Keep Dreaming: Cyber Arms Control is Not a Viable Policy Option

Tobias Burgers, David Ryland Scott Robinson

Abstract: Influential voices call for efforts to curb the accelerating cyber arms race. One proposed strategy is cyber arms control. We argue that the pursuit of this regulation would be stymied, and any regulation passed would be ineffective on the basis that 1) neither unilateral nor multilateral cyber arms control efforts would be effective, and that 2) cyber arms control would conflict with both sovereignty and legitimate peaceful development efforts.

Keywords: Arms control, cyber arms control, cyber conflict, cyber threats
Schlagwörter: Rüstungskontrolle, Cyberwaffenkontrolle, Cyberkonflikt, Cyberbedrohungen

1. Introduction

The digital technological revolution has changed boundaries, bypassed natural barriers, fueled revolutions, changed politics, altered news cycles, created near-instant access to (disputed) information, given rise to digital authoritarianism, and created a new space: cyberspace (Burgers and Robinson, 2016; Floridi, 2007; Hurwitz, 1999; Jenkins and Thorburn, 2003; Küng et al., 1999). This new and man-made space has come to take a dominant role in our contemporary societies. In the words of the UK's Science and Technology Facilities Council (2018): "We're all living in the information age. ... Technology has transformed our lives, and the digital revolution shows no sign of slowing down." As a result, societies and states have become dependent on a well-functioning cyberspace. As with any dependency, this creates vulnerabilities (Tynkkynen, 2016). In the last ten years, these vulnerabilities have created a cyber fear (Singer and Friedman, 2014, p. 130). Euphemisms such as a "Cyber Pearl Harbor," "Cyber 9/11," and other possible worst-case scenarios such as digitally hijacked nuclear power plants, hospitals, as well as suggestions that airplanes are hackable, have contributed to a wider fear towards cyber threats (Bumiller and Shanker, 2012; Nye, 2011a, pp. 21, 22; Singer and Friedman, 2014; Stavridis, 2017; Wirtz, 2017; Zetter, 2015). Yet, Healey notes (2013b, p. 6) "nations seem extremely reluctant to conduct damaging attacks to one another outside of traditional geopolitical conflict."

Nevertheless, perception and intention matter in international security relations (Stein, 2013; Walt, 1985). Or, in this case, the misperception. This state of overblown perceptions and misperceptions, the lack of clarity in the significance of cyber threats, and the qualitative and quantitative value of these threats have contributed to what Singer and Friedman (2014, p. 7) label as a situation of "confusion and misinformation". Such an environment is fertile ground for fear to take root through misperception. In her essay, Stein (2013) illustrates how (mis-)perceptions of and misinformation about threats and signals from actors can influence international security relations. Likewise, in his landmark work "Perception and misperception in international politics," Robert Jervis (1976) discusses the value, importance and implications of perceptions and misperceptions. Both Stein and Jervis illustrate how misperceptions influence decision making in international relations, which subsequently could increase security tensions and could contribute to the outbreak of conflict. The outbreak of World War One, the Vietnam conflict, and the recent Iraq War of 2003 are examples of such.

Misperception can also arise in the conduct of international cyber security relations (Cavelty, 2013). As Rid and Buchana (2014, p.4) argue, when it comes to attribution in case of cyber attacks, "attribution is what states make of it". Misunderstood signals play an important role in the perception of possible cyber threats and attributions of attacks. During the Clinton presidency, U.S. government institutions were hacked, and, in response, the Solar Sunrise investigation was launched, with the presumption that Iraq was the culprit. The existing perception among U.S. government intelligence was that the military and political leadership of Iraq was engaging in an information war (Arkin, 1999; Healey, 2013a; Poulsen, 2001). However, the hacks were, rather than an Iraqi effort, the product of four teenagers: two American, one Canadian and an Israeli (Arkin, 1999). Yet, the initial misperception, which according to Richard Clarke, at that time U.S. National Coordinator for Security, Infrastructure Protection, and Counterterrorism , lasted "for days, critical days" (Clarke, quoted in Arkin, 1999).

The Solar Sunrise example illustrates the problem of establishing adequate threat perceptions and how this could influence policy decisions. Yet, cyber systems have additional unique and problematic aspects that complicate the ways in which they may be perceived. First: the visibility of cyber threats remains limited. For example, a nuclear missile silo can be monitored. The opening of the silo's hatch indicates a likely imminent missile launch. Yet, there is no digital equivalent of a missile silo's hatch. Second: while conventional threats have geographical limitations, cyber threats do not (Nye, 2011b). Third: plausible deniability. The multitude of actors using similar tactics and with a wide range of goals makes many cyber offensive operations plausibly attributable. For instance, by mimicking tactics, one actor can impersonate another actor (Craig and Valeriano, 2016, pp. 144).

To counter these possible perceived threats, nation states have sought to bolster their defenses (Craig and Valeriano, 2016, pp. 141-142). Yet, in the cyber domain, the increasingly common claim is that offensive tactics are the most effective defensive tactics (ibid, p. 144; Slayton, 2017). So both state and non-state actors use offensive tactics to bolster their defenses. Galinec et. al (2018) refer to this as offensive security. Robinson et. al. (2013, p.44) illustrate how actors are "building offensive capabilities [...], which allow them to 'attack as the best form of defence'." Craig and Valeriano (2016, p.144)

https://doi.org/10.5771/0175-274X-2018-3-140
DOI: 10.5771/0175-274X-2018-3-140

outline the difficulty choosing between investing in defensive or offensive capabilities. "Offensive cyber capabilities are assumed to be more cost effective and efficient, whereas defense is difficult given the immense challenge involved in securing every civilian and privately-owned network and closing every vulnerability, many of which go undetected until an attack has pointed them out. The Internet's lack of geographical constraints further undermines the utility of defense. Offensive preparations may, therefore, become the dominant strategy". This strategy has created a loop in which nations favor the development of offensive cyber weapons. This in turn has created a constant need for improvements to their cyber offensive capabilities to ensure that their cyber defense is adequate to counter potential threats. This self-reinforcing cycle of arms development has resulted in what commentators are calling a "cyber arms race." Craig and Valeriano (2016, p. 142) describe arms races as situations in which threats are rapidly rising while competing actors seek to extend their capabilities. Right now, in the cyber world, more than 50 percent of cyber security experts and political leaders believe a cyber arms race is arising (McAfee, 2012). In their article, Craig and Valeriano (2016) confirm this perception as factual. Glenny (2011), Jellenc (2012), Mimran (2017) and Singer and Friedman (2014) likewise support the thesis that a cyber arms race is developing. As Wirth (2016) notes candidly: "The cyber arms race is on." Limnéll (2016) goes even further, arguing that the cyber arms race is already accelerating. The cyber arms race follows a classical arms race model as outlined by Jervis (1976). His "spiral model" argues that arms races develop as products of mutual fears, which forces each side into a self-reinforcing cycle of arms development (Jervis, 1976; Kydd, 2000). The existing cyber fear, outlined above, contributes to this self-reinforcing cycle of efforts to develop new cyber weapons.

Historically, arms races have contributed to increased risk of instability (Bull, 1966; Jervis, 1976; Kydd, 2000; Nye, 2011a). Therefore, it is not surprising that benevolent actors are exploring possibilities to limit and control this cyber arms race. The most visibly promoted possibility is the idea of establishing cyber rules, norms, confidence-building efforts, early warning mechanisms and possible arms control (Macak, 2017; Noor, 2015; Meyer, 2012; Ward and Morgus, 2016). Indeed, the concept of arms control – minimizing the costs and risks of the arms competition, as well as mutual interest in avoiding conflict, and limiting violence once conflict occurs – is in theory a policy option that could limit misperceptions, cyber arms development, and decrease cyber conflict (Schelling and Halperin, 1961). It has also proven to be a viable policy option. During prior global arms races, e.g., the nuclear arms race, the idea of arms control was widely discussed and implemented, thereby limiting nuclear arms development to some extent. Furthermore, it engendered stability and provided a platform for cooperation between actors, limiting the possibility of conflict (Borghard and Longergan, 2018). As such, actors now consider cyber arms control as a viable policy option to limit the cyber arms race. Nye (2015) has argued for the need for cyber arms control. Dittrich and Boening (2017) likewise advocated the need for control. Even actors like China and Russia, who have significant cyber capabilities and are actively engaged in offensive cyber operations, have raised the topic of cyber arms control through the formation of a treaty (Rid and McBurney, 2012, p. 6). Maybaum and Tölle (2016) appear optimistic, arguing that "arms control has been a success story since the late 1980s." However, this success story is unlikely to repeat itself. There is genuine interest among actors, both state and non-state, in the concept of cyber arms control. Yet, as we will illustrate in the next section, the technical structure of cyberspace and the dynamics of cyber threats make arms control in cyberspace not viable.

2. The Impossible Dream of Cyber Arms Control

First, we will give a definition of "cyber arms control." "Cyber arms" are, according to Rid and McBurney (2012, p.6), "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings." "Control" is, in principle, the regulation of the development, production, stockpiling, proliferation, or use of arms (U.N., 1996). Yet, the pursuit of forming international agreements to control cyber arms will find itself stymied. Any regulation passed would be limited in effectiveness: 1) that either unilateral resolutions or multilateral agreements for cyber arms control would be immediate 'dead letters', or 2) that cyber arms control would conflict with both sovereignty and legitimate peaceful development efforts.

Before directly grappling with the economic and moral arguments against cyber arms control, it is important to first point out and address the elephant in the room: a teenager, with a laptop and an Internet connection, is capable of harming well-funded and well-protected national, multinational, and supranational organizations (Nye, 2011b). Accordingly, these organizations are vulnerable in the cyber domain to any adversary capable of marshalling more resources than a child. Of course, the threat from a teenager, or most non-state actors, does not compare to the capabilities of state actors. Indeed, as Healey (2013b) notes, "strategic cyber warfare has thus far been well beyond the capabilities of stereotyped, teenaged hackers in their basements." Non-state actors have the ability to disrupt networks and cause problems; albeit, these threats are less consequential than strategic cyber warfare. This is a difficult reality to confront. No group desiring to participate in the global economy would relinquish general purpose computers or access to the Internet. But the costs, inefficiencies, and overhead to secure telecommunications technologies are high. The existing regulatory controls on computing – hacking is already illegal – are token at best. Even Internet access controls, to this point, have been limited to mass population control (Burgers and Robinson, 2016). Indeed, as the examples of China and Russia illustrate, governments have sought to curtail access to information, but not to systems nor the Internet as a whole in itself.

Yet, to some extent, the possibility of global Internet access controls has been raised by influential voices (Kaspersky, 2012; Smith, 2017). But fragmentation of the Internet would necessitate the fundamental restructuring of the global telecommunications infrastructure and every industry impacted by information technology. This restructuring would be quite literally from the ground up; for example, in the case of adding "air gaps" between low and high security networks. Such is simply not feasible. These calls are disingenuous, at best arising from an interest in continued profit and at worst from an interest in continued military advantage.

More realistic options for control exist, though these are also not yet viable in their current state. First, we take it as a given that cyber arms

control efforts can only be pursued at a national or supranational basis. Localities – towns, cities, counties, provinces – have neither the will nor the capability to restrict access to the two requirements for cyber arms development: access to general purpose computers and unrestricted Internet access. So, if cyber arms control – like its analogue of traditional Chemical, Biological, Radiological and Nuclear (CBRN) and Weapons of Mass Destruction (WMD) arms control – is to occur in a national scope, then the question arises: should the effort be unilateral or multilateral? There are neither rational nor irrational motivations for a country to unilaterally go down this path. On the contrary, persuasive motivations can be identified, as outlined in the next paragraphs, against unilateral action, which even support the development of a local cyber arms industry. Put simply, unilateral cyber arms control is a disadvantage. It would prevent participation in the global market for cyber arms and incur enforcement costs, and any enforcement actions would necessarily act as a tax upon local industry.

3. Cyber Arms as a Global Industry

Cyber arms is a global industry; its market is large, its ecosystem diverse. Threats exist online and offline. Legal and black markets trade software exploits, zero-days[1], and surveillance technology. Many governments have groups dedicated to cyber warfare; cyber commands of smaller nations influence security relations between leading military nations (Galeotti, 2018; Modderkolk, 2018). Many traditional arms manufacturers, e.g. General Dynamics (U.S.), BAE Systems (UK), and Leonardo (Italy) have cyber arms departments. There are many smaller companies that specialize in cyber arms (Boulanin, 2013). Incubating a local cyber arms industry is a win-win for any government, because cyber arms are cost-effective for asymmetric conflict and bolster hard and soft power. In the words of the Israeli Prime Minister Benjamin Netanyahu (2017), "Cyber security is a serious business. It's a great business because it's growing geometrically. There's never a permanent solution. Never. It's an endless business." Unsurprisingly, Israel's cyber security industry demonstrates how investment in expertise and research for development offers dual-use capabilities. Legal sales of cyber arms provide a revenue source, to the tune of tens of billions of dollars (IDC, 2017; Tsipori, 2016).

But restricting cyber arms development incurs a cost. Even the most totalitarian of regimes with the best surveillance technology are unable to control unsophisticated netizens.[2] It is almost tautological that cyber arms developers are even less impacted by soft controls, such as blocks and fines, on computing and Internet access. Harder controls would just ensure a brain drain, which enemies would welcome (Stecklow and Fassihi, 2009). Domestic security is not improved through enforcement actions, since cyber arms are delivered via the global Internet. The domestic or international provenance of cyber attacks is hard or impossible to determine due to the structure of the Internet. False flags attacks are trivial. In short, restrictions hinder security and help enemies (Nye, 2011b).

But even if restrictions were put in place, they would act as a tax upon local industry. Basic cyber arms research and development is dual-use[3]; for example, zero-day research both augments the capabilities of existing cyber arms and strengthens the defense of existing systems. Cyber arms research drives cyber security research, and cyber security is a common good with dual-use for the nation states, their societies, and a host of non-state actors. Global finance, online commerce, and industrial systems all depend on and invest heavily in cyber security. History serves as a reminder of this: The United States government and its allies tried to take an enforcement action in the 1990s as a part of the "Crypto Wars" (Levy, 2001). Strong cryptography was – and by many, still is – treated as a dangerous munition to be placed under severe export controls. But the controls were quickly found to be ineffective. Not only were they ineffective economically, because strong cryptography made online commerce possible; they were also ineffective logistically, because the math for then strongest encryption algorithms could be (and were) put on a t-shirt or printed on a sheet of paper and walked through customs.[4]

There seems to be no rational motivation for any country to unilaterally control its own cyber arms market. But what of irrational motivations? We see none. Unlike chemical weapons in Europe post-World War I, nuclear weapons in Japan post-World War II, or even handguns in Australia post-Port Arthur, cyber arms present no danger, clear and obvious, to the common man; there are no social traumas, no moral panics, no conflict with traditional or progressive value systems. The individual, groups and society are all relatively numb to the danger of cyber arms.

Therefore, cyber arms control must be multilateral. Yet, multilateral arms control is only effective if the participants will not be able to cheat easily (U.N. 1995; Jervis, 1976). Much effort is put into the effective intertwining of monitoring and verification for nuclear, biological, and chemical weapons. But even if a nation or polity were capable of controlling their local cyber arms industry, the question is: would they? Both the prisoner's dilemma and free rider arguments apply here. If cyber fear is to be reduced, states should seek to build confidence through mutual validation. Validation demands that cyber arms can be clearly attributed to their source. States need to know who was cheating to engender respect for the rules. But the catch is that the provenance of cyber arms is notoriously difficult to attribute as illustrated in the first section. Moreover, only actors from the cyber arms or cyber security industry have the requisite expertise to discover and research discovered cyber arms.

Then who are these actors with expertise? How do they arise? Can their research and development in cyber arms be controlled? As we

1 Zero-day is a flaw in software, hardware or firmware that is unknown to the party or parties responsible for patching or otherwise fixing the flaw. The term zero day may refer to the vulnerability itself, or an attack that has zero days between the time the vulnerability is discovered and the first attack. Once a zero-day vulnerability has been made public, it is known as an n-day or one-day vulnerability. Retrieved from https://searchsecurity.techtarget.com/definition/zero-day-vulnerability (accessed October 22nd, 2018).

2 Netizen: Blend of net and citizen and refers to a user of the Internet, especially a habitual or keen one. Retrieved from https://en.oxforddictionaries.com/definition/netizen (accessed October 22nd, 2018).

3 Dual-use technologies have both military and peaceful uses. Basic cyber arms research is dual-use as it improves the reliability of systems to (peaceful) accidental misuse and unintentional damage.

4 The best known example is Philip Zimmermann's (1995) "PGP Source Code and Internals", published by MIT Press. The book contains the entire source code for Pretty Good Privacy, a then state-of-the-art encryption tool banned for export from the United States. If one wanted to develop their own version of PGP, one simply had to scan all the pages or manually copy the code into a text file. With the help of the free and widely available GNU Compiler Collection software, one could then simply construct their own version of PGP. Adam Back was even more creative and printed the code on t-shirt. For further information see http://www.cypherspace.org/adam/rsa/uk-shirt.html (accessed 24.10.2018).

have already pointed out, controlling the knowledge of cyber arms would require wholesale control of global communications systems and all post-industrial knowledge workers. One such proposal by Kaspersky (2012), of a three-tier Internet with firewalls and controls between each level, would likely instantaneously create a global black market which would dwarf the existing markets for falsified national identification and passports. Yet, cyber arms control cannot exist without communication controls. Their import and export is informational, not physical. Also, the knowledge of how to produce cyber arms is already public, widely distributed, and basic to any post-industrial base. Small private companies of mostly fewer than a dozen people already produce cyber arms and market them to states (Boulanin, 2013). As such, it becomes apparent how on any multilateral level, a cyber arms control initiative seems poised to be ineffective. Any country can cheat. They have incentive to cheat as accurate attribution for cyber attacks is not currently possible. Unless a dramatic global shift in attitudes towards cyber security and arms control occurs, any multilateral effort will remain ineffective.

The second rejection of cyber arms control centers around the idea of peaceful development. Many countries will ostensibly limit their development of cyber weapons in the hope of negative peace.[5] But few countries will limit their hopes for peaceful post-industrial economic development. For example, the "Atoms for Peace" development program peacefully spread nuclear material and expertise to over 30 countries, whilst simultaneously building confidence for later establishment of both the IAEA, the Non-Proliferation Treaty (NPT), and the cessation of nuclear programs in countries like Sweden, Italy, and South Africa. However, this has also left the world with paranuclear nations like Japan.[6] The same tension between offensive use and peaceful development applies to cyber arms.

No country will accept limits on its own peaceful development of local cyber arms expertise. Yet, as illustrated before, cyber arms development is intrinsically dual-use. Software and cyber technologies are integral to both industrial and post-industrial economies. The effectiveness of most offensive cyber arms, exploits, and zero-days in particular, are due entirely to the robustness (or lack thereof) of complex software systems (Amoroso, 2012). These weapons take advantage of categorical flaws, described in broad terms like "buffer overflow" and "SQL injection." To make an analogy, when we discover that small doses of a chemical can kill a person, efforts are taken to educate and control access to that chemical to protect human life. Yet unlike human biology, software can be improved, rendering harmful material harmless. Even now, there are efforts being made to remove those categorical flaws from the greater software ecosystem (Nye 2011b).

Calls for cyber arms control, when viewed in this light, seem cynical. Cars kill. Pollution kills. Processed food kills. The appeal to a ban is undeniable, especially from the perspective of already developed nations. Developed nations reap the benefits of their advanced status as well as manage the long-term effects of well-intentioned but ultimately harmful efforts that were made in the journey to modernity. However cyber arms are less dangerous to global civilization than traditional arms. They only directly cause physical damage through the misuse or malfunction of managed infrastructure. The increasingly cybernetic infrastructure is hardened by researching and mitigating faults. The outcomes of that research are both how to break (arms) and how to fix (defenses).

If limiting cyber arms development and production is hard, another option might be control of stockpile. In 2014, under President Obama, the White House committed to just that, reducing offensive cyber arm stockpiles through their existing Vulnerability Equities Process (VEP) (Healey, 2016). The VEP is a U.S. government process to determine whether to withhold or disclose information about computer software security vulnerabilities. However, in 2017, it was publically revealed by Wikileaks how the agencies central to the VEP both steamrolled the process and completely ignored it. Not disclosing cyber arms was seen as critical for domestic security purposes (Nakashima, 2017).

Proliferation of cyber arms has its own unique difficulties. The only way to definitely defend against a cyber weapon is to fix the vulnerability it exploits. There has been a constant tension between the perspectives of "full disclosure" and "coordinated disclosure". The former, "full disclosure", is the practice of publishing the existence of vulnerabilities as publically and widely as possible. The latter, "coordinated disclosure", discloses existence of a system vulnerability to the party responsible for said system. There has been much debate on the relative merits of each philosophy; neither perspective has been proven strictly better for global cyber security. From the angle of reducing proliferation and its potential impacts on peaceful development however, we note two conflicts: 1) the reverse engineering industry, and 2) where "speech" and "arms" blend. We will tackle each in order.

There is a significant industry around reverse engineering – that is, the process of taking an existing product, and figuring out how it was produced and learning how to replicate it (Vacca, 2012). There are reverse engineers in industrial manufacturing, food science, and cyber arms. The richest source of vulnerabilities and exploits is not original research, but rather the reverse engineering of published protections to vulnerabilities. For example, when Apple releases a security update for their mobile phone operating system (iOS), researchers immediately look at what has changed in order to determine where the vulnerabilities were (Avgerinos, 2014; Ullrich, 2004). Very simply put, defending against cyber arms is cyber arms proliferation.

Whilst in the consumer domain, customers will quickly upgrade or apply updates for their personal electronics, the same is emphatically not true of larger organizations. Vulnerabilities in the systems of businesses, government, and critical infrastructure linger unattended and unresolved for years to decades (Ablon and Bogart, 2017). It is difficult, perhaps impossible, to mitigate the damage of disclosure and proliferation when the systems most likely to be targeted by nation-states are not maintained.

5 Negative peace refers to the absence of violence. When, for example, a ceasefire is enacted, a negative peace will ensue. It is negative because something undesirable stopped happening (e.g. the violence stopped, the oppression ended). Positive peace is filled with positive content such as restoration of relationships, the creation of social systems that serve the needs of the whole population and the constructive resolution of conflict. Retrieved from http://www.irenees.net/bdf_fiche-notions-186_en.html (accessed October 22nd, 2018).

6 Japan has ostensibly given up nuclear weapons and aren't a nuclear state. However, they have a peaceful missile development program under the auspices of the Japan Aerospace Exploration Agency (JAXA), have the expertise and materials to build a bomb in a short period, and even have spy satellites monitoring North Korea. In short, Japan did not limit their nuclear technology development. Instead Japan went the peaceful route of plausible deniability.

However, even ignoring this reality and pushing forward with proliferation controls, it is necessary to return to the earlier point of communication control. Nuclear weapons research is "born classified"; where dissemination of said information is under strict control within the context of the NPT. The atom and how it can be split is nevertheless public knowledge. For cyber arms, in the their current form, the line between a useful weapon and the knowledge of a vulnerability is thin. The mere vague announcement of a vulnerability in a piece of critical infrastructure has attracted the attention of third-party researchers, rendering attempted information embargos quickly moot (Goodin, 2008). Preventing cyber arms proliferation would mean censoring the existence of cyber arms. Mass censorship is, at least presently, the hallmark of an authoritarian state and not something any peaceful or progressive nation does to itself (Freedom House 2017).

4. Conclusion

Cyber arms control is something that should be considered because it would allow for regulation of offensive cyber arms and limit their development and use. Such would limit a possible arms race, reduce the risk of misperceived cyber threats and increase cyber international relations. Interested actors such as Japan, and even the United States, China and Russia are exploring the possibility of a cyber arms treaty. With an arms race taking off, and with no finish line in sight, it remains to be seen to what cyberspace would evolve in the near future: a space where conflict would be increasingly the norm? Furthermore, with cyber threats increasingly affecting physical targets, there are reasons to explore what can be done to limit cyber arms impact and possible damage on physical infrastructure. It has been argued that a "cyber Pearl Harbor" has not taken place, and that it seems unlikely that such worst case scenarios will occur. Yet, as our nascent cyber rules and norms are slowly changing, eroding even, there is a significant risk that cyber arms will spiral out of control and a) threat will be misperceived, b) nations will seek strong efforts in the cyber race, and c) could explore the increasing use of cyber weapons. Each of these points will have ramifications on existing security frameworks and relations.

In the past, the framework of conventional and nuclear arms control has been effective. In the cyber world, arms control would not work: it would be ineffective, only giving the impression that efforts are being made to limit an arms race. It could even backfire, hurting basic research, and industry defensive cyber security efforts such as Google Project Zero.[7] The new nature of cyberspace, as well as digital technology, require a different approach. Contemporary and future societies are changing as a result of the digital revolution. Cyberspace, as man-made space, is the outstanding example of it. As the world changed because of the digital revolution, it seems appropriate to find new feasible concepts and attitudes for arms control, limiting a cyber arms race. What's needed are concepts and attitudes not based on 20th century cyber arms control concepts, but that are germane to a digital environment.

Humanity is unlikely to establish an effective framework for arms control in cyberspace soon. Due to perceptions and misperceptions of cyber threats, there is a risk of a further escalation leading to an arms race. It is therefore time to consider other options to deal with the impact of human fears and the human approach to cyber security. In his article, Metz (2016) introduces non-human efforts effective in enhancing cyber security defense. This direction should be further researched to understand if non-human security efforts, based on artificial intelligence and robotic systems, could contribute to a viable framework for cyber arms control. In a 21st century environment, where automation and autonomous systems have gained influence, the idea of automated and autonomous cyber security systems is one that deserves further research and should be explored. Such will be the topic of next article which will explore the impact of artificial intelligence on cyber affairs.

Tobias Burgers is a doctoral candidate, Otto Suhr Institute, Free University Berlin and currently a visiting researcher at the Keio Global Research Institute, Keio University, Japan. His research focuses on new technologies – AI, cyber and robotic – and their impact on international security relations.

David R.S. Robinson is an expert in information technology. Over his 20-year career, he has consulted in the public and private sectors and presented at conferences on topics such as institutional culture, software development, and community organisation. He is an alumnus of Microsoft and ThoughtWorks.

References

Ablon, L., & Bogart, T. (2017) Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits. RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR1751.html

Amoroso, E. G. (2012). Cyber attacks: protecting national infrastructure. Elsevier. pp.4-33.

Arkin, W. M. (1999, March 29). Sunrise, Sunset. Washington Post. Retrieved June 2, 2018, from https://www.washingtonpost.com/wp-srv/national/dotmil/arkin032999.htm

Avgerinos, T., Cha, S. K., Rebert, A., Schwartz, E. J., Woo, M., & Brumley, D. (2014). Automatic exploit generation. Communications of the ACM, 57(2), 74-84.

Bull, H. (1966). The control of the arms race: Disarmament and arms control in the missile age. New York: Praeger.

Bumiller, E., & Shanker, T. (2012, October 11). Panetta Warns That U.S. Is Vulnerable to Cyber-Pearl Harbor. The New York Times. Retrieved February 26, 2018, from http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

Burgers, T. & Robinson, D.R.S. (2016), Networked Authoritarianism Is on the Rise, in Sicherheit und Frieden/Security and Peace, 34(4), 248–252.

Borghard, E. D., & Lonergan, S. W. (2018, January 16). Why Are There No Cyber Arms Control Agreements?, Retrieved March 1, 2018, from https://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements

Boulanin, V. (2013, May 30). Arms production goes cyber: a challenge for arms control Stockholm International Peace Research Institute. Retrieved from https://www.sipri.org/node/361

Bronk, C., & Wallach, D. (2013, March 26). Opinion: Cyber arms control? Forget about it. Retrieved June 2, 2018, from https://edition.cnn.com/2013/03/26/opinion/bronk-wallach-cyberwar/

Cavelty, M. D. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse, International Studies Review 15(1),105-122.

Craig, A., & Valeriano, B. (2016). Conceptualising Cyber Arms Races. In 2016 8th International Conference on Cyber Conflict Cyber Power, Pissanidis, N., Rõigas, H. & Veenendaal M. (Eds.),141-158, Tallinn: NATO CCD COE Publications.

Dittrich, P., & Boening, B. (2017). More security in cyberspace: The case for arms control. Security Policy Working Paper, (9), 1-5, BAKS Federal Academy for Security Policy, Berlin, Germany.

7 "The role of the Project Zero team is to find vulnerabilities in popular software products, including those created by Google itself. When the research team discovers and validates the [existence] of a vulnerability, the team reports the bug to the company responsible for the software and gives the company 90 days to fix the problem." Retrieved from https://searchsecurity.techtarget.com/definition/Google-Project-Zero (accessed October 22nd, 2018).

Freedom House. (2017). Freedom on the Net 2017. Retrieved from https://freedomhouse.org/report/freedom-net/freedom-net-2017

Floridi, L. (2007). A Look into the Future Impact of ICT on Our Lives. The Information Society,23(1), 59-64. doi:10.1080/01972240601059094

Galeotti, M. (2018, January 31). Size Doesn't Matter for Spies Anymore. Retrieved March 01, 2018, from https://foreignpolicy.com/2018/01/31/size-doesnt-matter-for-spies-anymore/

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: National level strategic approach. Automatika, 58(3), 273-286. doi:10.1080/00051144.2017.1407022

Glenny, M. (2011, October 12). The Cyber Arms Race Has Begun. Retrieved February 26, 2018, from https://www.thenation.com/article/cyber arms-race-has-begun/

Goodin, D. (2008, July 21). Researcher's hypothesis may expose uber-secret DNS flaw. The Register. Retrieved from https://www.theregister.co.uk/2008/07/21/dns_flaw_speculation/

Healey, J. (2013a). A fierce domain: Conflict in cyberspace, 1986 to 2012. Vienna, VA: Cyber Conflict Studies Association.

Healey, J. (2013b). The Lessons of Cyber Conflict History, So Far…. Atlantic Council. Excerpted from the introduction of A Fierce Domain: Cyber Conflict 1986 to 2012.

Healey, J. (2016, November 1). The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers. Columbia University, School of International and Public Affairs, Journal of International Affairs. Retrieved from https://jia.sipa.columbia.edu/online-articles/healey_vulnerability_equities_process

Hurwitz, R. (1999). Who Needs Politics? Who Needs People? The Ironies of Democracy in Cyberspace. Contemporary Sociology,28(6), 655-661. Retrieved from http://www.jstor.org/stable/2655536

International Data Corporation. (2017, March 29). Worldwide Spending on Security Technology Forecast to Reach $81.7 Billion in 2017, According to New IDC Spending Guide. Retrieved June 1, 2018, from https://www.idc.com/getdoc.jsp?containerId=prUS42425417

Jellenc, E. (2012). Explaining Politico-Strategic Cyber Security: The Feasibility of Applying Arms Race Theory. In 11th European Conference on Information warfare and security: ECIW2012, (20), 151-162). Reading: Academic Publishing.

Jenkins, H., Thorburn, D. (2003). Introduction: Digital Revolution, Informed Citizen and the Culture of Democracy, in Democracy and new media, 1-17, Jenkins, H and Thorburn, D. (eds.).

Jervis, R. (1976). Perception and misperception in international politics. New Jersey: Princeton University Press.

Kaspersky, E. (2012, July 3). What Are The Top IT Security Threats? Retrieved March 01, 2018, from https://eugene.kaspersky.com/2012/07/03/worse-than-cheese-five-main-issues-of-it-security/

Kehler, C. R., Lin, H., & Sulmeyer, M. (2017). Rules of engagement for cyberspace operations: A view from the USA. Journal of Cybersecurity, 3(1), 69-80. doi:0.1093/cybsec/tyx003

Kung, L., Kröll, A., Ripken, B., & Walker, M. (1999). Impact of the Digital Revolution on the Media and Communications Industries. Javnost – The Public Journal of the European Institute for Communication and Culture, 6, 29-47. doi: https://doi.org/10.1080/13183222.1999.11008717

Kydd, A. (2000). Arms Races and Arms Control: Modeling the Hawk Perspective. American Journal of Political Science, 44(2), 228-244. doi:10.2307/2669307

Levy, S. (2001). Crypto: How the code rebels beat the government--saving privacy in the digital age. Penguin Press.

Limnéll, J. (2016). The cyber arms race is accelerating – what are the consequences? Journal of Cyber Policy, 1(1), 50-60. doi:10.1080/23738871.2016.1158304

Litwak, R., & King, M. (2015). Arms Control in Cyberspace? (Wilson Briefs, pp. 1-8, Issue brief). Washington, DC: Woodrow Wilson International Center for Scholars.

Macak, K. (2017, July 18). From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers | Leiden Journal of International Law. Retrieved February 26, 2018, from https://www.cambridge.org/core/journals/leiden-journal-of-international-law/article/from-cyber-norms-to-cyber-rules-reengaging-states-as-lawmakers/63A45029B685C11BBD9512AC0459FAE5

Maybaum, M., & Tölle, J. (2016). Arms control in cyberspace – architecture for a trust-based implementation framework based on conventional arms control methods. Cyber Conflict (CyCon), 2016 8th International Conference on, 159-174. doi:10.1109/CYCON.2016.7529433

McAfee. (2012, January 30). 57% Believe a Cyber Arms Race is Currently Taking Place, Reveals McAfee-Sponsored Cyber Defense Report. Retrieved March 01, 2018, from https://www.mcafee.com/us/about/news/2012/q1/20120130-02.aspx

Metz, C. (2016, June 03). Will Humans or Bots Rule Cybersecurity? The Answer Is Yes. Retrieved February 27, 2018, from https://www.wired.com/2016/08/will-humans-bots-rule-cybersecurity-answer-yes/

Meyer, P. (2012) Diplomatic Alternatives to Cyber-Warfare, The RUSI Journal, 157(1), 14-19, DOI: 10.1080/03071847.2012.664357

Mimran, D. (2017). The cyberspace arms race: artificial intelligence & cyber security (Issue brief). The Forum Network (OECD).

Modderkolk, H. (2018, January 25). Dutch agencies provide crucial intel about Russia's interference in US-elections. De Volkskrant. Retrieved from https://www.volkskrant.nl/tech/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~a4561913/

Nakashima, E. (2017, November 15). Trump administration pulls back curtain on secretive cybersecurity process. The Washington Post. Retrieved from https://www.washingtonpost.com/world/national-security/trump-administration-pulls-back-curtain-on-secretive-cybersecurity-process/2017/11/15/f9a2e3ec-ca16-11e7-aa96-54417592cf72_story.html

Netanyahu,, B. (2017, June 26). PM Netanyahu addresses TAU Cyber-Tech conference. Retrieved from http://mfa.gov.il/MFA/PressRoom/2017/Pages/PM-Netanyahu-addresses-TAU-Cyber-Tech-conference-26-June-2017.aspx

Noor, E. (2015). Strategic Governance of Cyber Security: Implications for East Asia. In Navigating Change: ASEAN-Japan Strategic Partnership in East Asia and in Global Governance, 150-163, Rizal Sukma and Yoshihide Soeya (eds), Japan Center for International Exchange, Tokyo, Japan.

Nye Jr., J. S. (2011a). Nuclear Lessons for Cyber Security? Strategic Studies Quarterly, 5(4), 18-38.

Nye Jr., J. S. (2011b). The Future of Power, Public Affairs, NYC, New York

Nye Jr., J. S. (2015, October 01). The world needs new norms on cyberwarfare. Retrieved February 26, 2018, from https://www.washingtonpost.com/opinions/the-world-needs-an-arms-control-treaty-for-cybersecurity/2015/10/01/20c3e970-66dd-11e5-9223-70cb36460919_story.html?utm_term=.0492eca3e247

Poulsen, K. (2001, June 15). Solar Sunrise hacker 'Analyzer' escapes jail. Retrieved from https://www.theregister.co.uk/2001/06/15/solar_sunrise_hacker_analyzer_escapes/

Rid, T. & Buchanan, B. (2014) Attributing Cyber Attacks, In Journal of Strategic Studies, 38(1-2)

Rid, T., & McBurney, P. (February/March 2012). Cyber-Weapons. RUSI Journal, 157(1) 6–13.doi: 10.1080/03071847.2012.664354

Robinson, N., Gribbon, L., Horvath, V., & Robertson, K. (2013). Cyber-security threat characterisation A rapid comparative analysis (pp. 1-86, Rep.). Santa Monica, CA: RAND.

Rosenzweig, P. (2015, February 26). Problems with Cyber Arms Control. Retrieved June 01, 2018, from https://lawfareblog.com/problems-cyber-arms-control

Science and Technology Facilities Council. (2018). A BRIEF HISTORY OF THE DIGITAL REVOLUTION. Retrieved February 24, 2018, from https://www.stfc.ac.uk/files/digital-revolution-infographic/

Schelling, T. C., & Halperin, M. H. (1961). Strategy and arms control. New York: The twentieth century fund.

Schwartz, A. & Knake, R. (2016) Government's role in vulnerability disclosure: Creating a permanent and accountable vulnerability equities process, discussion paper 04, Belfer Center for International Affair Harvard Kennedy School.

Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: what everyone needs to know. New York: Oxford University Press.

Slayton, R. (2017). What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment. International Security, 41(3), 72-109. doi:10.1162/isec_a_00267https://doi.org/10.1162/ISEC_a_00267

Smith, B. (2017, March 09). The need for a Digital Geneva Convention. Retrieved March 01, 2018, from https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

Stavridis, J. (2017, May 15). The United States Is Not Ready for a Cyber-Pearl Harbor. Retrieved February 26, 2018, from http://foreignpolicy.com/2017/05/15/the-united-states-is-not-ready-for-cyber-pearl-harbor-ransomware-hackers-wannacry/

Stecklow, S., & Fassihi, F. (2009, December 11). Thousands Flee Iran as Noose Tightens. Wall Street Journal. Retrieved from https://www.wsj.com/articles/SB126049484505086861

Stein, J. (2013). Threat Perception in International Relations. In the Oxford Handbook of Political Psychology.: Oxford University Press. Retrieved 26 Feb. 2018, from http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199760107.001.0001/oxfordhb-9780199760107-e-012.

Tsipori, T. (2016, April 4). Israeli cybersecurity grabs 8% global market share. Retrieved May 31, 2018, from https://www.globes.co.il/en/article-israeli-cyber-industry-hits-the-big-time-1001114669

Tynkkynen, M. (2016). NEW TECHNOLOGIES – Risks and opportunities: Overview of the challenges and opportunities arising from new and developing technologies in risk management and workers' compensation insurance., for The Finnish Workers' Compensation Center, Analyses No 7E

Ullrich, J. (2004). The Disappearing Patch Window. Observations from the Internet Storm Center, SANS.

U.N. General Assembly, 50th Session. Verification in all its aspects, including the role of the United Nations in the field of verification (A/50/37). 22 September 1995.

U.N. General Assembly, 79th Plenary Meeting. General and complete disarmament (A/RES/51/45). 10 December 1996.

UN General Assembly (2013, June 24th) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98.

Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber realities: cyber conflict in the international system. New York: Oxford University Press.

Vacca, J. R. (2012). Computer and information security handbook. Newnes.

Walt, S. (1985). Alliance Formation and the Balance of World Power. International Security, 9(4), 3-43. doi:10.2307/253854

Ward, D., & Morgus, R. (2016). Professor Cy Burr's Graphic Guide to: International Cyber Norms, 1-26, New America.

White House (2017) Vulnerabilities equities policy and process for the United States government, White House Report.

Wirth, A. (2016) 'The Cyber Arms Race Is On': Lessons from the U.S. Presidential Election. Biomedical Instrumentation & Technology: 50 (6), 463-465.

Wirtz, J. J. (2017). The Cyber Pearl Harbor. Intelligence and National Security, 32(6), 758-767. Doi: https://doi.org/10.1080/02684527.2017.1294379

Wolter, D. (2013, September). The UN Takes a Big Step Forward on Cybersecurity. Retrieved June 2, 2018, from https://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity#source

Zetter, K. (2015, May 15). Feds says that banned researcher commandeered a plane. Retrieved February 26, 2018, from https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/