, the late noticing, the attribution, how can you even prove that, who was the aggressor. That's not trivial even with chemical weapons.”
Verification – cyber domain	All text passages that thematize verification as a challenge for arms	“These are not tangible, physical, material systems

	control in the cyber domain or which elaborate to what extent it represents a challenge	that can be counted or weighed and somehow have to be synthesized or bolted together first.”
Dual-Use – cyber domain	All text passages that thematize the dual-use nature of cyberweapons as a challenge for arms control in the cyber domain or which elaborate to what extent it represents a challenge	“Dual-use nature; that is, if we look at, for example, dealing with security vulnerabilities, that, so to speak, the techniques you need to secure yourself defensively are sort of the same techniques as the ones you need to attack.”
Political challenges – cyber domain	All text passages that thematize different political aspects or challenges as a general challenge for arms control in the cyber domain or which elaborate to what extent it represents a challenge	“I think given the technological developments here, the lots of different ways of cyberweapons can be used militarily, and for intelligence purposes, and corporate espionage purposes means that governments are not going to give up the advantage that they can get out of this and use them as well.”
Definition of the weapon – cyber domain	All text passages that thematize aspects of the general definition of a weapon or challenges in defining a cyberweapon as a challenge for arms control in the cyber domain or which elaborate to what extent it represents a challenge	“main challenge is, that there is no clear definition of what a cyber arm even is. It is not something that we can specify or define to the point”

Proliferation – cyber domain	All text passages that thematize the proliferation of cyberweapons as a challenge for arms control in the cyber domain or which elaborate to what extent it represents a challenge	“Proliferation, even unintentional proliferation, so to speak, even the attackers in many cases can’t be sure that their own capabilities won’t be further used and built by others – that’s certainly much more extreme here than in any other field where we’ve considered arms control so far.”
Constant technological progress – cyber domain	All text passages that thematize the expected constant technological progress in the cyber domain as a challenge for arms control in the cyber domain or which elaborate to what extent it represents a challenge	“cyber is such a quickly changing domain.”
Role of the private sector – cyber domain	All text passages that thematize the role of the private sector as a player in the cyber domain as a challenge for arms control in the cyber domain or which elaborate to what extent it represents a challenge	“we just have to work with the private actors, the owners of the infrastructure, the telecom providers, also with the cybersecurity companies who have to find their role in this, in terms of arms control, limiting the use of such software.”
Role of non-state actors – cyber domain	All text passages that focus on the role of non-state actors	“while cyber instruments can ultimately be used by any hacktivist. As a result, there is then also a completely different spread. This is a problem that we

		are currently facing in the Ukraine conflict.”
Further challenges for arms control – cyber domain	All text passages that thematize further challenges to arms control in the cyber domain	“What you always have in principle with disarmament agreements is the challenge of also getting on board those states that don’t feel that they are affected by it at all”
<i>Verification measures</i>	All text passages that thematize specific or possible verification measures	“the principle of managed access in verification, particularly in suspect inspections, was newly developed at that time to make such a tool possible in the first place.”
Further options	All text passages that focus on further options or alternatives to establish agreements for cyberspace	“What’s realistic would be an agreement between all the countries that have such capabilities and make a clear agreement on what targets are acceptable and what targets are not.”
Lists for differentiating prohibited and permitted components	All text passages that thematize lists for differentiating prohibited and permitted components as a specific or possible verification measure	“This declaration is related to list; that is, there are three lists where certain chemicals are on it. It’s based on how dangerous they are from a chemical weapons perspective.”

Verification regime	All text passages that thematize a verification regime as a specific or possible verification measure	“In the cyber domain, verification would require that you actually have a globally recognized attribution mechanism.”
Verification regime – challenges	All text passages that thematize challenges for the establishment of a verification regime	“It’s more a question of political will today whether we want to create such a place.”
Verification regime – requirements	All text passages that thematize requirements a verification regime would have to meet	“Further, this body would need to be endowed with credibility – the technical as well as the political credibility”
Focus on intent	All text passages that thematize a focus on the intent of a weapon as a specific or possible verification measures, to be understood against the background of the general purpose criterion	“First of all, with the chemical weapon, that approach is not to sanction the weapon or the instrument itself, but to sanction the behavior in using that instrument, that’s also the approach that needs to be taken with cyberweapons, if you want to call them that. So behavioral regulation, not technology regulation.”
Focus on intent – challenges	All text passages that focus on challenges against this backdrop	“I think, you can’t have the General-Purpose criterion without being able to find out who the perpetrators are

and who the persons are behind it.”

<i>Parallels – Chemical weapons domain and cyber domain</i>	All text passages that thematize parallels or similarities between the chemical weapons domain and the cyberweapons domain	“I think the bigger issue here is to narrow down which aspects of the parallels can actually be investigated”
Transferability	All text passages that thematize the transferability of chemical weapons arms control measures to cyber arms control	“the general-purpose criterion. Because I don’t see how you could implement prohibitions in the cyber area in any other way. So from that, I think the purpose – purpose or intent is always very difficult to determine, of course – could be a useful thing.”
Adaptation requirements	All text passages that thematize specific requirements to adapt measures of chemical weapons arms control to cyber arms control	“But that’s probably where you’d also have to try to have a lot of transparency, a lot of information.”
Similarity	All text passages that thematize similarities of the chemical domain to the cyber domain	“Chemical weapons, after all, are good for surprises, and that’s the same in the cyber domain. Just the covert, the late noticing, the attribution, how can you even prove who the aggressor was.”

Difference	All text passages that thematize differences of the chemical domain to the cyber domain	“for most military chemical weapons programs, you need to have a large infrastructure. You need to produce hundreds if not thousands of tons of chemical warfare agents, you need to fill them into munitions and there’s a lot there to look for. On the cyber side it could literally be one laptop”
<i>Cyber arms control – relevance</i>	All paragraphs that focus on or discuss the relevance of arms control in cyberspace	“You could now also conceive of a scenario where you have a cyberattack with massive effects on the civilian population – if we had something like that, it would of course be terrible, but it could also be a formative event that, from that point on, an awareness arises not only in the expert community, but in general that this is morally unacceptable. There is certainly a greater awareness of ‘cyber security’ in the meantime.”