EUROPEAN LEADERSHIP NETWORK

Building better security for wider Europe

What does cyber arms control look like? Four principles for managing cyber risk

GLOBAL SECURITY

POLICY BRIEF

Andrew Futter

June 2020

The European Leadership Network (ELN) is an independent, non-partisan, pan-European NGO with a network of nearly 200 past, present and future European leaders working to provide practical real-world solutions to political and security challenges.

About the authors

Dr Andrew Futter is an Associate Professor in International Politics at the University of Leicester, UK. Dr Futter has authored several books, including: Ballistic missile defence and US national security policy (2013/5); The politics of nuclear weapons (2015 and 2020); Reassessing the Revolution in Military Affairs (2015); The United Kingdom and the future of nuclear weapons (2016); Hacking the bomb (2018); and Threats to Euro-Atlantic security (2020), and regularly publishes in academic journals and contributes to conference papers. He recently completed a three-year UK Economic and Social Research Council funded Future Research Leader's award into cyber threats and nuclear weapons, and will shortly begin a five-year European Research Council Consolidator Grant exploring the technological drivers of the Third Nuclear Age.

Andrew was a Visiting Fellow at the Center for Arms Control and Non-Proliferation in Washington DC, as well a Visiting Scholar at the James Martin Center for Nonproliferation Studies in Monterey, California. In Spring 2017, he took up a Fellowship position at the Norwegian Nobel Peace Institute in Oslo. Dr Futter is an alumni member of the Younger Generation Leadership Network.

He can be contacted at ajf57@le.ac.uk and @andrewfutter on Twitter.

This paper is a reworked and extended version of a paper presented at the 2019 POSSE workshop.

Published by the European Leadership Network, June 2020

European Leadership Network (ELN)
100 Black Prince Road
London, UK, SE1 7SJ

@theELN

europeanleadershipnetwork.org

Contents

Introduction: Defining the problem

The question of how we control, manage, and mitigate the challenges, threats, and dangers posed by "cyber" is perhaps one of the most talked-about security problems of our time. Every aspect of modern life, the societies that we live in and the weapons we use to defend ourselves appear to be at risk from this new and inherently nebulous phenomenon produced by the latest information revolution. For sure, there have been attempts to get to grips with the potential hazards posed by hackers to the computer systems, networks and digital data that govern the modern world[1], but the cupboard remains bare when it comes to outlining any significant and long-lasting successes in this regard. Part of the reason for this is because the nature of the "cyber" problem still remains to be fully fleshed out and agreed, and it seems very difficult to begin constructing solutions before marking out exactly what it is that we are trying to "control". Thus, it is not simply the case that "cyber" arms control is impossible or that the cyber challenge represents the latest nail in the coffin of the broader international arms control agenda. To believe so is to misunderstand both the nature of the challenge posed by "cyber" as well as the fact that arms control is a fluid, multifaceted concept that we too often view in a constrained and rigid manner. Instead, we need to be prepared to think differently and recognise that the task of constructing new frameworks will take time.

"The question of how we control, manage, and mitigate the challenges, threats, and dangers posed by "cyber" is perhaps one of the most talked-about security problems of our time."

Consequently, what is presented here is more of a menu of options and a guide to how to think about this problem rather than a set of specific arms control recommendations that could follow. Increased clarity can be gained by returning to the first principles of arms control and employing a more holistic and broad view of what arms control can involve. Indeed, it is interesting how insights from the seminal works on arms control, and especially those from the 1960s, have been jettisoned or at least ignored in the modern era despite the fact that they have many important potential applications for the current "cyber" environment. This is because arms control is not simply about legally

binding, verifiable treaties between states, although these are of course welcome, but rather all measures designed to dampen incentives to begin hostilities, limit the damage if conflict should occur, and that enhance stability. Or as Thomas Schelling and Morton Halperin put it nearly 60 years ago, "…all forms of military cooperation between potential enemies in the interest of reducing the likelihood of war, its scope and violence if it occurs, and the political and economic costs of being prepared for it."[2] There are four lessons or insights that we might apply to the problem of cyber arms control.

1. It will depend upon what we seek to "control" and what we mean by "cyber"

At the heart of the "cyber arms control" puzzle must be a greater awareness of what we mean by both "cyber" and "arms control". "Cyber" as a concept is inherently contested and use of the word often serves to complicate and obfuscate rather than clarify a particular challenge or problem involving computers and networks. Likewise, we tend to have a very blinkered understanding of what is meant by "arms control" and what arms control agreements might look like. Taken together, this is not a particularly auspicious starting point for arms control in the digital realm, but it does suggest that clarity in the language we use and the way that we think through the problem is the more sensible and conducive place to begin before we can start designing complex agreements. It also produces an important first-order question: what exactly are we trying to "control" and how?

Arguably the biggest problem in answering this question is the fact that the "cyber debate" lacks an agreed definition of what this term means and refers to, and how it is being used.[3] The literature and policy space is replete with different understandings and conceptualisations of the concept and this has proved a major barrier in moving towards constructing viable agreements. Academics, professionals, policymakers and states appear to view the term and use it differently, often without realising. Consequently, the first thing that is required for any meaningful arms control is an awareness of the importance of semantics, and if possible, some type of agreement on how we are using different terms with potentially different meanings. This, in turn, may make it easier to delineate a credible and workable arms control agenda. The Tallinn Manual is certainty a move in the right direction, but this is not a universal document.[4]

Linked to this is the issue of what exactly it is that we are seeking to control, and what realistically we can control. There are four important aspects to this. First, are the distinct

differences between very low-level activities such as cyber-crime, hacktivism and nuisance–which are probably not best addressed through arms control, and operations that seek to cause damage and disruption, or use "cyber weapons" which might be. Second, are the differences between a very narrow conception of the problem focussing purely on Computer Network Attacks against a broader and more inclusive conception involving people, machines and the global digital information environment. Again, narrow definitions seem more suitable for our purpose. Third, is the distinction between activities that seek to alter the information space (broadly synonymous with Information Warfare/Operations) and those that target information systems directly–realistically it is the latter that we should seek to, and are likely to be able to, control. Fourth, is the distinction between the challenges of protecting systems and preventing malicious activities, which may require quite different arms control apparatus.

Each of these disambiguations suggests that a plethora of different approaches may be required for specific problems and that not all would fit logically into our contemporary understanding of arms control discussions or frameworks. Being clear about what we are trying to mitigate or secure against is a fundamental part of the challenge, and why semantic clarity in what we are doing is so important. This also suggests that traditional formal arms control efforts will need to focus on particular types of "cyber operations", namely those at the top end of the threat spectrum, that target systems directly rather than seek to muddy the information space, and that seek to cause damage and destruction rather than nuisance. A different arms control, law enforcement or regulatory approach may be needed for other "cyber" challenges.

2. "Cyber" arms control will probably be quite different from the nuclear realm

It has become commonplace to assume that we can borrow lessons and frameworks that have been developed in and for the nuclear realm and apply them to "cyber".[5] But while many questions might be similar, the answers and implications are likely to be quite different. This is because the two are very unalike in almost every aspect (even with a very narrow conception of "cyber"). Thus, the central pillars of nuclear arms control such as the Nuclear Non-proliferation Treaty, the Strategic Arms Reductions Treaty process, and the 2017 Nuclear Weapons Ban for example, might have limited applicability for models in the "cyber" realm.

The main reason why is the extent of the damage that nuclear attacks could

cause compared with "cyber" attacks: often likened to the difference between mass destruction and mass disruption. Approximately 200,000 people died as a result of nuclear use in August 1945, but so far no one has died as a direct result of a "cyber-attack". Traditional mechanisms of nuclear arms control such as limits on delivery vehicles, throw-weight, warhead numbers, or missile ranges, do not translate well into the "cyber" realm, albeit that some "cyber weapons" might also have both a payload and delivery vehicle.

Transparency is clearly also a major difference: nuclear weapons are big, quantifiable, conspicuous, and often used for signalling, whereas cyber capabilities are intangible, secret, and may lose any deterrent value when revealed, used, or attributed. This, of course, means that verification becomes a much more complicated, if not impossible task in "cyberspace". It is also difficult to see how Mutually Assured Destruction or MAD–arguably the condition that allowed for the US-Russia bilateral arms control process to begin-translates into the "cyber realm" given the difficulty of knowing what an adversary might have or can do, and the challenge of attributing attacks quickly and with high confidence. However, areas that could provide useful insights are the Nuclear Security Summits convened between 2012 and 2016, UN Security Council Resolution 1540, and possibly even the pre-nuclear era Geneva Conventions and International Humanitarian Law.[6] The way in which states (in the past two decades) have begun to address the threat from nuclear terrorism might be a helpful analogy more generally; seeking better defences and establishing universal norms for safety and security as the precursor to more formal (arms control) agreements. Recent moves towards stigmatising and delegitimising nuclear weapons might also be fruitful initiatives to imitate too.

"In the "cyber realm"... it might not necessarily be at the nation-state or the international level where arms control takes place."

Another big difference for "cyber" arms control is in who is and should be responsible for challenges in the digital realm. For a variety of reasons, chief amongst them cost and resources, states have always been the main players in the nuclear game, and governments and leaders have logically been the focal point for nuclear arms control. But this is not always quite so clear in the "cyber realm" and depending on how we conceptualise arms control and what it is that needs controlling, it might not necessarily be at the nation-state

or the international level where arms control takes place. Part of the reason for this is because the majority of disruptive activities in cyberspace, such as hacktivism, crime, Intellectual Property (IP) theft, and espionage, are probably not best, or at least not most effectively, dealt with at the international level. Thus, we might need to think about the importance and role of multinational technology companies, other non-state actors[7], and to some extent the responsibilities of us all as individuals to manage the challenge. It is instructive that a decade ago when discussions began between the US and Russia on "cyber arms control", that the two saw the problem and possible solutions very differently: Russia favoured a traditional international treaty, while the US favoured improved law enforcement cooperation.[8] We probably need bits of both.

3. It will involve a mixture of formal and informal mechanisms

Arms control in the "cyber" realm is likely to involve a mixture of formal and informal mechanisms, probably at the same time, for different issues and problems. Again, this is not necessarily a new idea–it was a key part of the canon of nuclear arms control in the 1960s. Indeed, it seems likely that we already abstain from some activities in the digital realm without formal agreement and this in itself is a form of arms control.[9] As Schelling and Halperin noted:

> *Arms control is necessarily thought of as entailing formal agreements, negotiated in detail at diplomatic conferences, embodied in a treaty, and with machinery or institutions for monitoring the agreement. But a more variegated and flexible concept of arms control is necessary–one that recognises that the degree of formality may range from a formal treaty…through executive agreements, explicitly but informal understandings, tacit understandings, to self-restraint that is consciously contingent on each other's behaviour.*[10]

Such measures may also be conducted unilaterally, at least in the first instance, and if possible, bilaterally or multilaterally too.

Formal arms control refers to arrangements that are public and involve some sort of legally binding agreement, usually between two or more parties. Examples would be the New START Treaty signed by the United States and Russia in 2010 or the Chemical Weapons Convention signed in 1993 and which now has 163 signatories. These arms control agreements categorically place restrictions on certain types of activities, and states sign up publicly (although of course they are allowed to withdraw) and are held

to account (possible forcibly) if they do not abide by the terms. Formal arms control might also be carried out unilaterally, such as through declaratory policy and moratoria– two methods that certainly could be applied to certain types of activities in "cyberspace", or through public statements. Making red lines clear is also in a way a form of arms control; for example, threatening a serious and perhaps specific response to "cyber" attacks on hospitals[11] or on nuclear command and control systems.[12] So is providing more information on doctrine, and capabilities and undergirding processes. There might also, of course, be points at which "unilateral actions can be extended or supplemented through joint understandings with our potential enemies" as Schelling and Halperin suggested a generation ago.[13]

Informal arms control is less tangible, but perhaps more useful to some of the problems in our digital world. These initiatives would not be codified in official treaties or declarations but signalled in other ways, through private conservations and back channels, certain actions or decisions. The aim would be to build trust and confidence, and perhaps even global epistemic communities focussed on cyber risks. It could also include measures designed to enhance understanding and communication, such as the US-Russia cyber hotline established in 2013 (though this is possibly a more difficult tool to use that it seems at first glance)[14], and those that seek to minimise time pressures on particular weapons systems or for decision making. In this regard, self-control, that is not pushing the boundaries or carrying out activities that might be seen as destabilising are in a sense a form of arms control. It could also involve actions that a state might wish to abstain from, "in the interest of reducing false alarms, accidents that might lead to war, dangerous crises, an excessive accumulation of threats and challenges, or just excessive tension."[15] This might, of course, include "enhance(ing) those aspects of technology that we like and that helps to nullify those that we do not."[16] Or simply refraining from "clumsy espionage", and mock attacks.

"...we should think broadly about arms control and encourage ideas and thinking 'outside the box.'"

The key point really is that we should think broadly about arms control and encourage ideas and thinking "outside the box."[17] While there may, of course, be a risk of "watering down" the concept, this should not prevent us from trying new methods. Moreover, just because these methods may not look like those of the past, does not mean that they are not useful. That said, we must also recognise that

the problems of detecting cheating, and the problems of enforcement will remain and perhaps become more pronounced in "cyber" arms control.[18]

4. Focussed and single-issue rather than broad and general agreements

The most productive way forward for arms control in the "cyber realm" seems to be looking for particular areas, issues and problems that might be "controlled" rather than seeing this a problem that can be combined and solved all in one go. This is because it appears very difficult to conceive of an all-encompassing "cyber treaty" possibly under the auspices of the United Nations[19], or a generic "cyber weapons" ban, although some have suggested that such a thing is possible.[20] Notwithstanding the considerable difficulties involved in defining what these would include, a far more productive approach seems to be working back from a particular problem, escalation risk or dynamic that we wish to control.

The first thing this means is that we have to be realistic about what certain states are willing or able to give up. This has always been a significant factor in arms control discussions and is unlikely to change with "cyber". A good approach to this problem might be to think about what is in everyone's interests as there seems little point in trying to control aspects of the "cyber" realm that key actors are not willing to limit or forego (at least for the time being). This might mean going for certain low hanging fruit, such as informal talks and exchanges designed to build confidence and maybe even share good practice. It might also mean turning a blind eye to "cyber espionage" and IP theft, in order to prioritise more serious security risks.

This could lead on to a discussion of whether it might be useful to think in terms of *weapons* versus *targets* for arms control in the "cyber" realm and whether this should be applied at the *tactical* or *strategic* level. It is difficult to see how we might think of controlling "cyber weapons" because they are likely to be so different, specialised, secret and intangible, but it might be productive to think about certain *targets* or even *actions* that might be declared off-limit or prohibited. Linked to this, and for similar reasons, it probably makes sense to focus on reducing *incentives* rather than reducing *capabilities* when we talk about "cyber" challenges. For example, focussing on better defence and security, building resiliency into systems, reducing the benefits to an attacker (deterrence by denial), and focussing on *qualitative* rather than *quantitative* estimates of force.

Finally, it may not make sense to treat "cyber" in isolation, because the concept is so intrinsically linked with other capabilities and more often

than not, facilitates and augments them. While some have decided to view "cyber" as a domain of military operations, the reality is that it impacts right across the spectrum of kinetic force and across all other domains. Moreover, "cyber" capabilities are inherently dual-use, and most are not best thought of as a single weapon system in the same way that we might view a bomb. We also need to recognise that we are dealing with a technological challenge that is constantly in flux and changing – in some cases very quickly – not least with greater incorporation of Artificial Intelligence (AI).

"... it is useful to remember that the nuclear arms control edifice that was developed to manage the Cold War and later the post-Cold War world did not look easy at the start either. ."

Conclusion: History tells that we should not expect the answers to be easy or quick

It is easy to point to the problems of pursuing arms control in "cyberspace": it is difficult to measure capabilities; there is uncertainty of effects; the challenges of verification and compliance appear daunting; and there are no rules of the road in terms of enforcement, compliance or punishment.[21] However, it is useful to remember that the nuclear arms control edifice that was developed to manage the Cold War and later the post-Cold War world did not look easy at the start either. Indeed, there were also many setbacks and scores of detractors along the way,[22] and it is also true that certain parts of the US government (and others) did not want arms control, much like the case today. But, with a few exceptions, these frameworks have helped manage our nuclear world and kept us safe from the horrors of nuclear use and war. This is not to say that the same frameworks and conceptualisation of arms control can be directly applied to today's digital world, but rather than arms control is a toolkit rather than a tool and must evolve to meet today's threat environment rather than being discarded as anachronistic.

While this article may not provide a panacea to this problem, it does, I hope, set out a number of key criteria that we need to consider in future "cyber arms control". First, it must be based on agreed definitions of

the problem; second, it probably will not look like agreements from the nuclear realm, but this is ok; third, it will not cover everything we label as "cyber", especially issues that are best addressed at the sub-state level, and probably will not include the many challenges presented by Information Warfare; fourth, it must include informal and unilateral mechanisms of control in addition to perhaps more complicated formal, multilateral, legal agreements; fifth, it is likely to be targeted and specific, and aimed at certain activities or targets rather than capabilities or weapons, and sixth it will require analysts, scholars and policymakers to think outside of the box and not be afraid to try new ideas and innovative avenues.

Interestingly, if we go back to the world of the 1960s, we find that the essence of these challenges is not completely new either. Writing in 1961, Schelling and Halperin noted that, "The most mischievous character of today's strategic weapons is that they may provide an enormous advantage, in the event that war occurs, to the side that starts it."[23] The same could clearly be said about the myriad challenges posed by "cyber" today. The key is in how we think about the problem and in recognising that we are currently at the start of this process.[24]

Endnotes

1. For example, the 2015 US-China agreement; See, Scott Harold, "The US-China cyber agreement: A good first step", RAND, (1 August 2016), https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html. The Council of Europe "Convention on Cybercrime", known as the Budapest Convention (23 November 2001), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. The Shanghai Cooperation Organization's International Information Security Agreement (2009), unofficial translation: https://www.ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf. And a Letter sent by Russia, China, Tajikistan and Uzbekistan to the UN Secretary General in 2011 for an International Code of Conduct for Information Security, https://www.rusemb.org.uk/policycontact/49

2. Thomas Schelling & Morton Halperin, Strategy and Arms Control, (Martino Publishing, CT, 2014 [1961]), p.2.

3. On this see, Andrew Futter, "Cyber semantics: Why we should retire the latest buzzword in security studies", Journal of Cyber Policy, 3:2 (2018) 201-216.

4. Michael Schmitt, Tallinn Manual on the International Law Applicable to Cyberwarfare, (Cambridge, Cambridge University Press: 2013, 2nd edition: 2017).

5. On this see, Joseph S. Nye, "From bombs to bytes: Can our nuclear history inform our cyber future?", Bulletin of the Atomic Scientists, 69:5 (2013) 8-14.

6. Tarah Wheeler, "In cyberwar there are no rules", Foreign Policy, (12 September 2018), https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/. See also, Erin Dumacher, "Limiting cyberwarfare: Applying arms-control models to an emerging technology", The Nonproliferation Review, 25:3-4, (2018) 203-202.

7. Robert Litwak & Meg King, "Arms control in cyberspace?", Wilson Center, (October 2015), p.3

8. John Markoff & Andrew Kramer, "US and Russia differ on treaty for cyberspace", New York Times, (27 June 2009), https://www.nytimes.com/2009/06/28/world/28cyber.html

9. Schelling & Halperin, Strategy and Arms Control, p.33.

10. Ibid, p.77.

11. Martin Giles, "We need a cyber arms control treaty to keep hospitals and power grids safe from hackers", Technology Review, (1 October 2018), https://www.technologyreview.com/s/612215/we-need-a-cyber-arms-control-treaty-to-keep-hospitals-and-power-grids-safe-from-hackers/

12. See for example, Andrew Futter, "Why we must prohibit cyberattacks on nuclear systems: The case for pre-emptive US-Russia arms control", Valdai Discussion Club No,95, (November 2018), http://valdaiclub.com/files/21235/

13. Schelling & Halperin, Strategy and Arms Control, p.4

14. See: Sean Gallagher, "US, Russia to install 'cyber-hotline' to prevent accidental cyberwar", Arstechnica, (18 June 2013), https://arstechnica.com/information-technology/2013/06/us-russia-to-install-cyber-hotline-to-prevent-accidental-cyberwar/. See also, "Fact sheet: US-Russia cooperation on information and communications technology security", White House Office of the Press Secretary, (17 June 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol

15. Schelling & Halperin, Strategy and Arms Control, p.32

16. Ibid, p.4

17. Alex Bell & Andrew Futter, "Reports of the death of arms control have been greatly exaggerated", War on the Rocks, (4 October 2018), https://warontherocks.com/2018/10/reports-of-the-death-of-arms-control-have-been-greatly-exaggerated/

18. Erica D. Borghard & Shawn W. Lonergan, "Why are there no cyber arms control agreements?", Council on Foreign Relations, (16 January 2018), https://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements

19. Andrei Khalip, "UN chief urges global rules for cyber warfare", Reuters, (19 February 2018), https://uk.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUKKCN1G31Q4

20. For an alternative view see, Mette Eilstrup-Sangiovanni, "Why the world needs an international cyberwar convention", Philosophy and Technology, 31:3 (2018), pp.379-407. "To be successful, an international treaty aimed at reducing risks of cyber warfare must fulfil (at least) four criteria: (1) it must offer sufficient positive incentives to ensure broad participation by states, (2) it must stipulate rules that effectively constrain behavior and that can be practically implemented given current technology, (3) it must provide sufficient credible information to reduce uncertainty about state interests and enable effective signaling, and (4) it must ensure significant costs to non-compliance."

21. Draws upon Borghard & Lonergan, "Why are there no cyber arms control agreements?".

22. John Maurer, "Why cyber arms control is not a lost cause", The National Interest, (11 November 2018), https://nationalinterest.org/feature/why-cyber-arms-control-not-lost-cause-31017

23. Schelling & Halperin, Strategy and Arms Control, p.9.

24. The article by Mischa Hansel, Max Mutschler & Marcel Dickow, "Taming cyber warfare: Lessons from preventive arms control", Journal of Cyber Policy, 3:1 (2018), pp.44-60, could be a good first step in this regard.

EUROPEAN
LEADERSHIP
NETWORK

European Leadership Network
100 Black Prince Road
London, UK, SE1 7SJ

secretariat@europeanleadershipnetwork.org
+44 (0)203 176 2555
@theELN
europeanleadershipnetwork.org