56 VALDAI PAPERS

September 2016

Valdai Discussion Club
www.valdaiclub.com

NUCLEAR WEAPONS IN THE CYBER AGE: NEW CHALLENGES FOR SECURITY, STRATEGY AND STABILITY

Andrew Futter

About the author:

Andrew Futter

Senior Lecturer in International Politics, Department of Politics and International Relations, University of Leicester; Fellow of the UK Higher Education Academy

The safe, secure and reliable management of nuclear weapons has always been a complex and complicated business, plagued by uncertainty and risks. But these challenges are being magnified and aggravated by new cyber tools, dynamics and capabilities, and from the threat posed by hackers seeking to gain access to, or interfere with, nuclear systems. The challenge is myriad in its scope, and ranges from the safe, secure and reliable nuclear C2, through fresh problems for information security, proliferation, and the safeguarding of highly sensitive nuclear secrets, to new complications for strategic deterrence and escalation, and the emergence of a cyber-nuclear security dilemma. While cyber threats may not currently undermine or supersede the role of nuclear weapons as the ultimate symbol of national security, increased uncertainty about the integrity and security of these systems raises questions for nuclear force management, thinking and strategy for all nuclear-armed states. The cyber challenge is nuanced and subtle, complicating and obfuscating the intrinsic difficulties of nuclear C2 and nuclear strategy rather than fundamentally transforming them. That said, these new challenges do represent an important shift in the environment in which nuclear weapons are thought about, states manage their nuclear forces and nuclear policy and strategy is made. Accordingly, the challenge will have both direct and indirect implications not just for nuclear security and C2, but also for strategic balances, the maintenance of arms control agreements, and future nuclear reductions.

The Nature of the Cyber Challenge

The nature and meaning of cyber is contested, is viewed differently by different states and actors, and there exists no one definition that all adhere to when seeking to use the concept. The result is that different analyses come to different conclusions and offer different solutions to cyber-related problems and questions; this has complicated the cyber debate. Cyber analyses range in scope from those that use a very narrow conception and that focus primarily on Computer Network Operations (CNO) and attacks over and through the *Internet*, across a broader model that sees cyber as closer to, or as part of, the field of Information Warfare, up to analyses that treat cyber as a holistic concept effecting every part of national security thinking. On a second level, cyber analysis is also hampered by the differences between types of cyber-*attack* and particularly what is meant by, and being referred to, by the phrase. These range

from simple hacking, hacktivism and crime, through denial of service and espionage, up to sabotage, destruction and possibly war. It is this diverse nature of the scope and challenge that creates many of the problems that underpin cyber analysis, and is a key reason for the continued disagreement about the level and nature of the threat.

When considering the challenges to the nuclear weapons enterprise, it makes sense to look at all aspects of the cyber phenomenon and consider it in its broadest scope and across the physical, informational and cognitive domains, in addition to the logical domain of CNO. The framework adopted here is designed to consider the impact that the broader cyber context is having on nuclear thinking and strategy by treating cyber as an operational domain, an offensive capability, a societal development, as well as set of actors. While the discrete threat of hacking and attacks through the Internet are important, they are not the only dynamics that will impact the nuclear weapons enterprise. Instead, the challenge can be thought of as all measures designed to attack, compromise, destroy, disrupt or exploit activities involving computers, networks, software and hardware/infrastructure, as well as the people that engage with them.[1]

Cyber-attacks on nuclear weapons might be *physical*, such as those carried out by people on computers, hardware, communications nodes, wires and machines that permit the circulation and storage of information; *logical*, such as attacking the commands that tell the hardware what to do and the software that allows the transmission, interpretation and sharing of key information; carried out through computer networks and over the Internet or attacks on software, such as through certain malware, logic bombs, hardware or software Trojans, and general hacking; and by attacking the information on which these systems and therefore human operators rely.[2] It also incorporates the natural problems in increasingly complex (computer) systems and the overall uncertainty of whether key systems will always work as expected. As such, the cyber challenge involves both *inherent* vulnerabilities in nuclear systems as well as the threat from actors seeking to gain access to these systems in order to alter, disable, disrupt or damage them. Finally, humans are a key aspect of the cyber challenge: it is people that design systems, write software, and place their faith in computers and machines to carry out tasks as intended.

---

[1] *This builds on Jason Andres & Steve Winterfield, "Cyber warfare: techniques, tactics and tools for security practitioners", (Waltham MA, Syngress: 2011) p.167.*

[2] *This draws on Lucas Kello "The meaning of the cyber revolution: perils to theory and statecraft", International Security, 38:2 (2013) p.18.*

The challenge is multifaceted and impacts across every level of the cyber-nuclear nexus: from single unit variables and nuclear C2, through state level structures and national security thinking, up to international strategic relations and crisis stability. While often discrete, these challenges are also interlinked – attacks on nuclear early warning systems for example have implications for crisis stability or deterrence. It therefore makes sense to consider the impact of cyber on nuclear weapons in its entirety, and across the three levels of the nuclear enterprise: the domestic nuclear weapons complex, state-based nuclear strategy, and the international system.

New Nuclear Vulnerabilities

Nuclear systems have always been susceptible to outside interference and attack, and the past is littered with miscalculations, accidents and near misses (many caused by computers and electronic systems). This is due to the needs of *positive control* (ensuring that weapons will always work), and *negative control* (ensuring that weapons aren't ever used by accident or by unauthorised actors). This means that weapons will never be invulnerable to attackers seeking to undermine either positive or negative control. Thus cyber threats build upon, rather than fundamentally change, the complex nature of nuclear C2 (and the security of associated infrastructure). There are two implications of this; increased complexity – particularly computerisation and digitisation – raises the risk of normal accidents within the nuclear enterprise, and more complex systems used to manage nuclear forces contain inherent vulnerabilities, weaknesses and bugs might be exploited or manipulated by hackers.

The inherent vulnerabilities within nuclear C2 systems are highlighted by the number of accidents, near misses and miscalculations that litter our nuclear past. Normal accidents theory posits that complex systems will not always work as intended and will go wrong some of the time. This is particularly the case with highly pressurized systems, those that can never be fully tested, or with systems that deal with hazardous technologies.[3] Nuclear C2 is a good example of a complex system, and the atomic age is littered with accidents and near misses. While not all previous nuclear accidents have involved computers and software, a significant number have,

[3] *Charles Perrow, "Normal accidents: living with high-risk technologies", (Princeton NJ, Princeton University Press: 1999).*

and is likely to increase as systems for nuclear weapons management become more complex, digitised and intricate.

A growing reliance on computers, code and software for all aspects of nuclear weapons management – from early warning, through the protection, collation and analysis of data, up to authorizing and firing the weapons – is also creating new ways in which nuclear systems might be exploited by hackers. One of the biggest challenges here is the natural and inherent problems that are contained in ever more sophisticated and complex software and coding – such as that used for nuclear C2. Complex systems are likely to contain more bugs, problems and unforeseen errors than basic ones, especially those that rely on complex code, link multiple functions and hardware, and must make accurate computations quickly. These vulnerabilities are also the primary means that allow hackers to break into systems and circumvent their security mechanisms. While this is clearly a threat to nuclear C2, it also has significant implications for the wider nuclear weapons enterprise, particularly the security of sensitive nuclear-related information.

While nuclear systems will of course be well protected against cyber threats and almost certainly air-gapped, they are by no means invulnerable. The possibility that hackers could initiate nuclear use or disable weapons systems; indirectly spoof warning sensors; jam communications to prevent orders reaching the weapons; or access and utilise highly sensitive information about weapons systems and operational procedures, is real and growing. This is the result of an increase in the number of vulnerabilities in this software that could be exploited by a would-be attacker; both within nuclear C2, and inside the various infrastructure that supports nuclear weapons management. The concern is that hackers might compromise nuclear systems through *disabling attacks*, or by seeking to facilitate a launch or explosion through *enabling attacks*. Software vulnerabilities also make it easier to hack into related systems, and provide new ways to steal data, spoof various systems with erroneous information, or interfere, disrupt or damage critical nuclear facilities and processes.

Cyber-Nuclear Espionage

The possibility that an adversary might steal nuclear secrets (weapon designs and capabilities or operational plans and procedures) has always been a major challenge for

nuclear-armed states. But the spread of computers, networks and digitally stored data has created new problems for nuclear secrecy and has changed, expanded and diversified the methods available for nuclear espionage. The challenge is not simply hacking into secret systems and downloading information over the Internet, but also the importance of computer and information security in those systems that may already be air gapped. Both are acute issues because of the large amount of information stored on computers and that can therefore also be stolen quickly and with (relatively) minimal effort. When such attacks can be carried out remotely, the risks are reduced even further so that no human agent needs to be placed in immediate danger. Likewise, new economies of scale allow widespread espionage attacks that attempt to steal as much information as possible about all types of things, as well as the more targeted attacks on specific and specialised information.

The cyber-nuclear espionage age began in the mid-1980s as computers and networks gradually expanded throughout (particularly US) defence and military establishments, and specifically to the 1986 *Cuckoo's Egg* episode.[4] In 1991 Dutch hackers broke into US military networks searching for nuclear secrets and missile data to sell to Saddam Hussein[5]; in 1998, the Cox Report revealed that China had stolen a considerable cache of highly sensitive secrets relating to the W88 thermonuclear warhead design[6]; later that year, a hacker broke in to India's Bhabha Atomic Research Centre and downloaded passwords and emails[7]; and in 1999 the extent of the infiltration of the *Moonlight Maze* attack on the Pentagon and sensitive information held by other US government departments was revealed.[8]

This trend has continued and deepened during the last decade: in 2005 hackers linked with the Chinese PLA infiltrated numerous US military systems searching for nuclear secrets – amongst other defence information – in an operation dubbed *Titan Rain*[9]; in 2006 the Israeli Mossad planted malware in the computer of a Syrian official which revealed the extent of the suspected Syrian nuclear weapons programme and

[4] *See Clifford Stoll, "The cuckoo's egg: tracking a spy through the maze of computer espionage", (London, Doubleday: 1989).*

[5] *Dorothy Denning, "Information warfare and security", (Reading MA, Addison-Wesley: 1999).*

[6] *Quoted in Vernon Loeb & Walter Pincus, "Los Alamos security breach confirmed", The Washington Post, (29 April 1999), http://www.washingtonpost.com/wp-srv/national/daily/april99/spying29.htm.*

[7] *Adam Penenberg, "Hacking Bhabha", Forbes, (16 November 1998), http://www.forbes.com/1998/11/16/feat.html .*

[8] *Adam Elkus, "Moonlight Maze", chapter in Jason Healey (Ed), "A fierce domain: conflict in cyberspace, 1986-2012", (USA, Cyber Conflict Studies Association: 2013) p.155.*

[9] *William Hagestad, "21st century Chinese cyberwarfare", (Ely, IT Governance Publishing: 2010) p.12.*

led directly to *Operation Orchard* in 2007 (see below)[10]; in 2008 an infected USB stick left in a car park led to *Operation Buckshot Yankee* where US classified networks were breached and the air-gap was jumped.[11] In 2011 the *Zeus* Trojan aimed at contractors building the UK Trident nuclear-armed submarine force was discovered[12], Iran was accused of hacking the International Atomic Energy Agency (IAEA)[13], and the *Shady RAT* malware targeting US government agencies, defence contractors and high-technology companies was discovered[14], and in 2012 *Anonymous* threatened to release highly sensitive data on the Israeli nuclear programme stolen from the IAEA.[15]

US laboratories and defence contractors have remained a primary target for at least the last decade,[16] and hackers have also targeted the US and Israeli ballistic missile defence programmes.[17] While many of the nuclear espionage attacks (that we know about) involve attacks on the US; *Operation Olympic Games* – which would produce Stuxnet – began primarily as an intelligence gathering and espionage operation against Iranian nuclear activities. Likewise, both *Flame* and *Duqu* were designed to gain intelligence on systems and infrastructure – likely as precursor to a possible future sabotage on the Iranian nuclear programme.[18]

The implications of this are mixed. At the lower end of the scale cyber-nuclear espionage is about acquiring intelligence on what a certain state or actor is doing and the capabilities of weapons programmes. On the next level nuclear secrets may be targeted to help combat or defend against certain systems or to provide a better idea of operational procedures. Of greater concern is that nuclear secrets are stolen to aid proliferation and that

---

[10] Eric Follarth & Holger Stark, "The story of Operation Orchard: how Israel destroyed Syria's Al Kibar nuclear reactor", Spiegel Online, (2 November 2009), http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html.

[11] Karl Grindal, "Operation Buckshot Yankee", chapter in Jason Healey (eds.), "A fierce domain: conflict in cyber-space 1986 to 2012", (USA, Cyber Conflict Studies Association: 2013) p. 208.

[12] Richard Norton-Taylor, "Chinese cyber-spies penetrate Foreign Office computers", The Guardian, (4 February 2011), http://www.theguardian.com/world/2011/feb/04/chinese-super-spies-foreign-office-computers.

[13] David Crawford, "UN probes Iran hacking of inspectors", Wall Street Journal, (19 May 2011), http://www.wsj.com/articles/SB10001424052748704281504576331450055868830.

[14] William Hagestad, "21st century Chinese cyberwarfare", (Ely, IT Governance Publishing: 2010) p.12.

[15] Michael Kelley, "Anonymous hacks top nuclear watchdog again to force investigation of Israel", Business Insider, (3 December 2012), http://www.businessinsider.com/anonymous-hack-iaea-nuclear-weapons-israel-2012-12?IR=T

[16] "US nuclear weapons researchers targeted with Internet Explorer virus", Russia Today, (7 May 2013), http://rt.com/usa/attack-department-nuclear-internet-955/.

[17] See Andrew Futter, "Hacking missile defense: the cyber challenge to BMD", The Missile Defense Review, (1 March 2015), http://missiledefensereview.org/2015/03/01/hacking-missile-defence-the-cyber-challenge-to-bmd/.

[18] Chris Morton, "Stuxnet, Flame and Duqu – the Olympic Games", chapter in Jason Healey (eds.), "A fierce domain: conflict in cyberspace 1986 to 2012", (USA, Cyber Conflict Studies Association: 2013) pp. 219–221.

designs could be traded on the nuclear black-market. Finally, attacks could be precursors to sabotage, designed to map nuclear systems and their vulnerabilities, implant logic bombs and ensure access to in the future.

Interference, Spoofing and Sabotage

The computerisation of society has transformed the scope for sabotage of key systems, both in terms of critical national infrastructure and directly against nuclear weapons systems. The challenge is divided between narrow and discrete attacks against nuclear forces and systems, and attacks not directed against nuclear weapons but that could affect nuclear. While nuclear systems are certainly likely to be far better protected against sabotage and attack than commercial infrastructure, the threat is real and manifests right across the nuclear weapons enterprise.

The procurement of nuclear software and components and the need to update and replace systems presents a serious challenge. The main threat is that vulnerabilities, problems, logic bombs, software and hardware Trojans, or faults, can be inserted into software, systems or components in the manufacturing, supply and maintenance stages. Sabotage can come in many guises: it could involve the physical alteration of components so that they don't work or at least not work as expected; the introduction of malware or doctored coding to change a process, or implanting malware that allows future access in order to control, disrupt or destroy it.

Cyber-sabotage can be traced back to the 1980s when the CIA began an operation to feed modified technical and computer related equipment to the Soviet Union. Under what became known as the *Farewell Dossier*, defective computer chips and doctored designs and drawings were fed in to the Soviet military-industrial complex.[19] During the 1990s the US and Israel modified vacuum pumps purchased by Iran to make them break down[20]; in 2012, Siemens was accused of planting tiny explosives inside equipment

[19] *Gus Weiss, "Duping the Soviets: the Farewell Dossier", Studies in Intelligence, 39:5 (1996) p. 125.*

[20] *David Sanger, "Confront and conceal: Obama's secret wars and surprising use of American power", (New York, Broadway Paperbacks: 2013) p. 194.*

that Iran had purchased for its nuclear programme[21]; and in 2014, Iran blamed the West for "trying to sabotage the heavy water nuclear reactor at Arak by altering components of its cooling system."[22]

The cyber challenge also involves attempts to attack, compromise or spoof early warning and communications systems, and to undermine the information that decision makers and systems rely upon. Attempts to jam communications or to deceive an adversary by providing misleading information have long been key components of warfare, but the nature of this challenge is also changing in the cyber age. There is no better example of this than the alleged use of the Suter malware by Israel against Syrian air defence radar in 2007 to allow bombing of a suspected nuclear site. Instead of simply jamming radar signals, the Suter programme [purportedly] hacked into the Syrian air defence system allowing the Israeli airplanes to bomb the suspected complex unhindered.[23] While this attack was limited, it nevertheless provides a stark warning of new types of vulnerability, particularly for nuclear communications and early warning systems.

The final set of challenges involves attacks intended to cause physical destruction or that are designed to cause a nuclear explosion. While the 2007 Aurora Generator test demonstrated the possibilities of sabotage through cyber means, there are only a handful of cyber-attacks that have caused physical destruction that are publicly known about, and only one – Stuxnet – that has caused direct damage to a nuclear facility (although there are rumours of US-led attacks on the North Korean nuclear programme[24]). Stuxnet probably entered the air-gapped Natanz system through an infected USB drive or other media via an unwitting employee who had access to infection points, and depended upon prior monitoring and mapping of the system.[25]

Both Stuxnet and *Operation Orchard* show that even systems thought not to be connected to the Internet as well as those vital for nuclear operations could be compromised

[21] *"Iran says nuclear equipment was sabotaged", New York Times, (22 September 2012), http://www.nytimes.com/2012/09/23/world/middleeast/iran-says-siemens-tried-to-sabotage-its-nuclear-program.html?_r=0.*

[22] *David Sanger, "Explosion at key military base in Iran raises questions about sabotage", New York Times, (9 October 2014), http://www.nytimes.com/2014/10/10/world/explosion-at-key-military-base-in-iran-raises-questions-about-sabotage.html.*

[23] *Richard Clarke & Robert Knake, "Cyber war: the next threat to national security and what to do about it", (New York, HarperCollins: 2010) pp. 6–8*

[24] *Salvador Rodriguez, "US tried, failed to sabotage North Korea nuclear weapons program with Stuxnet-style cyber-attack", International Business Times, (29 May 2015), http://www.ibtimes.com/us-tried-failed-sabotage-north-korea-nuclear-weapons-program-stuxnet-style-cyber-1945012.*

[25] *Jon Lindsay, "Stuxnet and the limits of cyber warfare", Security Studies, 22:3 (2013) p. 381.*

in a worst case scenario, and the risk of indirect interference or from third parties, remains a key challenge. Interestingly therefore, it may be that older and less sophisticated systems and infrastructure used in nuclear command and control are safer and more secure against (cyber) sabotage and interference.

Strategic Stability and Crisis Management

In the past decade, hackers and cyber-attack have become an increasingly important component of conflict. While cyber may be viewed by some as a separate domain, in reality cyber cannot be decoupled from these other dynamics, and *will* therefore play a role in future nuclear-related decisions and strategic balances. An increased role for cyber exploitation and attacks – either on their own or in concert with kinetic military force – is likely to have implications for the nature of conflict, strategic stability and particularly future crisis management between nuclear-armed actors.

There are four key areas that cyber-attacks may impact strategic and crisis stability between nuclear-armed actors.[26]

First, during a crisis, hackers could potentially disrupt or destroy communications channels, making it difficult to manage nuclear forces and reducing commanders' confidence in their systems. Attackers might also employ DDoS attacks to prevent communication, hamper battle management systems and make it difficult to identify what is happening.

Second, they can increase perceived time pressures to act/ respond or to act pre-emptively.

Third, they may reduce the search for viable alternatives, thereby compressing and obfuscating the escalation ladder.

Fourth, they may cause flawed images of intentions and capabilities or spoof early warning systems, a particular concern given the possibility of false flag interference by third parties, exacerbate concerns of strategic surprise, and create problems for signalling.

[26] *This list of adopted from that used by Stephen Cimbala in "Nuclear weapons in the information age", (London, Continuum International Publishing: 2012) pp. 56-57.*

Taken together these dynamics raise the likelihood of unintended escalation and make the management of crises more complicated and dangerous.

The most likely future cyber-nuclear dilemma is between the United States and China; both nations have been pretty open about the importance of cyber capabilities and attacks on information systems. The primary concern here is that a low-key conflict could quickly escalate to the strategic level. But there is also a risk – particularly in China – that nuclear C2 and associated systems could be targeted or compromised through cyber means. This could have implications for China's No First Use posture, particularly when combined with US BMD and conventional strike capabilities. The second is between the US, its NATO allies and Russia. NATO has made it clear that cyber-attacks are a major challenge and concern for the Alliance, and "that some cyber-attacks could have the same level of disruption on NATO countries and economies as conventional warfare."[27] Both NATO and Russian deterrence thinking remains anchored by nuclear weapons, and a significant number of these weapons remain on high alert.

While the threat of escalation driven by cyber is an important aspect of the east-west strategic balance, the direct and indirect cyber threat to US and Russia nuclear forces is particularly pressing. These challenges include attacks designed to neuter, interfere with or compromise nuclear C2 systems so that they do not work properly, as well as attacks by third parties seeking to precipitate or worsen a crisis or even cause a nuclear launch. While these challenges will be similar to those facing the US-China relationship, they are exacerbated by the large nuclear stockpiles, and particularly by the ICBMs that both sides keep on alert. These challenges will become magnified during any possible future crisis.

Deterring Cyber-Attacks with Nuclear Weapons?

The threat of a broad cyber-attack creates a range of new pressures for national security policy and the role of nuclear weapons. Formulating a credible way to respond to the cyber challenge has been difficult, and this has been complicated by the considerable differences between nuclear and cyber: the problems and limitations of cyber defence and arms control, the likely need for some type of cross-domain deterrence/ retaliation

[27] *Warwick Ashford, "Nato to adopt new cyber defence policy", ComputerWeekly.com, (3 September 2014), http://www.computerweekly.com/news/2240228071/Nato-to-adopt-new-cyber-defence-policy.*

strategy (that may or may not include nuclear weapons), the inherent difficulties of attribution, and the uncertainty of the nature and extent of any future cyber threat or attack. These dynamics make formulating a national nuclear-cyber strategy difficult and problematic.

The rise of the cyber has led to comparisons with nuclear weapons, but the two are profoundly different. There are at least four main differences between cyber and nuclear: the scale and nature of the threat; the types of targets to be attacked; the actors involved, and the rules and conventions which govern their use. In terms of the scale, even the most sophisticated cyber-attacks are unlikely to cause the destruction that a nuclear bomb can and has done, and it is difficult to think of cyber as being strategic. Part of the reason for this is that the intended targets of cyber and nuclear attack tend to be different. While it is possible to have limited or focused nuclear attack, nuclear weapons are generally seen as indiscriminate and intended to cause widespread destruction. In contrast, the most threatening cyber-attacks are likely to be specialised and target specific systems or machines and often require knowledge of the target beforehand (notwithstanding DDoS attacks).

While the cyber challenge may be different from that posed by nuclear weapons it nonetheless requires concerted thinking about how to defend, deter and potentially respond to cyber-attacks. But cyber security and defence, the broader notion of deterrence by denial, and the concept of cyber arms control are problematic. Any strategy will therefore need to include deterrence by punishment and through the threat of retaliation. However, deterring cyber-attacks through punishment raises the question of whether attacks can be confidently attributed, and what form this response might take if it is to be credible, proportional, and legal. There is also the question of whether cyber should be considered separately or as part of a broader (cross domain) deterrence strategy that involves other forms of military and political power. To make matters more complicated it is likely that deterrence thinking will have to be tailored to specific types of attack given the wide variety of activities that fall under the rubric of cyber-attack.

If deterrence of cyber-attacks must to be tailored to specific types of threat and attack and proportional, this raises the question of what types of response might be required. It also suggests that some types of cyber-attack might require an asymmetric response – including kinetic military force – and that therefore cyber might have to be included in cross-domain deterrence planning. Such thinking necessarily leads to consideration of whether there might be any role for nuclear weapons in anchoring the deterrence ladder and in the event of an existential cyber-attack.

There is certainly some logic to including nuclear forces as part of a cross-domain cyber deterrence strategy. But, the majority of analysis has questioned the wisdom of commingling nuclear and cyber weapons: cyber-attacks lack the destructive and existential threat of nuclear weapons; a nuclear response to a cyber-attack is not proportional and lacks credibility; cyber deterrence is difficult to achieve; linking the two provides a new rationale for nuclear proliferators.[28] Given the current cyber threat, nuclear weapons are not a good option for addressing and deterring cyber, but should the nature of the threat change then it is possible that nuclear weapons could have a role to play in the future.

Conclusion

Cyber will not supersede nuclear weapons as the ultimate symbol or guarantor of national security, or represent a strategic or existential threat, any time soon. But these dynamics do present an important shift in the context within which we think about nuclear weapons and nuclear security, manage nuclear relationships and strategic stability, and regulate global nuclear order. The emergence and spread of cyber capabilities is changing, recasting and exacerbating existing tensions across the nuclear weapons enterprise, and providing new dynamics and challenges that must be understood and addressed.

Cyber threats will also have implications on a larger scale. The possibility and perception that nuclear systems might be compromised, attacked and not work as intended, may lead to nuclear modernisation and proliferation, and impact current arms control agreements and nuclear regimes, and provide another barrier to nuclear cuts. This becomes even more troubling when cyber is combined with other potentially destabilising technologies, which may undermine strategic stability, enhance the possibility of interference by third parties, and increase chances of miscalculation and possibly even nuclear use.

There are no easy fixes, but a good starting point is to properly understand the nature of the challenge and come to some agreement on what the term means. A second recommendation would be for all nuclear-armed states to harden and protect nuclear

[28] *Timothy Farnsworth, "Is there a place for nuclear deterrence is cyberspace?", Arms Control Now, (30 May 2013), http://armscontrolnow.org/2013/05/30/is-there-a-place-for-nuclear-deterrence-in-cyberspace/.*

systems against cyber-attack, and embrace measures that minimise the implications of cyber interference, such as upgraded and redundant systems, better training and screening of operators, and the time it takes for weapons to be fired. This could be done cooperatively and form the basis of moratoria or agreement between states not to target each other's nuclear systems with cyber. While this would not rule out attacks by third parties it could present an opportunity for trust and cooperation building. Finally, cyber should be included alongside other emerging strategic dynamics in nuclear-related discussion, dialogue and arms control agreements.

This paper draws on ideas first published in English as "Cyber threats and nuclear weapons", RUSI Occasional Paper, (July 2016), https://rusi.org/publication/occasional-papers/cyber-threats-and-nuclear-weapons-new-questions-command-and-control. The research is funded by the UK Economic and Social Research Council grant number ES/K008838/1.

#Valdaiclub

ValdaiClubRu
https://twitter.com/ValdaiClubRu

ValdaiClubRu
https://www.facebook.com/ValdaiClubRu/

ru.valdaiclub.com

valdai@valdaiclub.com

Council on Foreign and Defense Policy

RIAC
Russian International Affairs Council

MGIMO UNIVERSITY

HIGHER SCHOOL OF ECONOMICS
NATIONAL RESEARCH UNIVERSITY