EUROPEAN
LEADERSHIP
NETWORK

# Managing the Cyber-Nuclear Nexus

POLICY BRIEF

Andrew Futter

July 2019

## About the author

**Dr Andrew Futter** is an Associate Professor in International Politics and Director of Research for Politics and IR 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); Reassessing the Revolution in Military Affairs (2015); and The United Kingdom and the future of nuclear weapons (2016) 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.

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 also a Member of the Younger Generation Leadership Network.

The opinions articulated in this report represent the views of the author, and do not necessarily reflect the position of the European Leadership Network or any of its members. The ELN's aim is to encourage debates that will help develop Europe's capacity to address pressing foreign, defence, and security challenges.

# Managing the Cyber-Nuclear Nexus

Andrew Futter[1]

Concern about cyber increasingly impacts all aspects of nuclear security, nuclear operations and nuclear thinking. The wide range of dynamics that fall under the cyber moniker are both changing and transforming the nature, capabilities and vulnerabilities of nuclear weapons, as well as the broader context within which security policy and warfare are conducted. This in turn has meant that states are wrestling with new issues of deterrence, arms control and stability as well as the safety, security and management of nuclear weapons and the future shape of the global nuclear order.

But what we mean by cyber and the cyber threat varies considerably across cases. This often causes more confusion than clarity and has made formulating credible and feasible responses difficult. It also often leads to worst-case scenarios and hype; the spectre of a "cyber 9-11" being a good example, or a repeat of the storyline from the 1983 film WarGames. The language we use when describing the challenge is therefore fundamental to finding solutions. Cyber threats are not homogenous, the impact of cyber is diverse and differentiated, and as a result there is not a one-size-fits all solution to the problem at the nuclear level. Challenges are also likely to be different for different states, and humans – as well as software, hardware and networks – are a central part of the cyber phenomenon. This in turn means that we may need to think differently about how we manage, moderate and perhaps mitigate the effects of these new challenges, and that the frameworks and thinking that shaped our nuclear past may not necessarily be the best place to start when addressing our cyber-nuclear future.

Consequently, in what has become an increasingly vociferous but also obfuscated policy and academic debate about cyber and the impact on nuclear weapons, we need to go back to basics. This will involve: (i) more clarity about the particular problem(s) posed by cyber to nuclear weapons and the language we use to describe these; (ii) a realistic assessment of what can, can't and should be done in this space and who ought to be responsible for it; and (iii) a recognition that the methods and mechanisms we need to adopt and apply today might be different from those of the past.

## What is cyber and what is the cyber threat?

This is arguably the most important part of the cyber challenge, and the question that often gets ignored or overlooked. Different actors, analysts, policymakers and even states use the term to refer to different things with very different dynamics and implications. Then Republican presidential candidate Donald Trump referring to doing "the cyber" better in a 2016 debate with Democratic hopeful Hilary Clinton is a good example of this.[2] It therefore needs to be recognised that cyber is an inherently nebulous and contested term. For some, cyber refers discretely to Computer Network Operations (CNO) and logical attacks against computer systems and networks, for others it is more akin to Information Warfare and therefore might involve manipulation of information or even of hardware and people, while the broadest conceptualisation uses the term to refer to a new digital age, which

[1] Associate Professor, University of Leicester, U.K. ajf57@le.ac.uk

[2] Adrienne Lafrance, "Trump's incoherent ideas about 'the cyber'." The Atlantic, (26 September 2016), https://www.theatlantic.com/technology/archive/2016/09/trumps-incoherent-ideas-about-the-cyber/501839/

essentially encompasses everything. Each of these clearly have different focuses, referents and agendas, and implications for nuclear weapons, ranging from manipulation of the nuclear-information space, cyber-nuclear espionage, protection of the digital and physical supply chain, and direct attacks on weapons systems infrastructure and people.

A way around this is to conceptualise the cyber challenge into: (i) a new set of capabilities that might be used and vulnerabilities that might be exploited within the computer systems and networks used across the nuclear weapons enterprise; and (ii) the broader context and environment within which nuclear policy is carried out. The former is about malware, cyber-attacks, bugs, and hacking, while the latter is about the digitised information space that all states operate in. There is even a case to be made that we should stop using the word cyber altogether, and instead revert back to the more precise language of Computer Network Attacks, Computer Network Defence, Computer/Network/Information Security, etc.[3] More precision in terminology is undoubtedly the first step towards constructing meaningful and tailored measures to deal with specific cyber challenges in the nuclear realm.

It is also important to note that there is no single cyber-threat. Instead, we are better off thinking of a diverse spectrum of threats and challenges with varying degrees of seriousness for nuclear weapons. This is because the vast amount of what we label as cyber-attacks are not really "attacks" at all, and certainly shouldn't be seen through the lens of "warfare". Nuisance, hacktivism, crime, espionage and Intellectual Property theft account for most of the cyber challenge – and only some of these apply to nuclear weapons directly. The threat of causing damage or destruction to nuclear systems is actually a niche part of the threat (albeit clearly very worrying), and we only know of a handful of examples of physical effects happening due to digital operations – Stuxnet[4] being most widely known about. Moreover, if you remove the cyber prefix, many of these challenges and methods are not really "new" either.

We might also break-up the cyber-threat to nuclear weapons into direct (hack into the system, deploy malware, cause damage and disruption, etc.) and indirect operations (that seek to alter the information and data upon which these systems rely). In most cases, cyber capabilities are also likely to be used alongside and to augment other kinetic military capabilities, including potentially nuclear weapons: preparing the battlefield, attacking enemy communications and networks, preventing weapons from being used, and facilitating attacks with kinetic forces. It is therefore difficult to envisage a pure cyber-war fought by and against computers, "geek versus geek", at least for the near future. Instead, we are likely to see conflict between nuclear-armed adversaries that takes place within a cyber environment. Lastly, often the easiest target in a cyber operation are humans. It is much easier to dupe humans through phishing attacks or social engineering than bypass sophisticated defences and firewalls. The cyber challenge is therefore inherently human: humans write coding, enter data, build systems, and make decisions based on human-made computers. Albeit Artificial Intelligence could change this in the future.

[3] See Andrew Futter, "Cyber' semantics: Why we should retire the latest buzzword in security studies," Journal of Cyber Policy, 3:2 (2018), pp.201-216.

[4] Stuxnet was the malware believed to be part of a cyber-attack against the control systems managing the Iranian uranium enrichment facility at Natanz.

“Cyber threats are not homogenous, the impact of cyber is diverse and differentiated, and as a result there is not a one-size-fits all solution to the problem at the nuclear level.”

## The cyber threat to nuclear weapons[5]

So far, the majority of the cyber-nuclear challenge has been espionage and protecting design and operational secrets (both for operational security reasons and to guard against computer-enabled proliferation). But the most serious threats of damage and disruption to nuclear weapons are real, and no nuclear system will be completely invulnerable to a well-equipped and determined adversary, no matter what policymakers like to think and often claim. Indeed, many leading figures have publicly questioned whether U.S., U.K., Russian or Chinese nuclear (and other) weapons are safe from attack, and the same must be true for France, India, Pakistan, Israel and North Korea.

> ***"Hacking into a nuclear weapon would undoubtedly be very hard, but no nuclear system or its support systems are invulnerable."***

However, the challenge should be divided into cyber attacks seeking to disable nuclear systems and prevent them from functioning as expected, and those attacks that seek to enable systems, such as causing a launch or explosion. In general, nation states seem likely to seek to prevent systems from working while non-state actors may be more interested in causing a launch/ explosion or in exacerbating a crisis. Nation states will probably be more capable because they are likely to have more time and resources, and because cyber is just one part of a terrorist's toolkit, and possibly not the most useful for many of their purposes. It is also possible that a cyber-attack against other critical civilian national infrastructure, such as a power grid, could have unknown nuclear escalatory potential during a crisis. Indeed, it is this unspecified interrelationship between cyber capabilities, signalling, civilian and military targets, and inadvertent and unintended escalation that perhaps represents one of the biggest risks when it comes to how nuclear weapons could come to be employed in the future.

Hacking into a nuclear weapon would undoubtedly be very hard, but no nuclear system or its support systems are invulnerable. A good example is the U.K. Trident system: certainly, it would be very difficult to hack the submarine while on patrol somewhere at the bottom of the North Atlantic, but the submarine and its weapons systems rely on coding written by humans for all aspects of its operations, and it is regularly patched and updated when in port.[6] Both provide potential access points for attackers wishing to deploy malware that might be used or triggered at a later date. Likewise, an adversary might attack early warning systems or command and control infrastructure as an aggressive, coercive or even pre-attack action. The 2007 Israeli bombing of a suspected Syrian nuclear facility, where hackers purportedly neutralised Syrian air defence radar, is a good example of this.[7]

Finally, in recent years we have seen the development of military doctrine that plans for the use of offensive cyber capabilities against an adversary's missile and nuclear programmes. This is known as "full spectrum missile defence" or "left of launch", and for the moment is a specifically U.S. programme. The idea is to augment kinetic missile defence capabilities with digital ones that can prevent weapons from being used, and this may have been the reason for a series of failed North

[5] For an overview see Andrew Futter, Hacking the Bomb, (Georgetown University Press: 2018).

[6] See Andrew Futter, "Is Trident safe from cyber-attack?", European Leadership Network, (February 2016), https://www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/Is-Trident-safe-from-cyber-attack-1.pdf

[7] See David Fulghum, "Why Syria's air defences failed to detect Israeli's", Aviation Week and Space Technology, (3 October 2007), www.imra.org.il/story.php3?id=36291

Korean missile tests in 2017.[8] The move towards incorporating this capability into the U.S. deterrence mission was reiterated in the Trump administration's 2019 Missile Defense Review.[9] This is a dangerous development given the clear pre-emptive and preventative nature of such operations, and risks setting a dangerous precedent if others choose to follow suit.

## What is and should be done?

There is clearly a recognition that more needs to be done to mitigate and control the myriad new challenges posed by what we term as cyber. But while there have been some successes, the cupboard remains bare in terms of agreements and international infrastructure, particularly when it comes to nuclear weapons. At least part of the reason for this is a lack of agreement about what the challenge/ problem is, and a concurrent issue about what actually should be controlled, prohibited or encouraged, by whom and how.

For sure, a few rules and conventions currently exist. These include the Budapest Convention (2001) which harmonises international laws on cybercrime[10]; and the reports from the U.N. Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security established in 2004.[11] There are also a number of other bilateral initiatives in various stages of development, such as the U.S.-Russia cyber hotline established in 2013.[12] And the Tallinn Manual is a very useful attempt to understand the relationship between cyber and international law. But the manual is an academic, non-binding study on how international law applies to cyber conflicts and cyber warfare written at the invitation of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence by an international group of experts. It is not a globally accepted glossary or rule-book.[13] There are currently no formal international agreements linking nuclear weapons and cyber capabilities.

> ***"Arms control is possible in the cyber realm and for the cyber-nuclear nexus, but it will not necessarily look like the arms control of the past."***

At least in part to fill this void, most states now dedicate considerable civilian and military resources to the "cyber" challenge. The U.S. established a "Cyber Command" in 2009 to direct military operations, the U.K. established a "National Cyber Security Centre" and "Cyber Security Operations Centre" in 2016, and NATO has run a "Cooperative Cyber Defence Centre" since 2008. Russia, China, Israel and many other states have also established "cyber" divisions and capabilities within their militaries and/or intelligence agencies. There has also been a move to categorise cyber-space as a separate domain of military

[8] David Sanger & William Broad, "Trump inherits a secret cyberwar against North Korean missiles", The New York Times, (4 March 2017), https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html

[9] U.S. Department of Defense, Missile Defense Review, (January 2019), https://www.defense.gov/Portals/1/Interactive/2018/11-2019-Missile-Defense-Review/The%202019%20MDR_Executive%20Summary.pdf

[10] Council of Europe, Treaty Number 185, "Convention on Cybercrime", (23 November 2001), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[11] See the 2015 report: http://www.un.org/ga/search/view_doc.asp?symbol=a/70/174

[12] See, "FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security", The 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

[13] Michael Schmitt, Tallinn manual 2.0 on the international law applicable to cyber warfare, (Cambridge University Press: 2017). Also available at: https://ccdcoe.org/research/tallinn-manual/

operations, notably by NATO, in recognition that this will have a significant impact on all future conflict. But this is problematic. Russia and China probably have a more efficacious understanding of the cyber challenge, seeing it as much more integrated across domains. Creating a domain seems to suggest the need to respond within that domain: i.e. a cyber response to a cyber-attack, which may neither be feasible nor proportional at the most serious end of the threat spectrum.

> ***"There are currently no formal international agreements linking nuclear weapons and cyber capabilities."***

This of course leads to questions of deterrence, and what role if any nuclear weapons should play in deterring cyber threats, and vice versa. But it is still unclear how cyber-deterrence will work in practice given the difficulties of establishing red-lines, achieving timely and confident attribution, and the fact that strategic cyber operations are unlikely to be carried out on their own. That said, cyber-deterrence (and attribution) are not the black-and-white issue that some seem to believe; it is entirely possible that deterrence can work in some situations, though perhaps not all, and attribution is usually a function of time and forensic capabilities rather than zero-sum. It is also clear that any cyber-attack against a state with nuclear weapons would run the risk – however slight – of a nuclear response. Albeit, that for most conceivable acts of cyber-aggression a nuclear response may currently seem neither proportional nor credible.[14] In general, we are probably better off thinking about cross-domain deterrence rather than cyber deterrence per se, and about the right mixture of deterrence by both denial (prevention) and punishment (retaliation after an attack).

Arms control is possible in the cyber realm and for the cyber-nuclear nexus, but it will not necessarily look like the arms control of the past. It will likely involve both formal and informal mechanisms, and both focussed and general applications. The most productive way forward for cyber arms control – both in general and in relation to nuclear weapons – may be to look for particular issue areas and problems that might be controlled in some way, rather than seeking a holistic all-encompassing solution. An edifice of cyber-nuclear arms controls rather than a single agreement. This should include unilateral mechanisms such as regular red teaming[15] and internal scrutiny, such as that provided by the U.S. General Accountability Office, as well as bilateral or multilateral initiatives.[16] It may also involve focusing on reducing incentives rather than reducing capabilities, and prohibiting attacks on certain targets rather than seeking to limit "cyber-weapons". We also need to be clear where responsibility lays: many challenges to the nuclear enterprise are best addressed through cyber-hygiene, that is better information, computer and network security and practices, rather than international agreements. Some of the responsibility is therefore incumbent upon individuals as much as governments.

Confidence building measures regarding cyber threats are of course hampered by issues of intangibility, verification and monitoring (classic apparatuses of the past), but this does not mean that expert and intergovernmental dialogue cannot be useful. Cyber early warning, sharing best practice and diagnosis, exchanges, and moratoria on attacking certain targets could be good ideas. All of this could be done through the U.N. Conference on Disarmament and GGE

[14] U.S. Department of Defense, Defense Science Board, "Resilient military systems and the advanced cyber threat", (January 2013), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf

[15] That is groups of experts hired to test systems by trying to break into or disrupt them.

[16] U.S. General Accountability Office, "Weapons systems cybersecurity: DOD just beginning to grapple with the scale of the problem", Report to the Committee on Armed Services, U.S. Senate, (October 2018), https://www.gao.gov/assets/700/694913.pdf

in the first instance, through international organisations or even through ad-hoc groups of states or non-governmental personnel. It is at least conceivable that states could sign up to a convention not to target each other's nuclear weapons and associated systems, although of course this would be very difficult to monitor, or might at least state publicly the dangers of doing so. It might also be useful to think in terms of pathways to nuclear use rather than focus on particular systems or capabilities – finding common agreement on risky and dangerous scenarios and working to understand how these can be avoided, rather than seeking to ban and moderate specific "weapons". For example, gaming out certain scenarios and challenging the canon of thought on escalation and crisis management. Another response to the challenge is to bring together experts from different backgrounds in order to establish an "epistemic community" to address cybersecurity threats, and the more niche issues of the cyber-nuclear nexus. This is not a social science or hard science problem–but a challenge that requires both sets of expertise and "new thinking".

While it won't make things easier, certain cyber issues might need to be included in established international arms control agreements rather than treated separately. Indeed, we have probably reached a point where focussing solely on nuclear weapons at Non-Proliferation Treaty Review Conferences or in bilateral arms control is no longer practical. Instead, we should see cyber challenges as part of a broader suite of emerging disruptive non-nuclear technologies that threaten national security and strategic stability, and which therefore must be treated holistically. We increasingly live in a much more blurred nuclear world where advanced conventional and unconventional weapons systems are complicating our understanding of nuclear order and established nuclear axioms.

## Summary

Cyber threats – often a rather unhelpful moniker – are not homogenous. We must therefore accept that there will be many different, and hopefully complementary approaches to managing the cyber challenge to nuclear weapons, utilising many different tools and mechanisms. Many of these will be relatively mundane, won't involve sophisticated operations or technical fixes, and some activities in cyberspace we may simply have to accept as unwelcome but inevitable (nuclear-related IP theft for example). The challenges and threats posed by cyber also need to be seen as part of a broader contextual shift in international politics driven by the latest information and technology revolution. This is because often what we refer to as cyber – the ubiquitous use of social media and a real-time information context – are not cyber but rather the manifestation of a new digitised environment.

As we move forward, we need to keep some of these nuances in mind, and make sure we have properly diagnosed and understood the problem before we start searching for answers. Thus, a number of key dynamics stand out. First, the use of language is fundamental to how we understand and mange cyber challenges to nuclear weapons. Second, not every cyber threat in the nuclear realm is equal. Third, intentions are as important as capabilities: just because an actor could or might be able do something to another's nuclear forces doesn't mean that they will. Fourth, treating cyber as a military domain is unlikely to be very helpful in reality when in comes to nuclear issues. Fifth, humans, cyber-hygiene and good practice are as important as sophisticated technological fixes. Sixth, deterring cyber threats will be as much about defence, security and minimising vulnerabilities as about credible forms of retaliatory threats or (nuclear) punishment (the bedrock of the nuclear era). Lastly, above all, we need to recognise that meeting this challenge will require thinking outside the box, and the application of new mechanisms and approaches to security, arms control and confidence building.

Ultimately, the best approach to these challenges is to disaggregate and triage the threat, find things that states can agree on, accept that not everything can be regulated, and work from the bottom-up rather than seeking an all-compassing agreement. As I have argued elsewhere, this might be aided by keeping nuclear weapons separate from other military systems, as secure as possible, and simple – that is, only using as much technology as is really needed – as a way to minimise many of the challenges that we face in the cyber era. Lastly, it is also important to remember that the essence of the cyber challenge is not new, and we have been faced with periods of significant technological change in the nuclear realm before. But the key is in how we think about the problem and in recognising that we are at the start of a long journey.

EUROPEAN
LEADERSHIP
NETWORK

**The European Leadership Network (ELN)** works to advance the idea of a cooperative and cohesive Europe and to develop collaborative European capacity to address the pressing foreign, defence and security policy challenges of our time. It does this through its active network of former and emerging European political, military, and diplomatic leaders, through its high-quality research, publications and events, and through its institutional partnerships across Europe, North America, Latin America and the Asia-Pacific region.