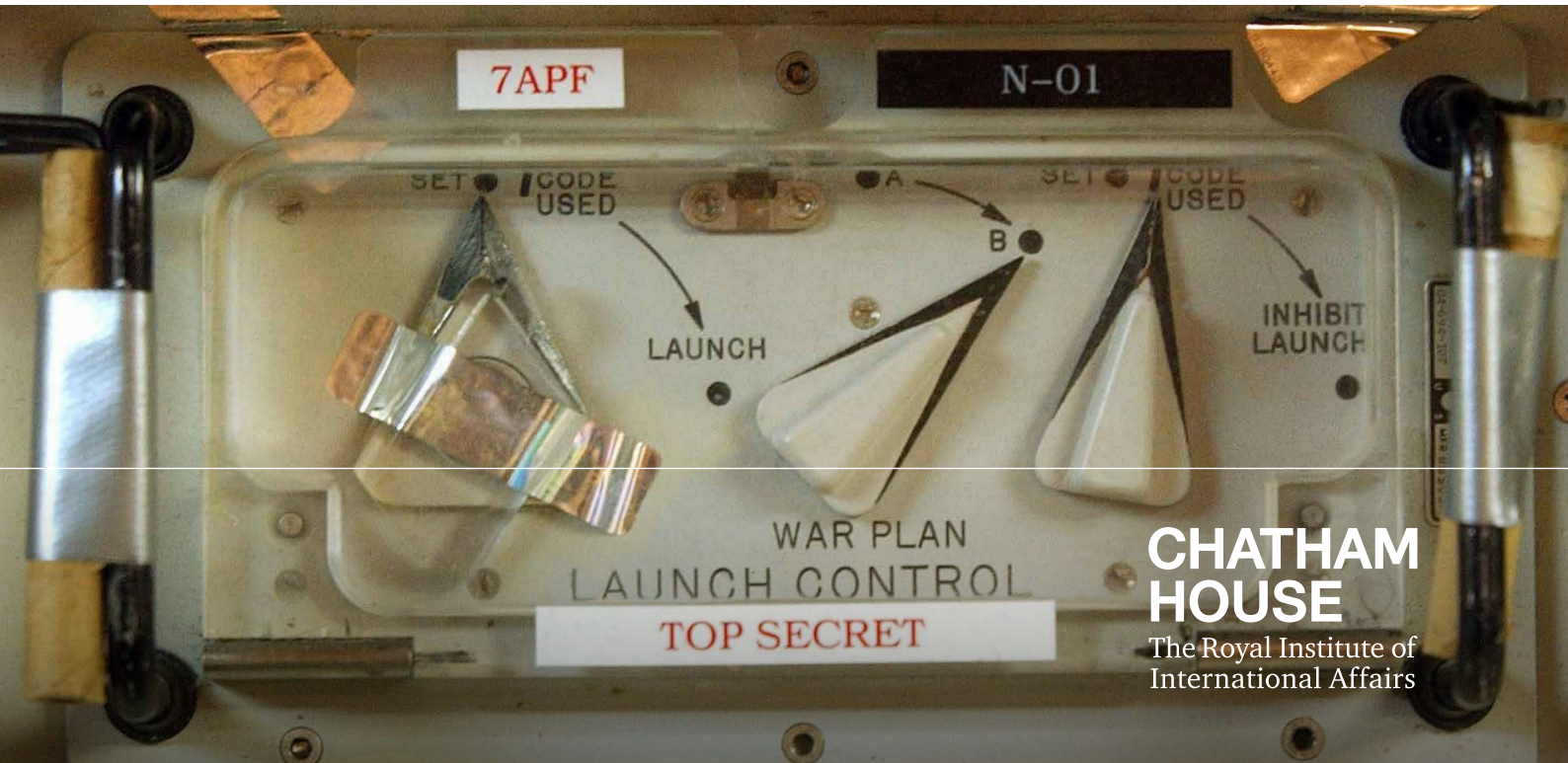
Research Paper

Beyza Unal and Patricia Lewis
International Security Department | January 2018

Cybersecurity of Nuclear Weapons Systems

Threats, Vulnerabilities and Consequences



CHATHAM HOUSE
The Royal Institute of International Affairs

Contents

Summary

- Nuclear weapons systems were first developed at a time when computer capabilities were in their infancy and little consideration was given to potential malicious cyber vulnerabilities. Many of the assumptions on which current nuclear strategies are based pre-date the current widespread use of digital technology in nuclear command, control and communication systems.

- There are a number of vulnerabilities and pathways through which a malicious actor may infiltrate a nuclear weapons system without a state's knowledge. Human error, system failures, design vulnerabilities, and susceptibilities within the supply chain all represent common security issues in nuclear weapons systems. Cyberattack methods such as data manipulation, digital jamming and cyber spoofing could jeopardize the integrity of communication, leading to increased uncertainty in decision-making.

- During peacetime, offensive cyber activities would create a dilemma for a state as it may not know whether its systems have been the subject of a cyberattack. This unknown could have implications for military decision-making, particularly for decisions affecting nuclear weapons deterrence policies.

- At times of heightened tension, cyberattacks on nuclear weapons systems could cause an escalation, which results in their use. Inadvertent nuclear launches could stem from an unwitting reliance on false information and data. Moreover, a system that is compromised cannot be trusted in decision-making.

- Possible cyber resilience measures include taking a holistic approach in creating trustworthy systems based on rigorous risk assessments. These should incorporate an analysis of a combination of threats, vulnerabilities and consequences.

- It is the responsibility of nuclear weapons states to incorporate cyber risk reduction measures in nuclear command, control and communication systems. Although some information is publicly available on US weapons systems, there is very little information regarding other nuclear weapons states. Academia and civil society should be encouraged to bring this issue to the attention of their government.

1. Introduction

The reliance on digital technologies in modern weapons systems – particularly in nuclear weapons systems – has led to growing concerns that cyberattacks may pose additional risks at a time of escalating conflict, which could undermine the confidence needed to make reliable decisions.

Cyber risks in nuclear weapons systems have thus far received scant attention from the nuclear weapons policy community. The potential impacts of a cyberattack on nuclear weapons systems are enormous. Data hacks can reveal sensitive information on facilities' layouts, personnel details, and design and operational information. Cyber interference could destroy industrial control systems within delivery platforms, such as submarines, causing them to malfunction. In addition, clandestine attacks could be conducted on targeting information or operational commands, which may not be discovered until the point of launch.

These risks raise significant doubts as to the reliability and integrity of nuclear weapons systems in a time of crisis, regarding the ability to: a) launch a weapon; b) prevent an inadvertent launch; c) maintain command and control of all military systems; d) transmit information and other communications; and e) the maintenance and reliability of such systems. This paper will focus on cybersecurity and cyber vulnerabilities and argue that the digitization of systems and the use of emerging technologies – while providing several benefits – increase the vulnerabilities to cyberattacks in nuclear weapons systems.

The first nuclear policies were instigated in the US decades ago and each country that has developed nuclear weapons has established individual doctrines and policies regarding their deployment and potential use. The risks associated with nuclear weapons, particularly given their capacity for devastating explosive yields and long-term harmful radioactive impacts, have been issues for discussion ever since.[1]

This paper does not claim that emerging technologies are the primary risk to consider in the nuclear field, or that the risks of nuclear weapons are new. Rather, the paper argues that while key risk areas have existed for a long time, new technology has exacerbated these risks. With each new digital component embedded in the nuclear weapons enterprise, new threat vectors may emerge. Solutions to these risks, therefore, should go beyond applying cybersecurity policies because, in this context, cyber risk reduction is actually about nuclear risk reduction. With the potential for such catastrophic consequences from a nuclear weapons detonation attack it is crucial to have the most robust nuclear policies in place.

The likelihood of attempted cyberattacks on nuclear weapons systems is relatively high and increasing from advanced persistent threats from states and non-state groups. As an example of what is possible, the US is reported to have infiltrated parts of North Korea's missile systems and

[1] Unal, B. and Lewis, P. (2017), 'Cyber Threats and Nuclear Weapons Systems', in Borrie, J., Caughley, T., and Wan, W. (eds) (2017), *Understanding Nuclear Weapons Risks*, United Nations Institute for Disarmament Research (UNIDIR), pp. 61–71, http://www.unidir.org/files/publications/pdfs/understanding-nuclear-weapon-risks-en-676.pdf (accessed 1 Dec. 2017).

caused test failures.[2] Recent cases of cyberattacks indicate that nuclear weapons systems could also be subject to interference, hacking, and sabotage through the use of malware or viruses, which could infect digital components of a system at any time. Minuteman silos, for example, are believed to be particularly vulnerable to cyberattacks.[3] Some of the known methods that would affect the decision-making process for launching a nuclear weapon include data manipulation, cyber jamming communication channels, or cyber spoofing.[4] In particular, successful cyber spoofing could hijack decision-making with potentially devastating consequences.

[2] Gartzke, E. and Lindsay, J. (2017), 'The U.S. wants to stop North Korean missiles before they launch. That may not be a great idea', *Washington Post*, 15 March 2017, https://www.washingtonpost.com/news/monkey-cage/wp/2017/03/15/the-u-s-wants-to-stop-north-korean-missiles-before-they-launch-that-may-not-be-a-great-idea/ (accessed 1 Dec. 2017); Gartzke, E. and Lindsay, J. R. (2017), 'Thermonuclear cyberwar', *Journal of Cybersecurity*, 3(1): pp. 37–48, https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyw017/2996537/Thermonuclear-cyberwar (accessed 1 Dec. 2017).
[3] Blair, B. G. (2017), 'Why our nuclear weapons can be hacked', *New York Times*, 14 March 2017, https://www.nytimes.com/2017/03/14/opinion/why-our-nuclear-weapons-can-be-hacked.html (accessed 1 Dec. 2017).
[4] Data manipulation is the process whereby hackers compromise data integrity by altering the information received by missile systems and missile operators. Cyber jamming is a method that compromises a system by denial-of-service attacks. Cyber spoofing goes one step further and creates false information that seems to come from a legitimate source and is seen as genuine, all without the receiver's knowledge. See, Livingstone, D. and Lewis, P. (2016), *Space, the Final Frontier for Cybersecurity?*, Research Paper, London: Royal Institute of International Affairs, https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf (accessed 24 Nov. 2017).

2. Cyber Risks

Communications as well as the transfer and storage of data are key targets for cyberattackers. In an earlier United Nations Institute for Disarmament Research (UNIDIR) paper, the International Security Department at Chatham House identified several areas within nuclear weapons systems[5] that could be potentially vulnerable to cyberattacks:[6]

- Communications between command and control centres;
- Communications from command stations to missile platforms and missiles;
- Telemetry data from missiles to ground- and space-based command and control assets;
- Analytical centres for gathering and interpreting long-term and real-time intelligence;
- Cyber technologies in transport;
- Cyber technologies in laboratories and assembly facilities;
- Pre-launch targeting information for upload;
- Real-time targeting information from space-based systems including positional, navigational and timing data from global navigational systems;
- Real-time weather information from space-, air-, and ground-based sensors;
- Positioning data for launch platforms (e.g. submarines);
- Real-time targeting information from ground stations;
- Communications between allied command centres; and
- Robotic autonomous systems within the strategic infrastructure.

These areas are subject to exploitation by groups or individuals with malicious intent. In risk analysis, as the attack surface (the number of vulnerabilities in a system or network) increases while cybersecurity measures lapse, malicious cyberattacks are likely to become more frequent. For each area within nuclear weapons systems, there are different pathways, also known as attack vectors, through which a malicious actor could gain access to sensitive information and even create false information. These attack vectors range from using remote malware to activating previously installed exploits or human elements to access systems.

[5] Unal and Lewis (2017), 'Cyber Threats and Nuclear Weapons Systems'.
[6] A cyberattack is a deliberate exploitation of computers, networks and digital systems. It can result in disruptive consequences, such as compromised data, data theft, and sector-specific consequences such as economic loss, reputational costs, and even loss of life.

Cyber risk analysis should also include the assessment of actor-specific threats. The biggest of these comes from other states attempting to neutralize their opponents' nuclear weapons systems through cyberattacks. Other actors include hackers, organized crime groups, lone-actors, and terrorist organizations. Although states currently possess the necessary capabilities and knowhow to conduct attacks on advanced strategic assets and industrial control systems, the higher degree of cooperation between hackers and organized crime groups has been identified as a growing concern.[7]

Similar cooperation between organized crime groups and terrorist organizations has already been seen in other areas, such as the illicit trafficking of radioactive and nuclear materials and terrorism-related activities, in Moldova[8] and in Georgia.[9] There is an emerging trend that these groups may share an interest in exploiting vulnerabilities in critical national infrastructure and strategic military assets.[10] For terrorist organizations, the primary interest lies in causing terror and to undermine state security whereas for organized crime groups it is solely about financial gain.[11] Recently, in Belgium, groups affiliated with ISIS monitored the movements and activities of a nuclear scientist – for what purpose, it is still unclear – which raised concerns about the vulnerability of civil nuclear facilities and their personnel.[12] Additionally, German-owned Patriot missiles in Turkey were reported to have been hacked in 2015.[13] Reports indicate two types of vulnerability in Patriot missiles: the real-time information exchange system – connecting the missile launcher and the missile's control system (known as the sensor shooter interoperability) – and in the computer chip that provides targeting guidance to the missiles.[14] Such hacking could result in damage to data and the loss of command execution authority of key systems.[15] Nuclear weapons systems rely heavily on real-time information exchange for targeting in ground- and space-based systems. Since weapons systems rely on real-time data and information, any malfunction needs to be addressed promptly.

As technology changes rapidly, jamming, spoofing and cyberattacks are almost impossible to prevent or defend against completely. However, no system has ever been entirely impenetrable. Electronic warfare systems, including sensors receiving information that contributes to electronic

[7] For instance, in Sicily, in October 2000, a group of people with links to mafia families worked with an insider and created a digital clone of a bank's online system. The plan was to divert around $400 million that was for the regional projects in Sicily. In another incident, a group of drug smugglers, importing heroin from South America, worked with hackers to infiltrate the containers system in the port of Antwerp. For more information, see Glenny, M. (2017), 'Organized crime finally embraces cyber theft', *Financial Times*, 7 March 2017, https://www.ft.com/content/a038cd98-0041-11e7-8d8e-a5e3738f9ae4 (accessed 1 Dec. 2017); see also Williams, P. (2001), 'Organized Crime and Cybercrime: Synergies, Trends, and Responses', http://www.crime-research.org/library/Cybercrime.htm (accessed 1 Dec. 2017).
[8] Unal, B. (2015), 'Growing Threat as Organized Crime Funnels Radioactive Materials to Terrorists', Chatham House Expert Comment, 13 October 2015, https://www.chathamhouse.org/expert/comment/growing-threat-organized-crime-funnels-radioactive-materials-terrorists (accessed 1 Dec. 2017).
[9] As discussed in Sokova, E. presentation 'Illicit Trafficking in Nuclear and Radioactive Materials in the Caucasus: the Case of Georgia', at the INMM Workshop 'Reducing the Risk from Radioactive and Nuclear Materials', 10–11 March 2009.
[10] Information sharing has become a norm between cyber groups. Recent WannaCry ransomware cryptoworm, for instance, is a good indication of how US National Security Agency (NSA) government exploits could be weaponized. The group that leaked the exploit, Shadow Brokers, was also different from those behind the WannaCry attack – ultimately attributed to the North Korea hacking group, Lazarus.
[11] Reitano, T. and Adal, L. (2017), *Examining the Nexus between Organised Crime and Terrorism and its Implications for EU Programming*, Brussels: European Union Counter-Terrorism Monitoring, Reporting and Support Mechanism, https://icct.nl/wp-content/uploads/2017/04/OC-Terror-Nexus-Final.pdf (accessed 29 Nov. 2017).
[12] Rubin, J. A. and Schreuer, M. (2016), 'Belgium Fears Nuclear Power Plants are Vulnerable', *New York Times*, 25 March 2016, https://www.nytimes.com/2016/03/26/world/europe/belgium-fears-nuclear-plants-are-vulnerable.html (accessed 27 Nov. 2017).
[13] Kumar, M. (2015), 'German Missile System Hacked; "Unexplained" Commands Executed Remotely', The Hacker News, 11 July 2015, https://thehackernews.com/2015/07/Patriot-anti-aircraft-missile-hacked.html (accessed 1 Dec. 2017).
[14] Storm, D. (2015), 'Did hackers remotely execute "unexplained" commands on German Patriot missile battery?', *Computer World*, 8 July 2015, https://www.computerworld.com/article/2945383/cyberwarfare/did-hackers-remotely-execute-unexplained-commands-on-german-patriot-missile-battery.html (accessed 1 Dec. 2017).
[15] Ibid.

signals intelligence and those that detect, identify and locate radio frequencies operating in a theatre, have periodically had to be upgraded to counter radar spoofing and deception techniques.[16] These technologies are not new and have been used since the Cold War. However, now the spoofing of digital information has to be added into the mix of signals intelligence spoofing and thus further complicates uncertainties.

Potential artificial intelligence (AI) applications, while creating new opportunities for enhancing cybersecurity, may also add new layers of complexity and risk to cybersecurity nuclear weapons systems. Russian President Vladimir Putin for instance recently made a speech for the start of a new school year at a Russian school in which he stated that whoever leads AI development will rule the world.[17] This message also correlates with Russia's efforts in working on a new spoofing device that can imitate jets, rockets or a missile attack and thus fool defence systems.[18] Hijacking the command, control or communication of these electronic warfare capabilities is possible through cyber means.

Automation and autonomy come with inherent risks, however. Future automation risks may include delegating the decision-making process to autonomous systems that rely on AI. These developments will enable machines to make decisions based on learning from experience rather than on pre-programmed responses. Over-reliance on an autonomous system may result in automation bias, where the data is believed without being questioned by both human operators and decision-making machines.[19] Rigorous monitoring of automated information could reduce automation bias but it requires critical and sceptical minds and algorithms that can critically analyse the received information.

Patching legacy systems with digital components or pre-delegating decision-making to autonomous systems would be likely to change safety conditions, resilience and integrity of the whole weapons system in the future as well. Human responsibility should not be taken away from the machine–human interface; as historical cases of nuclear near misses show, human judgment is vital to reduce misunderstandings in decision-making.[20] Despite such concerns, Russia has developed an autonomous submarine[21] with the ability to launch nuclear capable ballistic missiles.[22] Nuclear modernization policies that rely on new military capabilities and/or increased automation will have knock-on effects on strategic stability, creating conditions for escalation and an arms race.

[16] Keller, J. (2017), 'Navy continues buying radar-spoofing electronic warfare (EW) equipment from Mercury Systems', *Military & Aerospace*, 27 June 2017, http://www.militaryaerospace.com/articles/2017/06/radar-spoofing-electronic-warfare-ew.html (accessed 1 Dec. 2017).
[17] Meyer, D. (2017), 'Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World', *Fortune*, 4 September 2017, http://fortune.com/2017/09/04/ai-artificial-intelligence-putin-rule-world/ (accessed 1 Dec. 2017).
[18] Sukhankin, S. (2017), 'Russian Capabilities in Electronic Warfare: Plans, Achievements and Expectations', Real Clear Defence, 20 July 2017, https://www.realcleardefense.com/articles/2017/07/20/russian_capabilities_in_electronic_warfare_111852.html (accessed 1 Dec. 2017).
[19] Nelson, K. (2016), 'Automation Bias-Cognitive Biases (Pt. 6)', *Evolve Consciousness* blog, 19 November 2016, http://evolveconsciousness.org/automation-bias-cognitive-biases-pt-6/ (accessed 1 Dec. 2017); Parasuraman, R. and Manzey, D.H. (2010), 'Complacency and Bias in Human Use of Automation: An Attentional Integration', *Human Factors*, 52(3): pp. 381-410, doi: 10.1177/0018720810376055 (accessed 1 Dec. 2017).
[20] Lewis, P., Williams, H., Pelopidas, B. and Aghlani, S. (2014), *Too Close for Comfort: Cases of Near Nuclear Use and Options for Policy*, Chatham House Report, London: Royal Institute of International Affairs, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20140428TooCloseforComfortNuclearUseLewisWilliamsPelopidasAghlani.pdf (accessed 1 Dec. 2017).
[21] This unmanned submarine is code named in the Pentagon as 'Kanyon'. The nuclear warheads carried by this submarine are capable of destroying ports and cities.
[22] Griffin, M. (2016), 'Russia tests its new autonomous nuclear submarine off the US coast', Fanatical Futurist, 11 December 2016, http://www.fanaticalfuturist.com/2016/12/pentagon-detects-tests-of-russias-new-nuclear-capable-drone-submarine/ (accessed 1 Dec. 2017); Sputnik News (2015), 'Drone Control System for Naval Destroyers Created in Russia – Developer', 6 April 2015, https://sputniknews.com/russia/201504061020517190/ (accessed 1 Dec. 2017).

The organizational cultures in military services also pose inherent risks to mitigating cyberthreats in nuclear weapons systems. Military procurement programmes tend not to pay adequate consideration to emerging cyber risks – particularly in the supply chain – regardless of the government regulations for protecting data against cyberattacks. This could be due to constantly lagging behind the fast-moving nature of cyberthreats, a lack of skilled personnel, and the slow institutional and organizational implementation of changes. With the digitization of military assets, contracts for production specify the type of digital components, materials and software to be used in the procured item. These specified items may become obsolete or may even be compromised once the contract is in effect at any stage (such as production of warheads, systems design, system architecture, or maintenance). Without proper updates and patching, they are subject to intrusion. The UK's newest aircraft carrier, HMS Queen Elizabeth, for instance, was reported to be using a customized version of Windows XP in the control room.[23] Critics pointed out the vulnerabilities of such outdated software – these comments gained more credibility following the WannaCry ransomware attacks[24] – and questioned the reasoning behind allowing the HMS Queen Elizabeth, its sister ship the HMS Prince of Wales, along with the Royal Navy Trident submarines to operate at sea with the Windows XP system. The UK Ministry of Defence later indicated that the systems were up-to-date and at least the new-class aircrafts will not use the Windows XP system when in operation, which will not be until 2026.[25]

Furthermore, areas of cybersecurity risks are mainly protected by and still rely on human judgment and are therefore vulnerable to human fallibility.[26] Cyber intrusion may occur during the maintenance of strategic assets including nuclear weapons platforms such as submarines (for example, through digital equipment used to fix or test a system, such as backup power generators). Well-trained military personnel are able to identify potential cyber risks, but equally, staff without adequate cybersecurity knowledge and training may become targets of attacks. As a result, insufficient cybersecurity training actually raises the risk of cyberattacks by creating targets that are easy to exploit.

Hacking nuclear systems – such as command and control, critical assets, nuclear weapons facilities – was once believed to be an impossible task. Yet, history has shown that human error, system failures and design vulnerabilities are common occurrences in nuclear weapons systems.[27] Submarines, for instance, are claimed to be air-gapped – and therefore believed to be secure – when submerged. However, submarines are not always below the surface and breaches could happen during maintenance while docked.[28] This is particularly troublesome as complex and tightly coupled systems, such as nuclear weapons systems, may lead to attacks with severe consequences.[29]

[23] MacAskill, E. (2017), 'HMS Queen Elizabeth could be vulnerable to cyber-attack', *Guardian*, 27 June 2017, https://www.theguardian.com/technology/2017/jun/27/hms-queen-elizabeth-royal-navy-vulnerable-cyber-attack (accessed 1 Dec. 2017).
[24] It was recently reported that the WannaCry ransomware affected more systems running with Windows 7 (97 per cent) than Windows XP operating systems. This, however, does not suggest that the older versions of XP systems are safer. See Burgess, M. (2017), 'Wannacry ransomware hit Windows 7 worse than Windows XP, analysis suggests', *Wired*, 22 May 2017, http://www.wired.co.uk/article/wannacry-windows-7-xp (accessed 1 Dec. 2017).
[25] Burgess, M. (2017), 'Claims the Queen Elizabeth aircraft carrier is using Windows XP may not be what they seem', *Wired*, 27 June 2017, https://www.wired.co.uk/article/hms-queen-elizabeth-windows-xp (accessed 1 Dec. 2017).
[26] Another fast-growing area is bio-hacking. A kick-starter campaign, for instance, suggested using cockroaches, controlling their movement and navigation through a smart phone. The experiment showed that cockroaches got used to the signals and eventually adapt to them. As a result, it was not particularly effective. Yet, this type of experiment opens new pathways for remote control.
[27] Lewis et al. (2014), *Too Close for Comfort: Cases of Near Nuclear Use and Options for Policy*.
[28] Abaimov, S. and Ingram, P. (2017), *Hacking UK Trident: A Growing Threat*, London: BASIC, http://www.basicint.org/sites/default/files/HACKING_UK_TRIDENT.pdf (accessed 1 Dec. 2017).
[29] Perrow, C. (1999), *Normal Accidents: Living with High-Risk Technologies*, Princeton, NJ: Princeton University Press, p. 354.

Moreover, nuclear systems that function as they are intended to under normal circumstances may respond differently when under stress.[30] States rely on the integrity of operational information provided through information technology (IT); if the information is unreliable, the decision-maker's ability to respond accurately and effectively will also be compromised.

[30] Ibid.; Borning, A. (1987), 'Computer System Reliability and Nuclear War', *Communications of the ACM* 30(2): pp. 112–131, doi: 10.1145/12527.12528 (accessed 1 Dec. 2017).

3. Cyber Vulnerabilities

Nuclear command and control vulnerabilities[31]

Command and control vulnerabilities regarding nuclear weapons systems have been of concern for several decades now. In the 1960s, the initial main concern was the vulnerability of electronic systems to disruption caused by the electromagnetic effects of a nuclear weapons detonation. At that time, the US and Soviet Union engaged in electronic warfare by spoofing radar images being deciphered in command and control centres. The US, for instance, spoofed the Soviet air-defence radars in Cuba in the early 1960s in order to test the maturity of the Soviet radar and operators there,[32] at the same time the Soviet Union were testing the stealth of the US OXCART aircraft.[33] Interfering with strategic communications through electronic measures, in order to control information was also common, for example through the disruption of optical fibre systems.[34]

The role of nuclear weapons from a command, control and communications (C3) perspective is to serve as a key military asset for decision-makers, such as presidents and prime ministers, and such weapons can only be used with authorization from a decision-maker. The authorization can only be given once a reliability assessment of data has taken place. The confirmation of data readings signalling an event that may require a nuclear response must come from at least two independent sources (for example, radar and satellite systems).[35] This is known as dual phenomenology.

Each country has distinct nuclear C3 systems. In the US, for instance, the National Command Authority (NCA) is comprised of the president and the secretary of defense, with the president as the ultimate authority in the chain of command. If information received through the dual phenomenology approach demonstrates that the US is under attack, then a missile threat conference would first be conducted with senior leaders, the secretary of defense and the US Strategic Command. However, in such an instance the response time would be limited. To make matters worse, the dual phenomenology method is not infallible. If the communication methods have been compromised by interference from cyberattackers it may lead the decision-makers to issue an order without sufficient information.

Identifying, locating and reporting threats are also important in the C3 system.[36] In the US, the Integrated Threat Warning/Attack Assessment (ITW/AA) structure – which provides strategic surveillance and information about attack warnings – has a variety of sensors to detect nuclear

[31] This section relies on information primarily from the US due to the availability of information. A future study on nuclear command, control and communication for all nuclear weapons states would complement this study.
[32] Poteat, G. (2008), *Stealth, Countermeasures, and ELINT, 1960-1975 (unclassified)*, Washington: Central Intelligence Agency (CIA) Library, https://www.cia.gov/library/readingroom/docs/stealth_%20count.pdf (accessed 1 Dec. 2017).
[33] OXCART is the reconnaissance aircraft that succeeded the U-2 plane, operational on 12 November 1965. See, CIA (2015), 'OXCART vs Blackbird: Do You Know the Difference?', https://www.cia.gov/news-information/featured-story-archive/2015-featured-story-archive/oxcart-vs-blackbird.html (accessed 1 Dec. 2017).
[34] Long, A. (2016), 'A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning', *Journal of Cybersecurity*, 3(1): pp. 19–28, doi: 10.1093/cybsec/tyw016 (accessed 1 Dec. 2017).
[35] Halloran, R. (1983), 'Nuclear Missiles: Warning System and the Question of When to Fire', *New York Times*, 29 May 1983, http://www.nytimes.com/1983/05/29/us/nuclear-missiles-warning-system-and-the-question-of-when-to-fire.html (accessed 1 Dec. 2017).
[36] Hilland, D. H., Phipps, G. S., Jingle, C. M. and Newton, G. (1998), 'Satellite Threat Warning and Attack Reporting', *IEEE Aerospace Conference* 2: pp. 207–217, doi: 10.1109/AERO.1998.687911 (accessed 1 Dec. 2017).

missile launches.[37] The ITW/AA relies on key nodes, such as ground- and space-based assets, intelligence centres, weather support centres, space control centres and the missile warning centre.[38] The integrity of the ITW/AA is critical for receiving reliable communications, upon which decisions can be made. The ground-based systems, such as large-fixed radars, rely on electronic beams, which leaves them open to manipulation through cyber means. However, a space-based asset is more exposed to the risk of manipulation of its communication data.[39] If some of the ITW/AA key nodes are compromised, at the very least it would cause a loss of confidence in dual phenomenology.

There are different types of communication systems available for use in the nuclear command and control structure. The communication systems are used for delivering and validating information, video and audio messages as part of a Permissive Action Link, which is a mechanism for authorizing and authenticating codes. In addition, a Permissive Action Link is a code management system that allows for secure coding, locking, recoding, unlocking and managing weapons; the system maintains complete secrecy, authenticity and validity of the launch orders throughout a test or real procedure to launch.[40] The nuclear triad – land-based intercontinental ballistic missiles (ICBM), submarine-launched ballistic missiles (SLBM), and bomber aircraft – relies on different methods of communication characteristics. During peacetime fixed land-line systems as well as satellite systems, which are relatively robust could be used for transmitting information and communication; satellites may be more vulnerable in times of conflict.[41]

The extremely low frequency communication programme (ELF) is an additional example of a communication system that is used by the US to communicate with submerged submarines. It is a form of one-way communication that sends messages with a very long wavelength.[42] In emergency situations, where submarines are required to engage in two-way communication, the submarines need to either resurface or to deploy an antenna in shallow water.[43] Emergency action message (EAM) transmissions for commanding nuclear release options in the US, for instance, are supported by hybrid communication systems, which combine these different methods of communication and include survivable and non-survivable communication assets, i.e. those that may or may not continue to operate even if parts of the system are damaged or destroyed.[44] These systems are ground- or space-based systems and they include fixed and mobile emergency action plan dissemination routes.[45]

[37] Federation of American Scientists (1999), 'Cheyenne Mountain Complex', https://fas.org/nuke/guide/usa/c3i/cmc.htm (accessed 1 Dec. 2017).
[38] Ibid.
[39] For more information on satellites and cybersecurity, see Livingstone and Lewis (2016), *Space, the Final Frontier for Cybersecurity?*.
[40] Kristensen H. M. (2005), *U.S. Nuclear Weapons in Europe*, Natural Resources Defense Council, https://www.nrdc.org/sites/default/files/euro.pdf (accessed 10 Dec. 2017).
[41] Wilgenbusch, R. C. and Heisig, A. (2013), 'Command and Control Vulnerabilities to Communications Jamming', *Joint Force Quarterly*, 69: pp. 56–63, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-69/JFQ-69_56-63_Wilgenbusch-Heisig.pdf (accessed 1 Dec. 2017).
[42] Federation of American Scientists (2004), 'Extremely Low Frequency Communications Program', https://fas.org/nuke/guide/usa/c3i/elf.htm (accessed 1 Dec. 2017).
[43] Two-way communication is not desirable as it could reveal the location of submarines. See Koski, O. (2010), 'Run Wired, Run Deep: Subs May Finally Get Online', *Wired*, 7 August 2010, https://www.wired.com/2010/07/run-wired-run-deep-subs-may-finally-get-online/ (accessed 1 Dec. 2017).
[44] Chairman of the Joint Chiefs of Staff Instruction (2010), *The Defence Message System and Associated Legacy Message Processing Systems*, Washington: Department of Defense, http://www.jcs.mil/Portals/36/Documents/Library/Instructions/5721_01.pdf?ver=2016-02-05-175048-593 (accessed 1 Dec. 2017).
[45] Ibid.

There are some safeguards in place, for instance, the US navy has implemented a process whereby if an order comes at an unexpected time submarines must resurface and validate the launch order. While the fixed communications systems are vulnerable to attack, the US has only a few mobile systems that it can fall back on.

Similarly, during the Cold War, the Soviet nuclear command and control system was backed up by a command system called Perimeter. Perimeter was believed to be designed to respond to a strike automatically.[46] Today, a question remains: how much automation does Russia have in its command and control system?[47] However, according to a retired colonel in the Russian Strategic Rocket Forces, even during the Cold War, the system was not fully automated and the launch order could only be carried out by the crew.[48]

Supply chain vulnerabilities

Nuclear command, control and communication vulnerabilities are crucial, but they do not represent the whole scope of vulnerabilities in the overall nuclear enterprise. Other phases susceptible to attack or infiltration include the supply chain, the production of warheads and additive manufacturing, among others.

Many aspects of nuclear weapons development and systems management are privatized in the US and in the UK, potentially introducing a number of private-sector supply chain vulnerabilities. Presently, this is a relatively ungoverned space[49] and these vulnerabilities could serve to undermine the overall integrity of national nuclear weapons systems. For example, the backdoors in software that companies often maintain to fix bugs and patch systems are targets for cyberattacks once they are discovered and become known.

These private companies themselves are often under a constant state of cyberattack. In 2010, for example, General Dynamics and Northrop Grumman were breached a number of times.[50] In 2011, Lockheed Martin was the subject of a significant cyberattack.[51] Furthermore, in 2016, the US sentenced a Chinese businessman to prison for helping hackers steal sensitive military information from Boeing.[52]

Despite this constant threat, details of attacks – successful or otherwise – are scarce in the public domain, fitting with a wider culture of secrecy pervading the private sector in cybersecurity. There are a number of reasons why this attitude is prevalent including the risk of plummeting stock

[46] Gazeta, R. and Valagin, A. (2014), 'Ultimate Deterrent: How the Russian "Perimeter" system works', Russia Beyond, 3 April 2014, https://www.rbth.com/defence/2014/04/03/ultimate_deterrent_how_the_russian_perimeter_system_works_35633.html (accessed 1 Dec. 2017).
[47] Hoffman, D. (2011), *The Dead Hand: Reagan, Gorbachev, and the Untold Story of the Cold War Arms Race*, London: Icon Books Ltd.
[48] Yarynich, V. (1994), 'Doomsday Machine's Safety Catch', *The Baltimore Sun*, 2 February 1994, http://articles.baltimoresun.com/1994-02-02/news/1994033200_1_doomsday-launch-nuclear-nuclear-missiles (accessed 1 Dec. 2017).
[49] Each nuclear weapon possessor country has different plans for supply chain integrity. In some countries, such as the US, supply chain strategies are considered in risk management. Though it is unclear how well it is implemented or what measures other countries take.
[50] Greenberg, A. (2010), 'For Pentagon Contractors, Cyberspying Escalates', *Forbes*, 17 February 2010, https://www.forbes.com/2010/02/17/pentagon-northrop-raytheon-technology-security-cyberspying.html (accessed 1 Dec. 2017).
[51] BBC News (2011), 'US defence firm Lockheed Martin hit by cyber-attack', 30 May 2011, http://www.bbc.co.uk/news/world-us-canada-13587785 (accessed 1 Dec. 2017).
[52] BBC News (2016), 'US sentences Chinese hacker for stealing military information', 14 July 2016, http://www.bbc.co.uk/news/world-us-canada-36791114 (accessed 1 Dec. 2017).

values, potential legal liabilities, and severe reputational damage.[53] This secrecy complicates assessing cyber risks and the resulting damage. There is a notable disconnect between the kinds of threat government officials believe companies face and what is reported. Contracted defence companies should have a responsibility to disclose and share information about cyberattacks with nation states.

Supply chain vulnerabilities are a concern for manufacturers and vendors as well as states. The hardware, software, other digital and electronic components of nuclear weapons systems may be compromised before being introduced to the established systems. Presently, the supply chain is not secure by design and although there is some level of cooperation between countries and technology firms, very often these actors do not share a common view of threats. Closer engagement with the private sector and academia on developments in science and technology is an important part of defending strategic assets from disruptive innovation.

In order to reduce the vulnerability in the supply chain, a 'secure by design' holistic approach is needed, which takes into account the possible risks in system architecture, design, manufacturing and maintenance. While the protection of national nuclear forces is a responsibility of equal interest to all stakeholders, this is undermined by the persistence of unidentified or inadequately addressed vulnerabilities in the nuclear supply chain.

The administration of President George W. Bush realized that the US could infiltrate North Korea's nuclear program, and the president subsequently initiated an investigation into the supply chain of North Korean missiles.[54] The Obama administration considered its options in case deterrence failed; this was most clearly demonstrated in the Joint Integrated Air and Missile Defence Vision 2020 document, which indicated that the best option would be to rely on neutralizing an opponent's assets, such as its missile capabilities, prior to use.[55]

By analysing missile debris from North Korea's three-stage missile, the Unha-3, it was discovered that most of the components retrieved from the 2012 test were not restricted under UN sanctions but, in fact, came from the UK, the US and South Korea.[56] The UN Security Council Expert Panel also found other outsourced components (such as a camera electromagnetic interference filter and pressure transmitters) were used in the Unha-3 test and in a separate test in February 2016.[57] With such a number of outsourced items it seems clear that the North Korean missile programme is vulnerable to cyber infiltration, at least through the supply chain.

The vulnerability of North Korea's nuclear weapons programme to cyber infiltration in turn raises questions regarding the cybersecurity of other nations that possess nuclear weapons. In the US, the possible vulnerability of its nuclear weapons programme led to the modernization of Minuteman III

[53] Javers, E. (2013), 'Cyberattacks: Why Companies Keep Quiet', CNBC, http://www.cnbc.com/id/100491610 (accessed 1 Dec. 2017).
[54] Sanger, D. E. and Broad, W. J. (2017), 'Trump Inherits a Secret Cyberwar Against North Korean Missiles', *New York Times*, 4 March 2017, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html (accessed 1 Dec. 2017).
[55] The US Joint Chiefs of Staff (2013), *Joint Integrated Air and Missile Defence: Vision 2020*, Washington, DC: Department of Defense, http://www.jcs.mil/Portals/36/Documents/Publications/JointIAMDVision2020.pdf (accessed 1 Dec. 2017).
[56] Bryne, L. (2014), 'British components in North Korean rockets, UN finds', *Telegraph*, 27 March 2014, http://www.telegraph.co.uk/news/worldnews/asia/northkorea/10726798/British-components-in-North-Korean-rockets-UN-finds.html (accessed 1 Dec. 2017).
[57] United Nations Security Council (2017), *Report of the Panel of Experts established pursuant to resolution 1874 (2009)*, New York: United Nations Security Council, http://www.un.org/ga/search/view_doc.asp?symbol=S/2017/150 (accessed 1 Dec. 2017).

missiles' guidance systems and patching of their rocket motors.[58] Later, a report issued by the Obama administration revealed that the Minuteman silos used to store the US nuclear arsenal had potential vulnerabilities linked to their connection to the internet, which could cause the missile's flight guidance systems to malfunction.[59] The work to address this risk has been contracted out to Boeing, which is providing the design, modernization and testing of these missiles; it specifically incorporated a missile guidance computer to provide precision.[60]

Nuclear weapons design vulnerabilities and potential exploits

Cyberattacks on private sector IT systems may result in the theft of nuclear weapons design information in order to sell or pass on to interested parties, including non-state actors. Protecting nuclear weapons design information requires training personnel in nuclear weapons facilities, including laboratories, cybersecurity measures,[61] increasing awareness and best practice.

When nuclear weapons systems were first designed, there was no consideration of potential cyber vulnerabilities as computer capabilities were very limited. Cybersecurity measures, therefore, were not included in the development of the design structures. To mitigate risks, the US Department of Defense is currently applying a framework called Program Protection Plan, which is able to identify and manage risks to mission-critical systems.[62]

In order to infiltrate a nuclear weapons system, hackers may compromise source code, firmware or internal portals. The military term for this is 'compromised by design' where subcomponents (such as computer chips) are interfered with at the production and design stage.[63] Computer chips may be compromised to allow the exfiltration of data while the chip appears to function normally; the corruption of data within the chip; and to prevent the chip from functioning or affecting its performance.[64] Most countries acquire computer chips from the global marketplace rather than from national defence units and laboratories. Some countries are better at managing this risk than others. For instance, until recently Russia is understood to have used only domestic computer hardware components.[65] However, it has now begun to import hardware components and it remains to be seen whether the Russian cybersecurity strategy will be affected.[66]

[58] Woolf, A. F. (2017), *U.S. Strategic Nuclear Forces: Background, Developments and Issues*, Washington: Congressional Research Service, https://fas.org/sgp/crs/nuke/RL33640.pdf (accessed 1 Dec. 2017).
[59] Blair (2017), 'Why our nuclear weapons can be hacked'.
[60] Keller, J. (2016), 'Boeing to continue upgrading and maintaining missile guidance on fleet of Minuteman III ICBMs', *Military & Aerospace*, 1 February 2016, http://www.militaryaerospace.com/articles/2016/02/minuteman-missile-guidance.html (accessed 1 Dec. 2017).
[61] President's Foreign Intelligence Advisory Board (PFIAB) (1999), *Science at its Best, Security at its Worst: A Report on Security Problems at the U.S. Department of Energy*, Washington: PFIAB, https://www.energy.gov/sites/prod/files/cioprod/documents/pfiab-doe.pdf (accessed 1 Dec. 2017).
[62] Department of Defense (2011), *Program Protection Plan: Outline & Guidance, Systems Engineering Version 1.0*, Washington: Department of Defense, http://www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.pdf (accessed 1 Dec. 2017).
[63] Villasenor, J. (2016), *Compromised by Design? Securing the Defense Electronics Supply Chain*, Washington: Brookings, https://www.brookings.edu/wp-content/uploads/2016/06/Villasenor_HW_Security_Nov7.pdf (accessed 1 Dec. 2017).
[64] Ibid., p. 2.
[65] Rogoway, T. (2015), 'Look Inside Putin's New Military Command and Control Center', Foxtrot Alpha, 19 November 2015, https://foxtrotalpha.jalopnik.com/look-inside-putins-massive-new-military-command-and-con-1743399678 (accessed 1 Dec. 2017).
[66] Encyclopedia of Safety (2013), 'Angstrom has acquired IBM's technology for the production of 90-nanometer chips', 18 October 2013, http://survincity.com/2013/10/angstrom-has-acquired-ibm-s-technology-for-the/ (accessed 2 Dec. 2017)

4. Cyber Offence

While defence against cyber infiltrations is important, governments continue to develop offensive cyber techniques. Through cyber offensive campaigns, states are able to examine new weaknesses and backdoors that also help them reinforce their own cyber resilience. An ongoing dilemma for governments and militaries is to decide how much to invest in cyber defence and resilience and how much to spend on offensive cyber capabilities. From a cost perspective, on the whole, cyber offence capabilities are cheaper to develop and carry out than those of cyber defence[67] and cyber resilience, but cyber offence does not replace cyber defence, and cyber resilience is needed for when cyber defences do not intercept and deal with an attack.

It might seem likely that no country would be willing to face the consequences of starting a cyber offensive campaign in the nuclear weapons domain. However, an escalation is possible if cyber operations continue against key strategic assets of a country. To avoid this outcome, in peacetime strategic assets may be infiltrated silently by offensive stealth campaigns, meaning that the planted malware only becomes active later post-infection under certain conditions (such as when a launch order is received). As a result, states may not be cognizant of their own vulnerability and may not realize their nuclear weapons systems have already been compromised. A successful cyber offensive operation may not be discovered for days or years or perhaps ever.[68] The dilemma of not knowing whether a state's systems have been the subject of a cyberattack would likely have significant implications for its military decision-making and particularly affects its nuclear weapons doctrine and deterrence policy.

The US Presidential Policy Directive (PPD 20), revealed by WikiLeaks, directly instructed US departments and agencies to be ready for both defensive and offensive cyber operations, suggesting US willingness to utilize cyber offensive actions 'to advance U.S. national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging.'[69] The directive also included a call to look at the whole system, including processes and infrastructure, and for the US to maintain cyber offensive capabilities.[70] The US is not alone in doing this. It is generally assumed that most major states are preparing for or carrying out offensive cyber operations, and it must be assumed that some of these are directed at nuclear weapons systems. Russia, Iran and North Korea are also known to carry out offensive cyber operations[71] and the UK recently announced that it has been carrying out offensive attacks against ISIS.[72] These types of operations are carried out on a unilateral basis. In conjunction with other countries, such as those in the NATO alliance, defence and security policies are not based on cyber

[67] See Baylon, C. (2014), *Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives*, Research Paper, London: Royal Institute of International Affairs, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20141229CyberSecuritySpaceSecurityBaylonFinal.pdf (accessed 1 Dec. 2017).
[68] Denning, D. (2015), 'Assessing Cyber War', in Blanken, L. J., Rothstein, H. and Lepore, J. J. (eds) (2015), *Assessing War: The Challenge of Measuring Success and Failure*, Washington, DC: Georgetown University Press, pp. 266–285.
[69] Federation of American Scientists (2012), *Presidential Policy Directive 20: U.S. Cyber Operations Policy*, Washington: Federation of American Scientists, https://fas.org/irp/offdocs/ppd/ppd-20.pdf (accessed 1 Dec. 2017).
[70] Ibid.
[71] Cyber Security Intelligence (2017), 'Which Countries are Ready for Cyber War?', 18 September 2017, https://www.cybersecurityintelligence.com/blog/which-countries-are-ready-for-cyberwar-2763.html (accessed 30 Nov. 2017).
[72] Then UK defence secretary Sir Michael Fallon speaking at Chatham House Cyber 2017 Conference in June 2017.

capabilities. That said, NATO has a computer incident response capability and reaction teams that can be deployed in emergencies.[73]

The alliance's strategic assets in terms of communications between states are also vulnerable to cyber offensive activities. Protecting the information in interoperable weapons systems within NATO during operations is a hard task. There is a varying degree of awareness of this and little appetite to tackle the issue, which is further exacerbated by clashing cybersecurity cultures in the 29 member states. The Tallinn Manual 2.0, which addresses the application of international law in cyber operations, provides some guidance as to expected behaviour of states against cyberattacks in times of conflict and warfare.[74] Although it is established that international law applies in cyberspace[75] and it is proposed that the rules of warfare also apply, red lines in this area are not yet well defined or universally accepted.

The use or threat to use cyber offensive capabilities is inherently destabilizing, creating doubts in regard to the credibility and reliability of nuclear capabilities. In a crisis, offensive cyber capabilities might have disabled the nuclear weapons system, leading to asymmetric information that could result in both sides being overconfident in their retaliatory capabilities and thus more willing to act in a risky manner.

[73] NATO (2016), 'NATO Cyber Defence', www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf (accessed 1 Dec. 2017).
[74] NATO Cooperative Cyber Defence Centre of Excellence (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press.
[75] UN Secretary General's Group of Governmental Experts (2015), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, New York: United Nations General Assembly, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (accessed 1 Dec. 2017).

5. Cyber Resilience

Most countries rely on a form of best practice to deal with cyberattacks. Cyber hygiene – adhering to best practice in daily cyber routines and individual behaviours – in addition to robust cyber and supply chain security policies are necessary for all stakeholders, including when safeguarding nuclear laboratories, facilities and assembly mechanisms, and when securing the supply chain, in both hardware and software. Whereas a well-crafted cyberattack requires only a single port of entry to a system, cyber defence and resilience requires simultaneous protection of all critical systems and components in a timely fashion.[76]

While examining cyber risks, decision-makers should also consider offsetting risk with resilience measures. The best way to minimize the severe consequences of a cyberattack on nuclear weapons systems is to create resilient cybersecurity architecture, based on three key interlinked pillars: people, technology and processes. In this equation, people are both the strongest and the weakest link, particularly with the high volume of personnel at defence companies; technological advancements continuously challenge the integrity and resilience of systems in use; and organizational processes are not always mature enough, for instance, to accurately identify insider threat problems, report misconduct, or identify responsible units and personnel within an organization. In addition, the high volume of personnel from subcontracted agencies presents several opportunities for infiltration.

Technological advances and the human factor mean it is no longer sufficient (or perhaps even possible) to isolate computer systems from the internet, a process known as air-gapping. The Stuxnet attack on Iranian 'air-gapped' nuclear centrifuges, for instance, illustrated the ability to infiltrate sensitive systems through a simple thumb drive and therefore the unreliability of air-gaps. In 2014, researchers used radio signals to connect to an isolated network by using a remote mobile phone with malware – again demonstrating the unreliability of air-gaps.[77] In 2016, researchers in Ben-Gurion University of the Negev were able to exfiltrate data from an air-gapped computer through the sounds of the computer's cooling fans.[78] It is therefore necessary to discontinue reliance on air-gapping and embed layers of security in order to protect strategic assets, and it is clear that systems will continue to be challenged by human and technological interferences for the foreseeable future.

[76] Fritz, J. (2009), *Hacking Nuclear Command and Control*, Canberra: International Commission on Nuclear Non-proliferation and Disarmament, http://www.icnnd.org/Documents/Jason_Fritz_Hacking_NC2.pdf (accessed 1 Dec. 2017).
[77] Mordechai, G., Kedma, G., Kachlon, A. and Elovici, Y. (2014), 'Air-Hopper: Bridging the Air-Gap between Isolated Networks and Mobile Phones Using Radio Frequencies', *9th IEEE International Conference on Malicious and Unwanted Software (MALCON 2014)*, pp. 58–67, doi: 10.1109/MALWARE.2014.6999418.
[78] Ben-Gurion University of the Negev (2016), 'Cyber Security Researchers Find Another Way to Hack an Air-Gapped Computer Through the Machine's Cooling Fans', 30 June 2016, http://in.bgu.ac.il/en/Pages/news/hack_fan.aspx (accessed 1 Dec. 2017).

Possible resilience measures

Trust and trustworthy systems

Countries engaged in a military alliance must have trust at the centre of their nuclear weapons system architecture. Establishing a clear understanding of cyber nuclear security culture based on trust within the nuclear weapons industry, the supply chain, and in organizational structures (such as personnel recruitment and vetting) requires an ongoing effort. Common practices pay particular consideration to safety measures, but the security perspective plays less of a role.

IT and digital systems form a crucial part, for instance, of NATO's ballistic missile systems, ground surveillance system, aerial vehicle and ground control stations, and nuclear command and control structure. The crucial information and data needed to make a decision comes through IT and industrial control systems.[79] Any intrusion in the process of receiving information would impair system integrity and cripple confidence in the received information.

Risk and intelligence assessments

Effective risk assessment requires constant tests and checks for threats and vulnerabilities in industrial control systems. In 1997, the US National Security Agency (NSA) conducted its first large-scale cyber-testing operation to ascertain the US military's agility against cyberthreats. The exercise, known as Eligible Receiver, revealed that the US military's telecommunications system could be hacked through commercial software.[80] As a result of the exercise, the military purchased intrusion detection systems and installed them in a large number of computers. This allowed them to identify a real cyberattack just months after the exercise.[81]

A similar operation in 2008 revealed that the threat had not disappeared. The US Government Accountability Office (GAO) studied physical and cybersecurity in the Los Alamos National Laboratory. The results showed vulnerabilities in the areas of identifying and authenticating users; encrypting sensitive information; and monitoring and auditing security policy compliance.[82] In order to tackle these challenges to cybersecurity, the US National Nuclear Security Administration in the Department of Energy set up the Baseline Cyber Security Program, mapping out an organization-wide risk-management approach.[83]

While the likelihood of a cyberattack on nuclear weapons systems is increasing, current risk management approaches fall short of capturing the probabilities and consequences of such an attack. Since it is hard to quantify the probabilities, one way forward would be for risk assessments

[79] El Fertasi, N. and De Vivo, D. (2016), 'Cyber Resilience: protecting NATO's nervous system', *NATO Review Magazine*, 12 August 2017, http://www.nato.int/docu/review/2016/Also-in-2016/nato-cyber-resilience-security/EN/index.htm (accessed 1 Dec. 2017).
[80] Kaplan, F. (2016), *Dark Territory: The Secret History of Cyber War*, New York, NY: Simon & Schuster, pp. 57–73.
[81] Ibid. p.80
[82] US GAO (2008), *Nuclear Security: Los Alamos National Laboratory Faces Challenges in Sustaining Physical and Cyber Security Improvements*, Washington: Government Accountability Office, http://www.gao.gov/new.items/d081180t.pdf (accessed 1 Dec. 2017); US GAO (2009), *Information Security: Actions Needed to Better Manage, Protect and Sustain Improvements to Los Alamos National Laboratory's Classified Computer Network*, Washington: Government Accountability Office, http://www.gao.gov/assets/300/296796.pdf (accessed 1 Dec. 2017).
[83] National Nuclear System Administration (NNSA) (2012), *Baseline Cyber Security Program*, Washington, https://nnsa.energy.gov/sites/default/files/nnsa/08-13-inlinefiles/2013-08-21%202%20NAP-14.1D%2012-14-12.pdf (accessed 1 Dec. 2017).

to be made through an analysis of a combination of threats, vulnerabilities and consequences, specifically detailing different threat levels and/or areas of vulnerabilities in a qualitative manner.

This represents a new approach and could assist in closing the loopholes in nuclear weapons systems and generate cyber resilience.

Possible consequences

The most severe consequence of a cyberattack on one or more nuclear weapons systems would be the inadvertent launch of missiles and/or the inadvertent detonation of a warhead that lead to a significant loss of life. Further consequences of such a cyberattack include sector-level impacts, such as in the medical sector, which may have to deal with casualties; disruption of workforces and operations of defence companies or vendors; as well as economic and reputational costs to countries and private companies. Such an event would also increase the likelihood of crisis and conflict.

A compromised nuclear system that cannot be trusted and lacks credibility will undermine nuclear deterrence and its rationale. Additionally, the assurances that nuclear weapons states make to allies would likely lose their reliability if an adversary could successfully hack into the nuclear weapons systems on which several countries rely. The established bilateral and multilateral relations, based strongly on nuclear deterrence, are therefore likely to be brought into question as more evidence of cyber insecurities and the potential for cyberattacks within the nuclear weapons architecture come to light in the future.

6. Recommendations

Actions to reduce the risk of cybersecurity vulnerabilities may take place in the public and private sector, as well as at the national and international levels. The private sector is often on the cutting edge of innovation in cyber development. Therefore, in order to avoid being left behind the technological curve, it is important for states to retain private sector expertise into national defence strategies. Closer coordination between national defence departments and the private sector will ensure that the most recent technology is used and that defence policies are in sync with cyber innovation.

However, there is a contradiction in cooperating with the private sector. Although states need to limit their own cyber vulnerabilities, the existence of technical vulnerabilities could give them an advantage in future cyber offensive campaigns. In other words, national cyber agencies may prefer to be at the forefront of writing malicious codes and infiltrating industrial control systems, rather than openly sharing information about software vulnerabilities with manufacturers or users. For example, the NSA has been accused of developing and storing cyber vulnerabilities, which was demonstrated by the discovery of the WannaCry ransomware.[84]

At the national level, in times of uncertainty, states will tend to err on the side of shifting away from behaviour that could be misinterpreted. Russia, for instance, cancelled its air force exercises and called off planned missile testing in response to the 11 September 2001 Al-Qaeda attack.[85] The continuation of this type of behaviour will help prevent unintentional escalations at times of heightened tensions, particularly when time is limited and there is political and public pressure to respond to an attack.

Cybersecurity preparedness requires the analysis of possible cyber risk scenarios and an evaluation of threat vectors and consequences. There are nine countries that possess nuclear weapons and therefore, at a minimum, 18 scenarios involving two actors, an aggressor and a defender.[86] The likelihood of these scenarios and survivability of nuclear forces should be examined in detail in these studies. Survivability of nuclear forces differs from country-to-country and country-specific analysis should be incorporated in preparations. Defence planners already usually account for system failures and an opponent's defence mechanisms in their targeting strategies, a useful addition to this would be to take into account cyberattacks and their consequences. By understanding such pressures states can explore arms control and other cooperative security measures to reduce miscalculation and avoid unintentional destabilizing actions.

Mitigation measures to prevent misunderstanding between nuclear weapons states may include building in more time in the decision-making process to allow for better informed decisions. In

[84] Jopson, B. and Kuchler, H. (2017), 'US official defends NSA over WannaCry cyber attack', *Financial Times*, 15 May 2017, https://www.ft.com/content/74ae2600-39a3-11e7-ac89-b01cc67cfeec (accessed 1 Dec. 2017).
[85] Doscher, T. (2011), 'In their own words—NORAD members recall September 11: William Glover', Defence Video Imagery Distribution System (DVIDS), https://www.dvidshub.net/news/76668/their-own-words-norad-members-recall-september-11-william-glover (accessed 1 Dec. 2017).
[86] Scenarios could include improper launch in Pakistan, a compromised launch between China and North Korea, or a scenario between North Korea and the US, in which North Korea compromises the integrity of US EAM.

addition, increasing the number of people responsible for decisions in nuclear command and control, and increasing the number of intelligence-sharing measures, may lead to better informed decisions.

For critical systems, redundancy measures are very important – meaning that if a component fails, the system would continue to function through back-up components. One of the redundancy measures employed in nuclear weapons systems, for example, is to rely both on digital and analogue routes for command and control. Ongoing system engineering should also be incorporated into the whole lifecycle of weapons systems and used to maintain system integrity even under stress. To achieve this, cybersecurity needs to be considered and included from the design stage onwards.

Further precautionary measures may involve states reviewing significant procurement processes in the defence sector with special attention paid to cybersecurity. Such measures could include conducting stress-testing and simulation exercises to judge the suitability of components to provide reliable information. Moreover, engaging in multilateral threat and intelligence sharing with allies would help to rapidly assess the credibility of communication and information. On the technical side, examining the vulnerability management lifecycle of cyber systems would be a useful precautionary measure to ensure ongoing compatibility as IT systems and industrial control systems have different lifecycles. Protocols for submarine and other platforms and facilities and developing well-understood standards may help reduce the false belief about the security of air-gapping.

Cyber incident hotlines that provide direct links between governments for use in times of heightened tension would allow them to re-examine the emerging situation, to acknowledge the threat and respond accordingly. As part of this approach it may be essential to have a dedicated cybersecurity team on submarine patrols going forward. Similarly, it may become imperative to establish national cyber emergency response teams that focus fundamentally on industrial control systems in nuclear weapons complexes.

7. Conclusion

Cyber vulnerabilities within nuclear weapons systems and structures present a whole set of dangers and risks. At best, cyber insecurity in nuclear weapons systems is likely to undermine trust and confidence in military capabilities and in the nuclear weapons infrastructure. At worst, cyberattacks could lead to deliberate misinformation and the inadvertent launch of nuclear weapons. In times of crisis, loss of confidence in nuclear weapons capabilities would factor into decision-making and could undermine beliefs in nuclear deterrence – particularly in extending nuclear deterrence to allied countries. The challenges that cyber risks pose to nuclear weapons systems could be seen as an opportunity to create a cross-cutting risk mitigation measure that benefits both traditional adherents and sceptics of nuclear deterrence.

The loss of trust in nuclear weapons systems due to compromised data integrity or a systems failure would create significant issues for policymakers. In that eventuality, strategies that give decision-makers more time to respond will help to ease the process. Redundancy in communication systems may help to increase system resilience and help check the trustworthiness of information. At a time when decision-makers do not trust nuclear weapons systems, verification of information through diversified intelligence sources would be crucial.

Decision-makers should be informed about the confidence and uncertainties in the cybersecurity of nuclear weapons systems. They should also take part in simulations where decision-making processes can be elaborated in detail. For example, red-teaming exercises role play situations of high-uncertainty and reduced time frames to make decisions. It is highly important that decision-makers, rather than their deputies or staff, take part in this process.

This research paper covers the main attack vectors (both physical and cyber components) without prioritizing attack types based on the level of threat and vulnerability. The logic behind the equal treatment of attack vectors is that any of them could be the target of a successful cyberattack that would compromise an entire system. A future study on the scope of the attack surface that describes the different levels of threat for each attack vector would be particularly helpful for an overall technical assessment of nuclear weapons systems.

Future research could include semi-structured interviews with current or former military officials, technical officers, and political figures in nuclear weapons states and nuclear host countries. This would include discussing how confident they are or were with the nuclear weapons complex and digital systems (e.g. C3) while making decisions. It would also go some way to providing an answer to an important question: do key decision-makers have sufficient knowledge with regards to the integrity and trustworthiness of nuclear weapons systems?

A study into emerging technologies and their impact on strategic stability would be another worthwhile research area, key topics would include examining big-data processing and stealth technology capabilities, such as unmanned underwater vehicles.

Cyber vulnerabilities of nuclear weapons systems are presenting dangers that have been seldom considered in the public domain. The subject requires urgent attention from academia and

governments – including those without nuclear weapons but which have nuclear allies, particularly if nuclear weapons are stationed on their territories, and in any country that might be affected by the use of nuclear weapons.

It is unlikely that nuclear weapons possessing governments will be forthcoming in public or with each other on the cyber vulnerabilities of nuclear weapons systems. The one exception may be between the UK and the US, both of which possess systems that are already highly integrated and connected from the design to the deployment stages. However, it is vital that academics, think-tanks and NGOs press for information and reassurances from governments that such issues are being addressed, and that those governments are holding open discussions with the public, including the media and parliamentarians. After all, it is the public that will pay the ultimate price for complacency regarding cybersecurity of nuclear weapons systems.

About the Authors

Dr Beyza Unal is a research fellow with the International Security Department at Chatham House. She specializes in nuclear weapons policies and leads projects on chemical, biological, radiological and nuclear weapons. Dr Unal is also conducting research on cybersecurity and critical infrastructure protection, with a particular focus on civil nuclear power plants. She formerly worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, taught International Relations, transcribed interviews on Turkish political history, and served as an international election observer during the 2010 Iraqi parliamentary elections. She is interested in NATO's defence and security policy as well as security in the Middle East. She is a Fulbright Program Alumna.

Dr Patricia Lewis is the research director of the International Security Department at Chatham House. Her former posts include deputy director and scientist-in-residence at the James Martin Center for Nonproliferation Studies at the Monterey Institute of International Studies; director of UNIDIR; and director of VERTIC in London. She served on the 2004–06 WMD Commission chaired by Dr Hans Blix, and the 2010–11 Advisory Panel on Future Priorities of the OPCW, chaired by Ambassador Rolf Ekeus. She was an adviser to the 2008–10 International Commission on Nuclear Non-proliferation and Disarmament chaired by Gareth Evans and Yoriko Kawaguchi. She was a commissioner on the 2014–16 Global Commission on Internet Governance chaired by Carl Bildt.

Acknowledgments

Many people have contributed to this research paper. In particular, we wish to express our appreciation to our partners, the Stanley Foundation, and the generous contributions of Ben Loehrke, Danielle Jablanski and Magda Gibson throughout the process.

Particular thanks also go to Heather Roff and Austin Long for preparing papers for a meeting held at Chatham House in July 2017, the findings of which contributed to this paper. Realizing the importance of interdisciplinary research, we are grateful to all attendees from nuclear, cyber and artificial intelligence communities who participated in the meeting. We also wish to thank our colleagues at UNIDIR, John Borrie, Wilfred Wan and Tim Caughley for all of their feedback as well as the opportunity to discuss the paper's findings at the UN in Geneva.

Finally, many thanks to Henry Dodd and Nilza Amaral for their meticulous organizational skills; to Kevin Robb and Farah Bogani for assisting with the paper, and to the Chatham House editorial team.

Independent thinking since 1920

The
Stanley
Foundation

Cover image: Launch Control Center control panel for the Minuteman III nuclear intercontinental ballistic missiles located in New Ramer, Colorado.

Photo credit: Copyright © Andy Cross/Contributor/Getty Images

ISBN 978 1 78413 255 2

This publication is printed on recycled paper.

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700 F +44 (0)20 7957 5710
contact@chathamhouse.org www.chathamhouse.org

Charity Registration Number: 208223