Royal United Services Institute
for Defence and Security Studies

Occasional Paper

Cyber Threats and Nuclear Weapons

New Questions for Command and Control, Security and Strategy

Andrew Futter

Cyber Threats and Nuclear Weapons

New Questions for Command and Control, Security and Strategy

Andrew Futter

RUSI Occasional Paper, July 2016

Royal United Services Institute
for Defence and Security Studies

Over 180 years of independent defence and security thinking

The Royal United Services Institute is the UK's leading independent think-tank on international defence and security. Its mission is to be an analytical, research-led global forum for informing, influencing and enhancing public debate on a safer and more stable world.

Since its foundation in 1831, RUSI has relied on its members to support its activities, sustaining its political independence for over 180 years.

London | Brussels | Nairobi | Doha | Tokyo | Washington, DC

Published in 2016 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, July 2016. ISSN 2397-0286 (Online).

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)

Contents

Acknowledgements

The author would like to thank David Blagden, Des Browne, Peter Dombrowski, Matt Fuhrmann, Adrian Johnson, Martin Libicki, Nick Ritchie, Kris Stoddart, Ian Wallace and the anonymous reviewers and staff at RUSI for their comments and thoughts on this paper; the many experts and officials that generously gave up their time to be interviewed or speak with me both on and off the record about the project; and Bill Potter and the team at the James Martin Center for Nonproliferation Studies in Monterey who kindly agreed to host me while I finalised the writing. The research is part of a larger project investigating the impact of cyber threats for nuclear weapons, which is funded by the UK Economic and Social Research Council (ESRC) Future Research Leaders scheme, grant number ES/K008838/1.

Introduction: Hacking the Bomb

THE DEVELOPMENT AND spread of cyber 'weapons', information-warfare capabilities and the new dynamics of the 'cyber age' are providing a considerable – albeit nuanced – challenge to the management, thinking and strategy that underpins nuclear weapons. While the nature and extent of these challenges varies between nuclear-armed states and across nuclear systems, they do, taken together, represent a noticeable shift in the context and environment in which we think about nuclear weapons and nuclear security, manage nuclear relationships and regulate global nuclear order. The result is a new collection of both direct and indirect challenges for nuclear forces, which have implications for current arms control agreements and regimes, the maintenance of stable nuclear balances, and the possibility of future nuclear reductions.

The safe, secure and reliable management of nuclear weapons has always been a complex business, plagued by uncertainties and risks, and the past is littered with accidents, miscalculation and near misses. But many of the challenges associated with the command and control (C2) of nuclear weapons are being magnified, aggravated and, in some cases, recast by the new tools, dynamics and capabilities that fall loosely under the rubric of cyber. Of particular significance is the growing threat posed by hackers seeking to gain access to, or interfere with, these highly sensitive systems, their infrastructure, and the weapons that they control. As the Global Zero Commission on Nuclear Risk Reduction has pointed out:

> Questions abound: could unauthorized actors – state or non-state – spoof early warning networks into reporting attack indications that precipitate overreactions? Could such hackers breach the firewalls, the air gaps, and transmit launch orders to launch crews or even to the weapons themselves? What if an insider colluded with them to provide access and passwords to the launch circuitry? Might they acquire critical codes by hacking?[1]

While it has been over two decades since John Arquilla and David Ronfeldt warned, in a seminal article on the subject, that 'cyberwar [was] coming',[2] and over 30 years since a teenage hacker broke into a top-secret Pentagon computer and nearly started a nuclear Third World War in the Hollywood blockbuster *War Games*, the nature, challenges and implications of this new cyber–nuclear nexus remain understudied and little understood and, as a contemporary dynamic, it remains largely unaddressed.[3]

1. Global Zero Commission on Nuclear Risk Reduction, 'De-alerting and Stabilizing the World's Nuclear Force Postures', April 2015, p. 29.
2. John Arquilla and David Ronfeldt, 'Cyberwar is Coming!', *Comparative Strategy* (Vol. 12, No. 2, 1993), pp. 141–65.
3. A few notable exceptions include: US Department of Defense, Defense Science Board, 'Task Force Report: Resilient Military Systems and the Advanced Cyber Threat', January 2013; Jason Fritz, 'Hacking Nuclear Command and Control', International Commission on Nuclear Non-proliferation and disarmament, 2009, (updated 2016); Franz-Stefan Gady, 'Could Cyber Attacks Lead to Nuclear

The cyber threat to nuclear weapons is myriad in scope: there is the challenge to safe, secure and reliable nuclear C2; new problems for information security, proliferation and the safeguarding of highly sensitive nuclear secrets; challenges for strategic deterrence and escalation; and the emergence of a cyber-nuclear security dilemma that must be factored into future crisis management. However, while the growth of cyber capabilities and the associated technological dynamics of the information age are undoubtedly providing new challenges for established nuclear thinking, they do not – at least not yet – fundamentally undermine or supersede the role of nuclear weapons as the ultimate guarantor of national security. Attacks on computers, software or key systems are unlikely to become 'strategic' or 'existential' any time soon – even the highly sophisticated Stuxnet worm(s)[4] was limited in its destruction, did not cause any fatalities, and took many years and considerable expertise to perfect. Notions of a possible 'cyber Pearl Harbor'[5] or a 'cyber 9/11'[6] are therefore inherently problematic and – at least for the moment – probably over-hyped.[7] As PW Singer and Allan Friedman explain, 'crippling attacks out of the blue, the ultimate threat from the offense's advantage, are not as easy to pull off in the cyber world as is often depicted'.[8]

Nevertheless, the possibility that hackers might steal sensitive information, alter software code, infiltrate and compromise networks, computers and critical communications links, or interfere with other associated hi-tech systems – and the potential to do this in advance, from afar, and possibly without the adversary knowing – raises a whole new set of challenges and questions for nuclear weapons management, security and strategy. How has the challenge of safeguarding key nuclear secrets or other highly sensitive operational information changed? What impact might this have on nuclear non-proliferation efforts and the spread of nuclear weapons 'know-how'? How can a state be sure that early-warning systems or other components of nuclear C2 have not been compromised or sabotaged and will work as intended, especially in a crisis? Could terrorists or 'lone wolf' hackers somehow (either directly or indirectly) cause a nuclear launch or detonation through hacking? And what do these new types of 'weapon' mean for concepts of deterrence, nuclear and more broadly, strategic stability and possible escalation? Ultimately, increased uncertainty about the integrity and security of nuclear systems, and their component parts, means that we need to consider the implications for nuclear force management, thinking and strategy for all nuclear-armed states.

War?', *The Diplomat*, 4 May 2015; John Reed, 'Keeping Nukes Safe From Cyber Attack', *Foreign Policy,* 25 September 2012; Andrew Futter, 'War Games Redux? Cyber Threats, U.S.–Russian Strategic Stability and Future Nuclear Reductions', *Deep Cuts Issue Brief No. 6,* September 2015; Global Zero Commission, 'De-alerting and Stabilizing the World's Nuclear Force Postures'.

4. According to Kim Zetter, there were at least two versions of the Stuxnet worm, and possibly more yet to be discovered. Interview with the author.
5. 'Remarks by Secretary [of Defense Leon] Panetta on Cybersecurity to the Business Executives for National Security', New York City, 11 October 2012. <http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136>, accessed 22 June 2016.
6. A phrase used by US Homeland Security Secretary Janet Napolitano in January 2013. See Deborah Charles, 'US homeland chief: cyber 9/11 could happen "imminently"', *Reuters*, 24 January 2013.
7. Tom Gjelten, 'Is All the Talk about Cyberwarfare Just Hype?', *NPR*, 15 March 2015.
8. PW Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), p. 155.

As the above list of concerns demonstrates, the challenge of the cyber age for the ultimate weapon is actually more nuanced than it first appears. Cyber complicates and obfuscates the intrinsic difficulties of nuclear C2 and nuclear strategy, rather than fundamentally transforming them. Despite this, these new challenges – taken together – do represent an important shift in the nature of the environment in which nuclear weapons are thought about, how states manage their nuclear forces and how nuclear policy and strategy are made. Accordingly, the cyber challenge will have both direct and indirect implications not just for nuclear security and C2 but also for global and regional strategic balances, the maintenance of current nuclear arms control agreements, and for any future moves towards nuclear reductions and possible disarmament. Given the large number of nuclear weapons that remain in the world, and the spread of these weapons and the associated technology and expertise to a new range of actors, we are fast entering a period where the central dynamics, beliefs and thinking that underpin global nuclear order need to be reassessed in the light of the new cyber context.

The main aim of this paper is to unpack and demystify the cyber challenge to nuclear weapons, place it in context, and provide a framework through which to understand, evaluate and ultimately address the emerging cyber–nuclear nexus. The paper proceeds in three parts: the first begins by clarifying what is meant by the term 'cyber' and presents a suitable framework through which to examine the nuclear weapons enterprise, before going on to explain how and in what ways nuclear weapons systems might be vulnerable to cyber threats. The second part looks at the different challenges posed by hackers. These range from espionage and threats to systems and information security, through to sabotage and the risk of interference, destruction or even unauthorised nuclear use. The actors involved, and their intentions, also vary markedly, particularly with regard to the differences between the dangers posed by non-state actors and by nation states. The third part considers the implications of the cyber challenge for strategic stability and crisis management, nuclear strategy and the logic of seeking to deter cyber-attacks with nuclear weapons. The conclusion brings the central themes and arguments of the piece together, puts cyber in context alongside other emerging techno-military dynamics affecting the contemporary global nuclear environment, outlines the key challenges for the nuclear enterprise, and makes some recommendations for policy-makers and government officials for managing the cyber–nuclear nexus in the future.

I. The Nature of the Cyber Challenge to Nuclear Weapons

COMPUTERS AND COMPLEX systems have always been central to nuclear C2, and the need to manage and co-ordinate increasingly sophisticated and intricate weapons, sensors and war plans, was a principal driver of early computer technology.[1] But the many, and often competing, requirements of nuclear C2 have also meant that these systems have always contained certain vulnerabilities, and the past is littered with accidents and near misses – a reasonable proportion of which can be linked either directly or indirectly to computers and the inherent problems of high-tech systems. In this way cyber threats are both exacerbating and recasting the intrinsic challenges of nuclear C2, security and strategy. They are doing this by presenting and creating new vulnerabilities within existing systems that might be exploited by hackers, rather than fundamentally altering the business of nuclear weapons management. The aim of this part of the paper is therefore to outline the nature of the cyber challenge and explain how this is creating new problems and dynamics for the safe, secure and reliable C2 of nuclear weapons, and for the nuclear weapons enterprise more broadly.

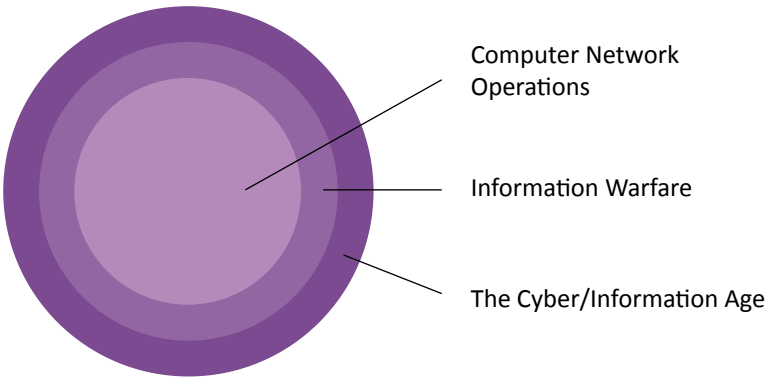
What is Cyber?

The nature and meaning of the term 'cyber' is fundamentally contested, it is viewed differently by different states and actors,[2] and there exists no one definition that all adhere to when seeking to use and analyse the concept.[3] The natural result is that different analyses – and analysts – come to different conclusions and offer different solutions to cyber-related problems and questions; this unfortunately continues to hamstring much cyber analysis, and has complicated the ongoing cyber debate. Definitions of 'cyber' range from the very narrow to the very broad. Narrow definitions are used in the work of those who focus primarily on computer network

1. For an interesting overview of how this developed in the US see Kent Redmond and Thomas M Smith, *From Whirlwind to MITRE: The R&D Story of the SAGE Air Defense Computer* (Cambridge MA: MIT Press, 2000).
2. For example, Russia and China tend to prefer the label 'information' as opposed to the Western preference for 'cyber'. For more on this see Keir Giles and William Hagestad II, 'Divided by a Common Language: Cyber Definitions in Chinese, Russian and English' in K Potins, J Stinissen and M Maybaum (eds), *Proceedings of the 5th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE Publications, 2013).
3. Perhaps the best definition is provided by Daniel Kuehl, who describes cyber as 'an operational domain framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and Internetted information systems and their associated infrastructure', see Daniel Kuehl, 'From Cyberspace to Cyberpower: Defining the Problem', in Franklin Kramer, Stuart Starr and Larry Wentz (eds), *Cyberpower and National Security* (Dulles VA: Potomac Books Inc, 2009), p. 28.

operations (CNOs)[4] and attacks over and through the internet. Somewhat broader definitions are used in the work of those who tend to see cyber as closer to, or part of, the field of information warfare, which includes more than just CNOs – it also involves other information operations and, possibly, other types of electronic warfare (see Figure 1). The broadest definitions of 'cyber' are used in analyses that treat cyber as a holistic concept affecting every part of national security thinking, on the basis that we are living in a 'cyber age'. As William Owens, Kenneth Dam and Herbert Lin remark: 'It is perhaps emblematic of the state of discussion today that there is no standard and widely accepted term that denotes attacks on computer systems and networks'.[5]

Figure 1: Taxonomy of Cyber Definitions

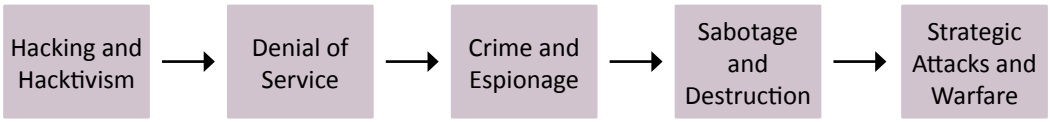


As well as being hamstrung by a lack of definitional clarity in the use of the word 'cyber', cyber analysis is also hampered by the considerable differences between types of cyber-attack and how 'attack' is defined.[6] Attacks can range from simple hacking, hacktivism, nuisance and crime – which might be carried out by a number of different types of actor and be of relatively minimal concern – through to denial of service and espionage, sabotage, destruction and possibly existential attacks and war (see Figure 2). These latter threats are much more likely to be the preserve of powerful actors or nation states.[7] As Thomas Rid and Peter McBurney explain: 'Cyber

4. Computer Network Operations (CNO) includes both Computer Network Attack (CNA), which refers to sabotage/attack and possibly warfare, and Computer Network Exploitation (CNE), which refers primarily to hacking and espionage. However, 'attack' is often used indiscriminately to refer to all cyber activities.
5. William Owens, Kenneth Dam and Herbert Lin (eds), *Technology, Policy, Law and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities* (Washington DC: National Academies Press, 2009), pp. 14–15.
6. As Owens et al. suggest, 'cyberattack must be clearly distinguished from cyberexploitation, which is an intelligence gathering activity rather than a destructive activity'. Owens, Dam and Lin, *Technology, Policy, Law and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities*, p. 1.
7. As former US Director of National Intelligence Mike McConnell puts it, 'There is a hierarchy. You go from nation states which can destroy things, to criminals who can steal things, to aggravating

weapons span a wide spectrum. That spectrum ... reaches from *generic but low-potential tools to specific but high-potential weaponry*'.[8]

Figure 2: Range of Cyber Threats



It is the diverse nature of the scope and challenge of cyber-attacks that creates many of the problems that affect cyber analysis and is a key reason for the continued disagreement about the level and nature of the threat.[9]

Clearly each of these frames of analysis, from the very narrow to the very broad, has benefits and drawbacks. But when considering the challenges to the nuclear weapons enterprise, it makes most 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 primarily logical domain of CNOs.[10] In this way, the framework adopted in this study is designed to take account of the impact that the broader cyber environment is having on nuclear thinking and strategy by treating cyber as an operational domain, an offensive capability, a societal development, and also as a set of actors. While the discrete threat of hacking and attacks through the internet are clearly important, they are far from the only dynamics that will affect the nuclear weapons enterprise in the cyber context. Instead, the cyber 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.[11] Importantly, this approach also allows consideration of what is new and what is not when understanding the cyber phenomenon.

---

but skilful hackers', see Mike McConnell, 'Cyberwar is The New Atomic Age', *New Perspectives Quarterly* (Vol. 26, No. 3, 2009), p. 76.

8. Thomas Rid and Peter McBurney, 'Cyber-weapons', *RUSI Journal* (Vol. 57, No. 1, 2012), p. 8.
9. As Danny Yadron and Jennifer Valentine-Devries point out, 'cyber is both overused and too vague as a description of anything – often bad – that involves a computer'. See Danny Yadron and Jennifer Valentine-Devries, 'This Article Was Written With the Help of a "Cyber" Machine', *Wall Street Journal*, 4 March 2015.
10. Franklin Kramer has described cyber as involving 'physical infrastructure, operational software, information and people', see Franklin Kramer, 'Cyberpower and National Security: Policy Recommendations for a Strategic Framework' in Kramer, Starr and Wentz, *Cyberpower and National Security,* p. 6. Martin Libicki has proposed a three-tiered framework that encompasses 'physical, syntactic and semantic' levels of analysis. See Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), p. 24.
11. This builds on a definition provided by Jason Andres and Steve Winterfield in *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Waltham MA: Syngress, 2011), p. 167.

In this way cyber-attacks on nuclear weapons infrastructure 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; or *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. Logical attacks might be carried out remotely through computer networks and over the internet by attacking software, such as through the deployment of certain malware, logic bombs, hardware or software Trojans,[12] or in situ by those with close physical access to systems (either wittingly or unwittingly). Cyber-attacks might also be directed at the information on which these systems and therefore human operators act and make their decisions – such as by altering key information sets and data.[13] The cyber challenge therefore also incorporates the natural problems inherent in increasingly complex (computer) systems – such as badly written software or program 'bugs'[14] – and the overall uncertainty and risk of whether key systems will always work as expected. As such, the cyber challenge to nuclear security 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, perhaps the key components of cyber are humans: it is people that design systems, write software and place their faith in computers and machines to carry out tasks as intended.[15] It is important to remember that the human–computer interface remains a key battlefield in the cyber age – computers do not think (at least not yet), they do what they are programmed to do.

As a result of these observations, this paper adopts an approach that seeks to consider the challenge to nuclear weapons posed by cyber in a holistic manner (see Figure 3). As such, it considers not just attacks on nuclear weapons over the internet, but also broader types of attack on information and information systems related to the nuclear weapons enterprise, as well as other cyber-attacks that may involve – but are not necessarily directed against – nuclear weapons (more on this in Chapter III). We can classify this in terms of seven sets of descriptors:

1. *Broad-based* attacks on civilian or military infrastructure that might have implications for nuclear forces (such as deterrence and strategy) and *discrete* attacks directed at nuclear weapons, C2 and associated components and infrastructure specifically.

12. A Trojan is malware that can be buried in a system and activated remotely or when certain conditions are met.
13. This draws on the framework developed by Lucas Kello in 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft', *International Security* (Vol. 38, No. 2, 2013), p. 18.
14. Bugs are unintended errors in software and coding and not 'cyber attacks'. The phrase 'bug' derives from a moth that became caught between relays of an early and primitive computer at Harvard University in 1947. See 'Moth in the Machine: Debugging the Origins of "Bug"', *Computer World*, 3 September 2011.
15. As Bruno Tertrais has pointed out, 'Nuclear security procedures and controls are only as strong as their weakest part, and, as in most other organizations, that is often the human element'. See Bruno Tertrais, 'The Unexpected Risk: the Impact of Political Crises On the Security and Control of Nuclear Weapons', in Henry Sokolski and Bruno Tertrais (eds), *Nuclear Weapons Security Crises: What Does History Teach?* (Carlisle PA: Strategic Studies Institute and US Army War College Press, July 2013).

2. Attacks and vulnerabilities that primarily target *computers* and *machines*, those that principally focus on *humans*, and those that involve a combination of the two.
3. *Physical* attacks on computers, software, hardware, communications links or networks related to nuclear weapons (such as destroying an early-warning satellite or radar, crashing a computer or compromising communications), and *logical* attacks – those conducted either at a distance and remotely, and through the exploitation of malware, logic bombs and other computer-based attacks.
4. Attacks conducted from afar through networks or the internet, or those conducted either intentionally or unwittingly by actors in close proximity to the target.
5. Attacks on nuclear systems directly (either espionage or sabotage) and attacks that target nuclear systems indirectly (such as through the information they rely upon).
6. Problems that are *inherent* in software (or hardware) and technology that could lead to normal accidents and create vulnerabilities to be exploited, and attacks that are *deliberate* and carried out intentionally by an adversary – likely through exploiting these vulnerabilities.
7. Challenges that are *actual* – such as infected software, compromised systems, hardware that has been damaged or destroyed, altered or corrupted – and those that are *perceptual*, and are based on worst-case thinking and an assumption that the systems have been compromised or may not work, irrespective of whether they have been, might be, or will be.

Figure 3: A Holistic Approach to Understanding the Cyber Challenge to Nuclear Weapons

Focus/Target	Broad Focus (Against Society or Critical National Infrastructure)	Discrete Focus (Against Nuclear C2 or Specific Systems/Components)
	Machines/computers	Humans/operators
	Physical	Logical: internet/CNO
Method of Attack	Direct	Indirect
	Close proximity	From afar (remote)
Nature/Type	Inherent problems and vulnerabilities	Deliberate attacks
	Actual attacks	Perceptual (the fear that systems have been compromised)

As can be seen above, wherever nuclear weapons and cyber technology intersect, there is risk. In fact, there are challenges at every level of the cyber–nuclear nexus, and it therefore makes sense to consider the impact of cyber on nuclear weapons in their entirety, and across the three levels of the nuclear enterprise: the domestic nuclear weapons complex; state-based nuclear thinking and strategy; and the international system. Specifically, we need to consider single unit variables and nuclear C2 at the domestic level (missiles, warheads, specific computers, sensitive data, or early-warning systems), state level structures and national security thinking (about nuclear deterrence, strategy and nuclear posture), and international strategic relations and crisis management. While often discrete, these challenges are of course also interlinked – attacks on nuclear early-warning systems, for example, clearly have implications for crisis stability or notions of deterrence.

New Challenges and Vulnerabilities for Nuclear Weapons Management

Nuclear C2 systems have always been susceptible to outside interference, attack and possible sabotage, and the past is littered with miscalculations, accidents and near misses (many of which were caused by computers and electronic systems). This is primarily due to the central challenge of balancing two separate but co-constitutive nuclear requirements: the need for *positive control* (ensuring that weapons will work and can be used under all circumstances) and the need for *negative control* (ensuring that weapons are never used by accident or by unauthorised actors). As Peter Feaver explains:

> At the heart of nuclear command and control lies the always / never dilemma. Leaders want a high assurance that the weapons will always work when directed and a similar assurance the weapons will never be used in the absence of authorized direction. Weapons must be reliable: unlikely to fail at the moment when leaders want to use them; safe: unlikely to detonate accidentally; and secure: resistant to efforts by unauthorized people to detonate them.[16]

Despite many protective mechanisms (such as, among others, Permissive Actions Links, dual phenomenology, encryption, redundancy, and in some cases a 'two-man rule'[17]), this central problem of nuclear C2 means that weapons will never be invulnerable, and will always be susceptible to attackers (of any kind) seeking to undermine either positive or negative control. This is particularly the case during times of high tension, for systems that are tightly coupled and especially for states operating a posture of launch on warning (for more on this see Chapter III).[18] In this way, arguably the biggest factors in understanding the nature of the cyber challenge are the inherent vulnerabilities and tensions within nuclear systems themselves; both in terms of antagonistic pressures, and also an increasing reliance on computers and connectivity.[19] Thus cyber threats build upon, rather than fundamentally change, the complex and delicate nature of nuclear C2 (and the security of associated infrastructure).

There are two significant implications of this for nuclear weapons management and nuclear strategy: first, increasing complexity, particularly through computerisation and digitisation, raises the risk of normal accidents within the nuclear enterprise; and second, complex systems used to manage nuclear forces contain inherent vulnerabilities, weaknesses and bugs that might be exploited or manipulated in a variety of different ways by hackers.

16. Peter Feaver, 'Command and Control in Emerging Nuclear Nations', *International Security* (Vol. 17, No. 3, 1992), p. 163.
17. See, for example, Gerald Johnson, 'Safety, Security and Control of Nuclear Weapons' in Barry Blechman (ed.), *Technology and the Limitation of International Conflict* (Washington DC: Foreign Policy Institute, Johns Hopkins University, 1989), p. 145.
18. A 'tightly coupled' system is one where orders to launch can be made very soon after an attack is detected – a good example being 'launch on warning'.
19. The US is currently moving towards more 'internet like' systems for nuclear C2, and others are likely doing the same. See US Department of Defense, Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs, 'The Nuclear Matters Handbook', 2011, ch. 4.

The vulnerabilities and problems that are inherent within nuclear C2 systems are best demonstrated by the number of accidents, near misses and miscalculations that litter our nuclear past.[20] The 'normal accidents' theory posits that complex systems – particularly computer systems – will not always work as intended and will naturally go wrong some of the time,[21] and this is particularly the case with highly pressurised systems, those systems that can never be fully tested, or with systems that deal with hazardous technologies. In the words of Paul Bracken, 'In a world of experience we feel complex systems are bound to go awry precisely because they are so complex'.[22] There is perhaps no better example of a complex – or a tightly coupled and highly pressurised – system than those developed for nuclear C2, and it should be no surprise that there have been so many accidents and nuclear near misses in the atomic age. Indeed, there have probably been many more that we will never know about. As Ross Anderson points out:

> Despite the huge amounts of money invested in developing high-tech protection mechanisms, nuclear control and safety systems appear to suffer from just the same kind of design bugs, implementation blunders and careless operations as any others.[23]

Scott Sagan has even suggested that 'from a normal accidents perspective, the fact that there has never been an accidental nuclear weapons detonation or an accidental nuclear war is surprising'.[24] While not all previous nuclear accidents have involved computers and software – and many have simply involved human error – a significant number of incidents have involved computers and software, and this seems likely to increase as systems for nuclear weapons management become more complex, digitised and intricate. As Soviet physicist Boris Rauschenbach says, 'In terms of potential nuclear war, the very existence of mankind is becoming dependent on hardware and software'.[25]

Perhaps the most notable normal accidents in the nuclear realm occurred at the US North American Air/Aerospace Defense Command (NORAD[26]) between 1979 and 1984 (although

20. The best overviews of nuclear accidents and near misses are provided by Shaun Gregory, *The Hidden Cost of Nuclear Deterrence: Nuclear Weapons Accidents* (London: Brassey's, 1990) and Eric Schlosser, *Command and Control* (London: Allen Lane, 2013). See also Patricia Lewis et al., 'Too Close for Comfort: Cases of Near Nuclear Use and Options for Policy', *Chatham House Report* (April 2014).
21. Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (Princeton NJ: Princeton University Press, 1999).
22. Paul Bracken, 'Instabilities in the Control of Nuclear Forces' in Anatoly Gromyko and Martin Hellman (eds), *Breakthrough: Emerging New Thinking: Soviet and Western Scholars Issue a Challenge to Build a World Beyond War* (New York: Walker & Company Inc, 1988), p. 23.
23. Ross Anderson, *Security Engineering: a Guide to Building Dependable Distributed Systems* (Indianapolis IN: Wiley Publishing, 2008).
24. Scott Sagan, *The Limits of Safety: Organizations, Accidents and Nuclear Weapons* (Princeton NJ: Princeton University Press, 1993), p. 45.
25. Boris Raushenbach, *'*Computer War*',* in Gromyko and Hellman (eds), *Breakthrough*, p. 47. This is a theme examined in some detail by Peter Hayes in 'Nuclear Command-and-Control in the Millenials Era', *NAPSNet Special Reports*, Nautilus Institute for Security and Sustainability, 17 February 2015.
26. In 1981, NORAD was renamed, and Air Defense became Aerospace Defense.

there are likely to have been others that remain classified, or have not been recorded in the official files).[27] The first took place in October 1979 after computers at NORAD indicated that a missile had been launched from a submarine in the waters off the west coast of the US. A low-level state of nuclear war was declared and nuclear-armed missiles across the US went on alert. The attack warning was later discovered to have been caused by a technician accidentally loading a war game training tape simulating a Soviet nuclear attack onto the computer at the operations centre.[28]

In June 1980, a faulty computer processer twice caused false attack indications at NORAD after it began writing data into warning messages that indicated a massive nuclear attack.[29] In 1984, a computer malfunction indicated that a US nuclear-armed missile was about to fire.[30] More recently, in October 2010, the US Air Force lost contact with 50 intercontinental ballistic missiles (ICBMs) after a computer circuit card had been dislodged, and it is suggested that they could have been vulnerable to an unauthorised launch.[31] Data for other nuclear-armed states is very limited, but it should be assumed that similar accidents – perhaps due to computer problems – have taken place in other countries in the past as well.[32] This risk of accidents and other problems are only likely to grow as nuclear-armed actors come to rely more on computers and complex systems for nuclear weapons management.[33]

---

27. The rise of computer induced problems in military command networks can be traced back to the early 1960s. See Gordon Corera, *Intercept: The Secret History of Computers and Spies* (London: Weidenfeld and Nicholson, 2015), pp. 71–2; and James Anderson, 'Computer Security Technology Planning Study', ESD-TR-73-51, Electronic Systems Division, United States Air Force (October 1972), <http://csrc.nist.gov/publications/history/ande72.pdf>, accessed 24 June 2016. See also William Broad, 'Computer Security Worries Military Experts', *New York Times*, 25 September 1983. Eric Schlosser has noted that even as far back as the 1960s a series of major power surges could have accidentally launched up to 50 intercontinental ballistic missiles (ICBMs), see Eric Schlosser, 'Neglecting our Nukes', *Politico*, 16 September 2013.
28. William Broad, 'Computers and the Military Don't Mix', *Science* (Vol. 207, No. 14, 1980), p. 1183.
29. US General Accounting Office, 'NORAD's Missile Warning System: What Went Wrong?'(15 May 1981), <http://www.gao.gov/assets/140/133240.pdf>, p. 13, accessed 24 June 2016.
30. Gregory, *The Hidden Cost of Nuclear Deterrence,* p. 97.
31. Schlosser, 'Neglecting our Nukes'. Bruce Blair has warned that such events could raise the possibility of accidental or deliberate nuclear launch, possibly through cyber means, see Bruce Blair, 'Could Terrorists Launch America's Nuclear Missiles?', *TIME* (11 November 2010).
32. According to Eric Schlosser, 'I have no doubt that America's nuclear weapons are among the safest, most advanced, most secure against unauthorized use that have ever been built … other countries, with less hard-earned experience in the field, may not be so fortunate', see Schlosser, *Command and Control*, p. 481.
33. Christopher Stubbs suggests that, 'The most demanding quantitative risk assessment problems are those that have high consequences for failure that contain complex systems of systems with a combination of sophisticated hardware and software, and that include humans in short-time-scale critical decisions'. See Christopher Stubbs, 'The Interplay between Cultural and Military Nuclear Risk Assessment' in George Shultz and Sidney Drell (eds), *The Nuclear Enterprise: High Consequence Accidents: How to Enhance Safety and Minimize Risks in Nuclear Weapons and Reactors* (Stanford CA: Hoover Institution Press, 2012), p. 228.

Perhaps more importantly, they also provide an interesting insight into how systems might be hacked. As Peter Neumann notes, 'If an event can happen accidentally, it often could be caused intentionally.'[34] 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 authorising and firing the weapons – is also creating new ways in which nuclear systems might be exploited by hackers.[35] One of the biggest challenges here is the natural and inherent problems and bugs that are contained in increasingly sophisticated and complex software and coding – such as that used for nuclear C2. Generally speaking, complex systems – particularly computer-based systems – are likely to contain more bugs, problems and unforeseen errors than more basic analogue ones, especially those that rely on complex code, link multiple functions and hardware, and must make accurate computations quickly. As Martin Libicki explains:

> Unfortunately, complexity is bad for security. It creates more places for bugs to lurk, makes interactions among software components harder to understand, and increases the flow rate of packets well past where anyone can easily reconstruct what happened when things go wrong.[36]

These bugs are also the primary means that allow hackers to break into systems and circumvent their security mechanisms. Details of such inherent vulnerabilities – particularly 'zero-day exploits' (vulnerabilities that are yet to be discovered or patched) – can now be purchased on the black market.[37] Stuxnet, for example, is believed to have relied on five of these undiscovered vulnerabilities in order to penetrate and attack the enrichment plant at Natanz in Iran.[38] While this is clearly a fundamental threat to the highly sensitive components of nuclear C2 (such as the weapons, warning systems and communications), it also has significant implications for the wider nuclear weapons enterprise and particularly for the security of sensitive nuclear-related data and information (this is discussed in more detail in Chapter II).

While nuclear systems – and especially C2 – will of course be among the best protected against cyber threats and almost certainly air-gapped[39] from the wider internet, they are by no means invulnerable (see Chapter III). There is a real growing likelihood that hackers could initiate nuclear use, disable weapons and systems, indirectly 'spoof' warning sensors into believing an attack is underway, jam information flows or communications to prevent orders reaching the weapons, or access and utilise highly sensitive information about weapons systems and operational

34. Peter Neumann, *Computer Related Risks* (New York NY: Addison-Wesley Publishing Company, 1995), p. 126.
35. Or, as Martin Libicki has argued, 'The future of information systems' security has far more to do with the future of information systems vulnerabilities than with information weapons'. See Martin C Libicki, *Conquest in Cyberspace* (Cambridge University Press, 2007), p. 40.
36. *Ibid.*, pp. 293–4.
37. Andy Greenberg, 'Shopping for Zero-Days: a Price List for Hackers' Secret Software Exploits', *Forbes* (23 March 2013).
38. Liam O'Murchu, 'Stuxnet Using Three Additional Zero-Day Vulnerabilities', *Symantec Official Blog* (14 September 2010).
39. An air-gapped system is one that is physically isolated and separated from external and unsecured networks. The Natanz system in Iran was air-gapped from the internet.

procedures. This is the natural result of an increase in the number of vulnerabilities in nuclear-related software that could be exploited by a would-be attacker, both directly within nuclear C2 systems, and indirectly inside the various systems and infrastructure that supports nuclear weapons management. Of the two, the former – the increase in the number of vulnerabilities and ways in to operational software and the systems used for nuclear C2 – is clearly the more serious, although hacking into weapons software directly would probably be very difficult.[40]

For the purposes of this paper there are two types of cyber-attack (see Figure 4). *Disabling attacks* are when hackers seek to compromise or retard nuclear systems (by jamming communications or radar, sabotaging the weapons systems so they do not work or do not work as expected). *Enabling attacks* are when hackers seek to facilitate a launch or explosion (perhaps through spoofing systems into believing an attack is underway, or by hacking directly into launch control systems).

Figure 4: Enabling and Disabling Cyber Attacks

Enabling	Disabling
Directly hack into weapons and cause a launch or explosion.	Sabotage weapons and systems so they do not work or do not work as expected.
Send launch orders to weapons and commanders.	Disable communications and early-warning systems so that orders or launch commands cannot be received.
Spoof early-warning systems into believing an attack is underway.	Undermine nuclear systems through stealing information on how they work.

The threat to US nuclear security from disabling or enabling attacks is recognised by leading generals, even if the extent of the threat is unknown. For example, although former head of US Strategic Command General C Robert Kehler has remarked that he is confident that US C2 systems and nuclear weapons platforms 'do not have significant vulnerability' that cause him to be concerned,[41] he has also admitted, in a different interview, that 'we don't know what we don't know'.[42] Similar concerns about security have been raised by the UK government's choice of software for their Trident submarines. Their choice, known as 'Windows for Submarines', was strongly criticised by the software community, who viewed the decision not to purchase the more expensive Linux software as dangerous, and suggested that it could lead to losses in

40. Although, as is noted later in this paper, this is far from impossible. This threat is addressed in some detail by the Global Zero Commission on Nuclear Risk Reduction, 'De-alerting and Stabilizing the World's Nuclear Force Postures'.
41. Aliya Sternstein, 'Officials Worry About Vulnerability of Global Nuclear Stockpile to Cyber Attack', *Global Security Newswire* (14 March 2013).
42. Schlosser, 'Neglecting our Nukes'. According to Adam Segal of the Council on Foreign Relations, the US National Security Enterprise experiences up to ten million significant cyber-attacks every day: the majority of which are automated bots that are 'constantly scanning the Internet looking for vulnerabilities'. See Jason Koebler, 'US Nukes Face up to 10 Million Cyber Attacks Daily', *USNews* (20 March 2012).

security, reliability and assurance.[43] More broadly, software vulnerabilities also make it easier to hack into other nuclear-related systems and, in particular, make it easier to steal data, 'spoof' various systems with erroneous information, or potentially interfere, disrupt or damage critical nuclear facilities and processes.

While the cyber challenge varies across nuclear actors and systems, and the less sophisticated a system is, the less vulnerable it will be to cyber-attack,[44] it remains the case that, as Shaun Gregory notes, 'the requirement for military readiness will always mean that nuclear weapons will not be as safe as human ingenuity could make them'.[45] This is exacerbated by the fact that cyber is quickly becoming an important component of maintaining military readiness, especially as states seek to modernise their nuclear command structures and as reliance on computers and complex systems continues to grow.[46] As is explained in the next two chapters, these new challenges associated with cyber therefore have considerable implications right across the nuclear weapons enterprise, as well as for the global nuclear order more broadly.

43. Lewis Page, 'Royal Navy Completes Windows for Submarines Rollout', *The Register*, 16 December 2008. Interestingly, the US decided not to use Windows systems for its nuclear submarines and opted instead for Linux. See 'US Navy Rejects Windows for Linux', *Tech Khabaren*, 24 June 2012.
44. There is therefore arguably a case against modernising the software and computers used for C2 and nuclear weapons. As Peggy Morse, ICBM systems director at Boeing, puts it, 'while it's old it's very secure'. See John Reed, 'Keeping Nukes Safe from Cyber Attack', *Foreign Policy*, 21 September 2012.
45. Gregory, *The Hidden Cost of Nuclear Deterrence*, p. 47.
46. It should, however, be noted that the systems used for nuclear C2 vary across nuclear armed states. See Peter Hayes, 'Nuclear command-and-control in the Millenials Era'. See also Andrew Futter, 'The Double-Edged Sword'.

II. What Might Hackers Do to Nuclear Systems?

THERE ARE NUMEROUS scenarios in which hackers might seek to exploit or attack nuclear C2 and related systems. These vary markedly in terms of the actors involved, the seriousness of the threat and the possible ramifications of the attack. As explained in Chapter I, the cyber challenge is not homogenous. It must be dissected and placed in context, and the variances between attacks – and the motivations and intentions of different hackers – must be understood and differentiated.

By far the biggest challenge of the cyber age is the threat of espionage, and by extension the new measures that are required to protect sensitive nuclear information, such as weapons designs or operational procedures. The protection of such secrets has always been difficult, but new cyber capabilities are transforming and perhaps widening the scope of this task. A much smaller aspect of the challenge, but a far greater worry, is the possibility that hackers might in some way compromise nuclear systems, preventing them from working as intended, or precipitating some sort of crisis, even a launch, either directly or possibly indirectly by interfering with the data on which such systems rely. While the possible sabotage of nuclear systems has also always been a key challenge, the Farewell Dossier, Aurora Generator Test, Operation Orchard and, most recently, Stuxnet all demonstrate the possibility of interfering with, or damaging, nuclear systems through cyber means. The main aim of this chapter is to explain the different types of attack hackers might try to undertake against nuclear systems and the various types of threat posed by these actions.

Stealing Secrets: Spying, Hacking and Nuclear Espionage

The possibility that an adversary might steal nuclear secrets – be they weapon designs and capabilities or operational plans and procedures – has always been a major challenge for nuclear-armed states. Indeed, the importance of nuclear espionage can be traced as far back as the early 1940s as Soviet spies sought (and acquired) information on the Manhattan Project and early US nuclear bomb designs.[1] All aspects of nuclear spying and information security have remained a constant challenge ever since. However, the spread of computers, networks and digitally stored data has created new problems for nuclear secrecy and information security, and has changed, expanded and diversified the methods available for nuclear espionage. As PW Singer and Allan Friedman put it: 'while computer networks are allowing groups to work more efficiently and effectively than ever before, they are making it easier to steal secrets'.[2]

1. See, for example, Mike Rossiter, *The Spy Who Changed the World* (London: Headline, 2015).
2. Singer and Friedman, *Cybersecurity and Cyberwar*, p. 92.

The nature of the threat posed does not simply involve hacking into secret systems and downloading and copying information over the internet and from remote locations (although this is of course a key aspect of the problem), it also involves compromising the computer and information security in those systems that may already be air-gapped, or separated from the internet. Both issues are particularly acute because of the large amount of information that can be stored on computers and that can therefore also be stolen quickly and with (relatively) minimal effort. Rather than having to rely on copying by hand, taking photos, or risk removing documents, enormous amounts of information can now be downloaded or removed on a USB drive, a CD or in some other digital format.[3] When such attacks are carried out remotely over the internet, the risks to the spy/hacker are reduced even further so that no human agent needs to be placed in immediate danger.

Likewise, these new economies of scale also allow widespread 'hoovering' espionage attacks that attempt to steal as much information as possible about all types of things, as well as more targeted attacks on specific and specialised information. The very nature of hacking means that some secrets may be accessed for no purpose other than to prove that it can be done or just to monitor what a potential enemy may be doing.

The cyber-nuclear espionage age began in the mid-1980s as computers and networks gradually expanded throughout (particularly US) defence and military establishments.[4] It is often said to have been inaugurated by the 1986 'Cuckoo's Egg' episode, when a systems administrator, Clifford Stoll, discovered that a German hacker named Markus Hess had breached numerous research and military computers in the US in order to acquire information on nuclear weapons and the Strategic Defense Initiative (SDI).[5] It later transpired that Hess had been working for the Soviet KGB, who had been desperate to find out about SDI and the Reagan administration's nuclear plans.

Since then the volume and scope of cyber-nuclear espionage has expanded exponentially: in 1991 it was feared that a group of Dutch hackers who broke into US military networks were searching for nuclear secrets and missile data to sell to Iraqi leader Saddam Hussein prior to Operation Desert Storm.[6] In 1998, the Cox Report revealed that China had stolen a considerable cache of highly sensitive secrets over a number of years from the US, particularly those relating to the W88 thermonuclear warhead design.[7] Matthew McKinzie later remarked that it was

3. That said, paper could still sometimes be the easiest and least traceable method of stealing secrets.
4. The first cases of 'cyber espionage' can be traced back to an East German spy charged with espionage in 1968. See Michael Warner, 'Cybersecurity: a Pre-history', *Intelligence and National Security* (Vol. 27, No. 5, 2012), p. 784.
5. Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (London: Doubleday, 1989).
6. Dorothy Denning, *Information Warfare and Security* (Reading, MA: Addison-Wesley, 1999).
7. Select Committee US House of Representatives, 'Report of the Select Committee on US National Security and Military/Commercial Concerns with the Republic of China', 25 May 1999, Chapter 2, <https://www.gpo.gov/fdsys/pkg/GPO-CRPT-105hrpt851/html/ch2bod.html#anchor4311396>, accessed 23 June 2016.

an 'unprecedented act of espionage … The espionage in the Manhattan Project [would] pale in comparison.'[8] This became known as Kindred Spirit.[9] Later that year, an American teenage hacker broke into India's Bhabha Atomic Research Centre (BARC) and downloaded passwords and emails.[10] In 1999, the Moonlight Maze attack, believed to have emanated from Russia, was revealed to have stolen thousands of files and other pieces of sensitive information, and to have infiltrated deep into the Pentagon and other US government departments.[11]

This trend has continued and in fact deepened during the last decade. In 2005 hackers believed to be linked with China's People's Liberation Army (PLA) infiltrated numerous US military systems searching for nuclear secrets (among other defence information) in an operation dubbed Titan Rain.[12] In 2006 the Israeli secret service, Mossad, planted a Trojan in the computer of a senior Syrian government official which revealed the extent of the suspected Syrian nuclear weapons programme and led directly to Operation *Orchard* in 2007.[13] In 2008 an infected USB memory stick left in a car park led to Operation *Buckshot Yankee* after US classified networks were breached and the air-gap was jumped – the agent.btz malware was purportedly designed by Russia to steal military secrets and contained a beacon to allow mass data exfiltration.[14]

In recent years the cyber espionage threat has diversified to include all manner of nuclear-related systems. In February 2011, the Zeus was discovered, an information-stealing Trojan aimed at contractors involved in building the UK Trident nuclear-armed submarine force.[15] In May 2011, Iran was accused of hacking the International Atomic Energy Agency (IAEA), looking for secrets regarding the monitoring of its nuclear programme.[16] In August 2011, the Shady RAT malware targeted US government agencies, defence contractors and numerous high-technology companies.[17] In November 2012, the group Anonymous claimed to have hacked the IAEA and

8. Vernon Loeb and Walter Pincus, 'Los Alamos Security Breach Confirmed', *Washington Post*, 29 April 1999.
9. Dan Stober and Ian Hoffman, *A Convenient Spy: Wen Ho Lee and the Politics of Nuclear Espionage* (New York NY: Doubleday, 1989); Notra Trulock, *Code Name Kindred Spirit: Inside The Chinese Nuclear Espionage Scandal* (San Francisco CA: Encounter Books, 2002); Shirley Kan, 'China: Suspected Acquisition of U.S. Nuclear Weapon Secrets', *US Congressional Research Service*, RL30143, 1 February 2006.
10. Adam Penenberg, 'Hacking Bhabha', *Forbes*, 16 November 1998.
11. Adam Elkus, *'*Moonlight Maze*'* in Jason Healey (ed.), *'A Fierce Domain: Conflict in Cyberspace, 1986 to 2012'* (Cyber Conflict Studies Association, 2013), p. 155.
12. William Hagestad, *21st Century Chinese Cyberwarfare* (Ely, UK: IT Governance Publishing, 2010), p. 12.
13. Eric Follarth and Holger Stark, 'The Story of Operation Orchard: How Israel Destroyed Syria's Al Kibar Nuclear Reactor', *Spiegel Online*, 2 November 2009.
14. Karl Grindal, 'Operation Buckshot Yankee' in Healey (ed.), *A Fierce Domain*, p. 208.
15. Richard Norton-Taylor, 'Chinese Cyber-Spies Penetrate Foreign Office Computers', *The Guardian*, 4 February 2011.
16. David Crawford, 'UN Probes Iran Hacking of Inspectors', *Wall Street Journal*, 19 May 2011.
17. Hagestad, *21st Century Chinese Cyberwarfare,* p. 12.

threatened to release 'highly sensitive data' on the Israeli nuclear programme that they had allegedly seized.[18]

US nuclear laboratories and defence contractors have remained a primary target for at least the last decade,[19] and in 2013 hackers believed to be from the group Deep Panda (linked with the Chinese PLA) targeted the computers of US nuclear researchers directly.[20] Hackers have also sought to attack nuclear-related systems, perhaps most notably the US and Israeli ballistic missile defence (BMD) programmes, and are suspected of stealing important and secret data on these systems too.[21]

While many of the nuclear espionage attacks (that we know about) involve attacks on the US, Operation *Olympic Games* – the programme that would produce Stuxnet – began primarily as an intelligence-gathering and espionage operation against Iranian nuclear activities.[22] Similarly, both the Flame and Duqu cyber-attacks were designed to gain intelligence on systems and infrastructure – likely as a precursor to possible future physical attack or sabotage on the Iranian nuclear programme.[23] Indeed in 2012, an incident at the Iranian Fordo enrichment plant – where a suspected monitoring device, disguised as a rock, blew up – suggested that the US and Israel had continued to spy on the Iranian nuclear programme through cyber means.[24]

This list (see Figure 5) is by no means exhaustive, and it is highly likely that many more espionage and exploitation attacks have taken place. Moreover, as with banks and other financial institutions, national security organisations are extremely reluctant to reveal when they have been compromised or attacked, and are even more reluctant to share the details of these attacks. While this may be understandable, it is a major barrier to co-operatively addressing the challenge of cyber-nuclear espionage.

18. Michael Kelley, 'Anonymous Hacks Top Nuclear Watchdog Again to Force Investigation of Israel', *Business Insider*, 3 December 2012.
19. See, for example, US Government Accountability Office, 'Nuclear Security: Los Alamos National Laboratory Faces Challenges in Sustaining Physical and Cyber Security Improvements', 25 September 2008, <http://www.gao.gov/assets/130/121367.pdf>; or Aliya Sternstein, 'Attack on Energy Lab Computers Was Isolated, Officials Say', *Global Security Newswire*, 26 April 2011.
20. *Russia Today*, 'US Nuclear Weapons Researchers Targeted with Internet Explorer Virus', 7 May 2013.
21. *Global Security Newswire*, 'Chinese Hacking Targets US Missile Defense Designs', 28 May 2013; Debalina Ghoshal, 'China Hacking Iron Dome, Arrow Missile Defense Systems', *Gatestone Institute*, 5 August 2015; Andrew Futter, 'Hacking Missile Defense: The Cyber Challenge to BMD', *Missile Defense Review*, 1 March 2015.
22. Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York, NY: Crown Publishers, 2014), p. 321.
23. Chris Morton, 'Stuxnet, Flame and Duqu – the Olympic Games' in Healey (ed.), *A Fierce Domain,* pp. 219–21.
24. Uzi Mahnaimi, 'Fake Rock Spying Device Blows up Near Iranian Nuclear Site', *Sunday Times*, 23 September 2012.

Figure 5: Typology of Cyber-Nuclear Espionage Attacks by Intent

	Steal Sensitive Information	**Defend Against/ Combat Systems**	**Aid Proliferation**	**Precursor to Cyber Sabotage**
Cuckoo's Egg (1986)	✓	✓		
Dutch hackers (1990–1)		✓	✓	
Kindred Spirit (1995–8)		✓	✓	
BARC hack (1998)	✓			
Moonlight Maze (1999)	✓	✓		
Olympic Games, Flame & Duqu (2000s)				✓
Attacks on US defence contractors/nuclear labs (2000s–)	✓	✓		
Titan Rain (2005)	✓	✓		
Syrian nuclear programme (2007)				✓
Buckshot Yankee (2008)	✓	✓		
Attacks on US/Israeli BMD systems (2010s–)	✓	✓		
Iran hacks IAEA (2011)	✓			
Shady RAT (2011)	✓	✓		
Zeus Trojan (2011)	✓	✓		
Anonymous hacks IAEA (2012)	✓			

While the volume of cyber spying and the attempted theft of a wide variety of nuclear secrets has increased exponentially in recent years, the implications of cyber-enabled nuclear espionage are mixed, and the threat is far from homogenous. At the lower end of the scale, cyber-nuclear espionage is primarily about acquiring knowledge and intelligence on what a certain state is doing and the relative capabilities of key (weapons) programmes. Further up the scale, nuclear secrets may be targeted in order to help combat or defend against certain systems or to provide a better idea of operational procedures. A good example of this is the recent attempts to steal Israeli and US missile defence information (discussed above). Continuing up the scale, nuclear secrets might be stolen to aid proliferation – this was certainly the case with China and the US W88 warhead – and nuclear weapons designs could be traded on the nuclear black-market to states or non-state actors looking to acquire nuclear capabilities.[25] At the top end of the scale, these attacks are used as precursors to sabotage and physical destruction, and are designed principally to find out about nuclear systems and their vulnerabilities, map sensitive networks, implant logic bombs and ensure access to these systems in the future. Operation *Olympic Games* is the classic example of this, but it is feared that other attacks – notably Moonlight Maze – may have been designed with a similar purpose in mind. A big part of the problem, of course, is that it is very difficult to ascertain what exactly an attacker is trying to achieve, because attacks with different ends often look the same. Equally, espionage might escalate into sabotage without warning.

Could Nuclear Systems Be Sabotaged, 'Spoofed' or Compromised?

The cyber age and the computerisation of society has transformed the scope for sabotage of key systems, both in terms of critical national infrastructure and direct attacks against nuclear weapons and associated systems. In this way the challenge is divided into two different kinds of attacks. On the one hand, there are narrow and discrete attacks that are directed against nuclear forces and systems, such as in procurement, supply chain, early warning or the destruction of facilities. On the other, there are attacks that are not directed against nuclear weapons but that could affect nuclear thinking, such as a strategic attack against critical national infrastructure (the implications of this are considered in more detail in Chapter III). While nuclear weapons systems are certainly likely to be far better protected against sabotage and attack than commercial infrastructure, the threat is real and is manifest right across the nuclear weapons enterprise. As a US Defense Science Board report warned in 2013: 'US nuclear weapons may be vulnerable to highly sophisticated cyberattacks'.[26] Ultimately, this is also likely to be true for other nuclear-armed actors.[27]

The procurement of nuclear-related software and components and the need to update and replace key systems presents a serious challenge for the nuclear weapons complex. The main threat here

25. Catherine Collins and Douglas Frantz, 'Down the Nuclear Rabbit Hole', *Los Angeles Times*, 3 January 2011.
26. Timothy Farnsworth, 'Study Sees Cyber Risk for U.S. Arsenal', *Arms Control Today*, 2 April 2013.
27. Greg Austin and Pavel Sharikov have argued that Russia now sees cyber threats against its nuclear C2 as one of the greatest challenges at the strategic level. See Greg Austin and Pavel Sharikov, 'Preemption is Victory: Aggravated Nuclear Instability in the Information Age', *Nonproliferation Review* (forthcoming 2016).

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 do not work or at least do not work as expected; it could involve the introduction of malware or 'doctored' coding to change a process, or even the implanting of malware to allow access to the component in order to control, disrupt or destroy it in the future. As Ross Anderson suggests, 'the moral is that vulnerabilities can be inserted at any point in the tool chain, so you can't trust a system you didn't build yourself'.[28] That said, even protecting systems built 'in house' – as nuclear C2 systems almost certainly will have been[29] – is not straightforward, and some vulnerabilities may simply be the result of accidents, bugs or unanticipated circumstances (as discussed in Chapter I).

Sabotage has always been a principal nuclear risk, but the first known example of 'cyber-sabotage' can actually be traced back to the 1980s, when the CIA began an extensive operation to feed modified technical and computer-related equipment to the Soviet Union.[30] Under what became known as the 'Farewell Dossier', 'defective computer chips, flawed aerospace drawings, and rewritten software were all injected into an unsuspecting Soviet military-industrial complex',[31] 'contrived computer chips found their way into Soviet military equipment' and the 'Pentagon introduced misleading information pertinent to stealth aircraft, space defense and tactical aircraft'.[32] While the extent of the operation remains much disputed,[33] former Air Force Secretary Thomas Reed would later claim that the huge explosion of a Russian gas pipeline in 1982 was a direct result of the Farewell Dossier.[34]

More recently, and while the majority of attention has focused on Stuxnet, it is clear that a widespread sabotage campaign (including cyber) directed against the Iranian nuclear programme has been underway for well over a decade. According to Michael Adler:

> It seems to be clear that there is an active and imaginative sabotage program from several Western nations as well as Israel involving booby-trapping equipment which the Iranians are procuring, tricking black-market smugglers, cyber operations, and recruiting scientists.[35]

28. Anderson, *Security Engineering*, p. 645.
29. In confidential interviews with the author, several experts have expressed concern that some nuclear-armed states rely on certain hardware and software developed outside their national borders for weapons and C2.
30. One former senior government official told the author that Western attempts to undermine Soviet strategic systems through computer-based attacks were widespread as early as the 1980s, and many systems could have been compromised had it been ordered.
31. Thomas Reed and Danny Stillman, *The Nuclear Express: A Political History of the Bomb and Its Proliferation* (Minneapolis, MN: Zenith Press, 2009), p. 274.
32. Gus Weiss, 'Duping the Soviets: the Farewell Dossier', *Studies in Intelligence,* (Vol. 39, No. 5, 1996), p. 125.
33. See, for example, Anatoly Medetsky, 'KGB Veteran Denies CIA Caused 82 Blast', *Moscow Times*, 18 March 2004.
34. Thomas Reed, *At the Abyss: an Insider's History of the Cold War'* (New York, NY: Presidio Press, 2007).
35. Eli Lake, 'Operation Sabotage', *New Republic*, 14 July 2010.

In fact, during the 1990s the US and Israel 'modified' vacuum pumps purchased by Iran to make them break down;[36] in 2012, Iranian lawmaker Alaeddin Boroujerdi accused the German company Siemens of planting tiny explosives inside equipment that the Islamic Republic had purchased for its disputed nuclear programme;[37] in 2014, Iranian Foreign Minister Mohammed Javad Zarif blamed 'the West' for 'trying to sabotage the heavy water nuclear reactor at Arak by altering components of its cooling system';[38] and a huge explosion at the Parchin military base in October 2014 again raised the question of sabotage.[39] Similar techniques have also been used by various governments to bolster counter-proliferation efforts against certain states and terrorist groups seeking to acquire nuclear capabilities. As Eli Lake points out 'the specific benefit of [cyber] sabotage is that it makes countries [and terrorists] wary of purchasing crucial [nuclear-related] materials on the black market'.[40]

In addition to the direct threat of sabotage, the cyber challenge also involves attempts to attack, compromise or 'spoof' early-warning and communications systems, and therefore to undermine the information that nuclear decision-makers and nuclear systems rely upon. Attempts to 'jam' electronic communications or to deceive an adversary by providing false or misleading information have long been key components of warfare,[41] but the nature of this challenge is also changing in the cyber age. There is perhaps no better example of this than the alleged use of the Suter computer programme by Israel against Syrian air-defence radar in 2007 to allow Israeli jets to bomb a suspected nuclear site at al-Kibar. Instead of simply jamming radar signals, the Suter programme reportedly hacked into the Syrian air-defence system, allowing it to 'see what enemy sensors see and then to take over as systems administrator so sensors can be manipulated into positions so that approaching aircraft can't be seen'.[42] As a result, the non-stealthy F-15 and F-16 Israeli airplanes used in the attack remained undetected and were able to bypass the Syrian air defence system and bomb the suspected complex unhindered. It remains unclear exactly how the Suter system worked, but it is possible that code could have been beamed into the radar from above or the system could have been hacked or compromised electronically in another way prior to the attack.[43] The Syrian radar system was likely purchased from Russia and is currently being used by a number of other states – among them, reportedly, Iran.[44] While this attack was fairly limited, it nevertheless provides a stark warning of new types of vulnerability,

36. David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York NY: Broadway Paperbacks, 2013), p. 194.
37. *New York Times*, 'Iran Says Nuclear Equipment Was Sabotaged', 22 September 2012.
38. David Sanger, 'Explosion at Key Military Base in Iran Raises Questions About Sabotage', *New York Times*, 9 October 2014.
39. *Ibid.*
40. Eli Lake, 'Operation Sabotage'.
41. Electronic warfare and the use of the electromagnetic spectrum for operations remains a key part of the 'cyber' challenge. The use of dis- and misinformation is as old as warfare itself.
42. David Fulghum, 'Why Syria's Air Defenses Failed to Detect Israelis', *Aviation Week*, 12 November 2013.
43. Richard Clarke and Robert Knake, *Cyber War: the Next Threat to National Security and What to Do About It* (New York, NY: HarperCollins, 2010), pp. 6–8.
44. John Leyden, 'Israel Suspected of "Hacking" Syrian Air Defences: Did Algorithms Clear Path for Air Raid?', *The Register*, 4 October 2007.

particularly for key nuclear communications and early-warning systems.[45] While there are ways to protect and ensure against such attacks, nuclear communications and early-warning systems represent an obvious target in any future crisis, both for states and terrorist groups.[46] Likewise, the risk of 'spoofing' remains ever-present – for example, in July 2014 an Israeli military twitter account was hacked and an erroneous report published that the top-secret nuclear facility at Dimona had been attacked by rockets and had caused a 'radiation catastrophe'.[47]

The final set of cyber-sabotage challenges involves attacks intended to cause physical destruction and harm or that are designed to cause a nuclear explosion. While the 2007 Aurora Generator test demonstrated the possibilities of sabotage through cyber means,[48] there have only been a handful of cyber-attacks that have caused physical destruction and are publicly known,[49] and only one – Stuxnet – that has caused direct damage to a nuclear facility (although there are rumours that there have been US-led attacks on the North Korean nuclear programme too).[50] The Stuxnet worms were designed to attack the supervisory control and data acquisition control systems operating the centrifuges needed to enrich uranium, first by attacking the valves that manage the flow of uranium hexafluoride into the centrifuge, and later more directly by attacking the frequency converters themselves which regulate the speed of the device.[51] The thinking, according to one of the architects of the attack, speaking to David Sanger, 'was that the Iranians

45. Indeed, the Obama administration considered employing a cyber-offensive against both Syria in 2010 and Libya in 2011 prior to air-strike hostilities. According to Jim Michaels, the US worked on a number of cyber-attack capabilities to be used against Syrian air defence radar during the civil war: 'Electronic methods to disable enemy air defense systems include the injection of malware, a form of computer software, into the air defense network through a computer attack or by traditional electronic warfare aircraft capable of jamming radar. … The radars act like wireless transmitters and jammers can send false or destructive information to the radar, which then gets into the network'. See Jim Michaels, 'US Could Use Cyberattack on Syrian Air Defenses', *USA Today*, 16 May 2013. As Eric Schmitt and Thom Shanker point out: 'While the exact techniques under consideration remain classified, the goal would have been to break through the firewalls of the Libyan government's computer networks to sever military communications links and prevent the early warning radars from gathering information and relaying it to missile batteries aiming at NATO warplanes'. See Eric Schmitt and Thom Shanker, 'US Debated Cyberwarfare in Attack Plan on Libya', *New York Times*, 17 October 2011.
46. In fact, according to Jason Fritz, there is evidence that 'attempts have been made by hackers to compromise the extremely low radio frequency once used by the US Navy to send nuclear launch approval to submerged submarines'. See Fritz, 'Hacking Nuclear Command and Control'.
47. *Global Security Newswire*, 'Hacked Israeli Military Twitter Account Declared Nuclear Leak', 7 July 2014, <http://www.nti.org/gsn/article/hack-israeli-military-account-erroneous-post-announces-nuclear-leak/>, accessed 26 June 2016.
48. Jeanne Meserve, 'Sources: Staged Cyber-Attack Reveals Vulnerability in Power Grid', *CNN*, 26 September 2007.
49. The attacks on Saudi Aramco in August 2010 and a German steel mill in December 2014 are the best known. See Christopher Bronk and Eneken Tikk-Ringas, 'The Cyber Attack on Saudi Aramco', *Survival: Global Politics and Strategy* (Vol. 55, No. 2, 2013), pp. 81–96; and Kim Zetter, 'A Cyberattack Has Caused Confirmed Damage for the Second Time Ever', *Wired*, 8 January 2015.
50. Salvador Rodriguez, 'US Tried, Failed to Sabotage North Korea Nuclear Weapons Program with Stuxnet-Style Cyber Attack', *International Business Times*, 29 May 2015.
51. Zetter, *Countdown to Zero Day*, pp. 302–3.

would blame bad parts, or bad engineering, or just incompetence'.[52] The success of Stuxnet was dependent upon a considerable amount of prior monitoring and mapping of the system before any attack could take place, and this information was integral to its ability to work as planned. Moreover, it is believed that Stuxnet entered the air-gapped Natanz system through an infected USB drive, or another similar medium, and probably via an unwitting employee who had access to infection points.[53] Stuxnet has been credited with causing damage to centrifuges and delaying any Iranian bomb (albeit perhaps only temporarily),[54] and demonstrating that it is possible to infect and damage physical systems – often not connected to the internet – by hacking into the computers and networks that control them.

However, while Stuxnet represented a quantum leap in cyber capabilities and Operation *Orchard* demonstrated the vulnerabilities of early warning and communications, the direct threat of cyber-sabotage to the nuclear enterprise remains limited – at least for now. That said, recent events have shown that even systems thought not to be connected to the internet, as well as those vital for nuclear operations, could be compromised in a worst-case scenario, and the risk of indirect interference or interference from third parties, notably a terrorist group, remains a key challenge (as discussed in Chapter III). Therefore, it may be that older and less sophisticated systems and infrastructure used in nuclear C2 are safer and more secure against (cyber) sabotage and interference.[55] As General C Robert Kehler, former head of US Strategic Command, testified to Congress in March 2013:

> Much of the nuclear command and control system today is the legacy system that we've had. In some ways that helps us in terms of the cyber threat. In some cases it's point to point, hard-wired, which makes it very difficult for an external cyber threat to emerge.'[56]

Modernisation and added complexity of nuclear systems is therefore very much a double-edged sword: greater functionality, speed and processing power must be balanced against a higher possibility of vulnerabilities and the creation of new vectors for attack.[57]

52. Sanger, *Confront and Conceal*, p. 188.
53. Jon Lindsay, 'Stuxnet and the Limits of Cyber Warfare', *Security Studies* (Vol. 22, No. 3, 2013), p. 381. However, it is possible that this was achieved through a phishing attack, but no 'dropper' (a program designed to install the virus) has yet been found.
54. For a detailed discussion of this see David Albright, Paul Brannan and Christina Walrond, 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?', ISIS Report, Institute for Science and International Security, 22 December 2010.
55. In a confidential interview with the author, one former official commented that 'the UK nuclear firing chain is protected precisely because it is so outdated'.
56. US Senate Committee on Armed Services, 'Hearing To Receive Testimony on U.S. Strategic Command and U.S. Cyber Command in Review of The Defense Authorization Request For Fiscal Year 2014 and the Future Years Defense Program', 113th Congress, 12 March 2013.
57. Futter, 'The Double-Edged Sword'.

III. Implications for Strategic Stability, Crisis Management and Nuclear Strategy

THE VARIOUS DYNAMICS and challenges to nuclear security and command and control (C2) that are being driven, shaped and exacerbated by the growth of cyber threats will also have implications for strategic stability, nuclear strategy and crisis management. This is true on two levels. First, discrete and focused cyber-attacks against nuclear systems and associated infrastructure might have an impact on strategic stability and crisis management. In part this is due to the emergence of a cyber-nuclear security dilemma whereby the challenges described in the previous chapters must be factored into how future crises are managed and how unintended escalation (or nuclear use) can be avoided between nuclear-armed actors. Second, there is a much broader cyber threat against national and critical infrastructure and this raises new questions for national security and nuclear deterrence. While a policy of seeking to deter cyber-attacks through nuclear retaliation is (at least at the time of writing) at best disproportionate and inherently problematic, the fact that cyber will likely be used alongside – if not as a precursor to – conventional capabilities, and the fact that nuclear weapons remain the ultimate form of deterrence, means that they are and will remain linked.

This final chapter provides a discussion of how the various challenges described earlier *might* play out and become incorporated at the strategic level, both as a potentially destabilising dynamic between nuclear-armed actors, and in terms of national nuclear thinking and strategy.

Strategic Stability, Crisis Management and a New Cyber-Nuclear Security Dilemma

In the past decade, hackers and cyber-attacks have become an increasingly important and influential component of conflict, and while the nature and form that these attacks will take in the future remains unclear, it seems likely that this trend will continue and develop.[58] While cyber may be viewed by some as a separate domain from other forms of military power (at least theoretically), and especially with regard to nuclear weapons, in reality cyber cannot be decoupled from these other dynamics and it *will* therefore play a role in future nuclear-related decisions and strategic balances.

58. As the US Defense Science Board has pointed out, 'The [US] DOD should expect cyber attacks to be part of all conflicts in the future, and should not expect competitors to play by our version of the rules, but instead apply their rules (e.g. using surrogates for exploitation and offense operations, sharing IP with local industries for economic gain, etc.)'. US Department of Defense, Defense Science Board, 'Task Force Report', p. 5.

This increased role for cyber-attacks, either on their own or (more likely) in concert with the use of traditional kinetic military force, will probably alter the nature of conflict, strategic stability and particularly future crisis management between nuclear-armed actors. This will likely introduce a range of new destabilising factors to what is already a complicated and delicate endeavour. The threat of direct attacks on, or indirect interference with, nuclear systems, combined with the increased likelihood that cyber capabilities could lead to escalation in future crises, will undoubtedly have implications for the role and perceived utility of nuclear forces, strategic balances, perceptions and risks, as well as having potential force multiplier implications.

Bearing in mind what has been discussed earlier in this paper, and building on the list developed by Stephen Cimbala[59], we can identify several key areas where cyber-attacks may influence crisis stability between nuclear-armed actors. First, during a crisis hackers could potentially disrupt or destroy communications channels,[60] making it difficult to manage (nuclear) forces and reducing commanders' confidence in their systems. Indeed, according to PW Singer and Allan Friedman, 'only a relatively small percentage of attacks would have to be successful in order to plant seeds of doubt in any information coming from a computer'.[61] Attackers might also employ distributed denial of service attacks (DDoS) to prevent communication, hamper battle management systems and make it difficult to identify what is happening.[62]

Second, cyber-attacks can increase perceived time pressures to respond in kind, act pre-emptively, or take some other form of action. As Stephen Cimbala explains:

> A nuclear-armed state faced with a sudden burst of holes in its vital warning and response systems might, for example, press the preemption button instead of waiting to ride out the attack and retaliate.[63]

Third, the fear of cyber-disablement may reduce the search for viable alternatives to military action and create considerable problems for successful signalling, thereby compressing – or at least making unclear the various steps of – the 'escalation ladder', particularly the steps between

59. Stephen Cimbala, *Nuclear Weapons in the Information Age* (London: Continuum International Publishing, 2012), pp. 56–7.
60. As the Global Zero Commission on Nuclear Risk Reduction points out: 'At the brink of conflict, nuclear command and warning networks around the world may be besieged by electronic intruders whose onslaught degrades the coherence and rationality of nuclear decision making'. See Robert Burns, 'Former US Commander: Take Nuclear Missiles off High Alert', *Associated Press*, 29 April 2015.
61. Singer and Friedman, *Cybersecurity and Cyberwar,* p. 129.
62. According to Jason Fritz, 'A nuclear strike between India and Pakistan could be coordinated with Distributed Denial of Service attacks against key networks, so they would have further difficulty in identifying what happened'. See Fritz, 'Hacking Nuclear Command and Control'.
63. Cimbala, *Nuclear Weapons in the Information Age,* p. 206. Or as David Gompert and Martin Libicki have warned, 'In a situation where countries believe that they cannot afford to strike second, cyber-warfare options augment conventional first strike capabilities with the means to paralyse the enemy's forces at the outset, by either retarding their flow into the theatre of war or impairing their operation and facilitating their defeat once they arrive'. See David Gompert and Martin C Libicki, 'Cyber Warfare and Sino-American Crisis Instability', *Survival: Global Politics and Strategy* (Vol. 56, No. 4, 2014), pp. 11–12.

conventional and nuclear use. Fourth, cyber-attacks may lead to flawed perceptions of enemy intentions and capabilities, or 'spoof' early-warning systems. This is a particular concern given the possibility of 'false flag' cyber interference by third parties: that is, conducting operations so that they appear to have been carried out by another actor. Lastly, the use of cyber-attacks may also exacerbate concerns over strategic surprise.[1] Indeed, it is not inconceivable to see this as the beginning of a possible transition to a condition of mutually unassured destruction (MUD): a context where states may no longer feel that they will always be able to threaten nuclear retaliation to deter nuclear attack.[2]

Taken together, these dynamics raise the likelihood of (unintended) and potentially uncontrollable escalation and make the management of nuclear crises more complicated and dangerous.[3] In fact, an Israeli war game held in 2013 showed how a regional conflict involving cyber-attacks could very quickly escalate, in this case bringing the US and Russia to the brink of war.[4] Haim Assa, the designer of the game, later remarked: 'What we all learned was how quickly localized cyber events can turn dangerously kinetic when leaders are ill-prepared to deal in the cyber domain'.[5] The basic point is that we should be concerned that nuclear weapons might be used due to miscalculation or as a result of interference from third-party actors.[6]

Perhaps the most likely future cyber-nuclear dilemma is between the US and China in the Asia-Pacific, where both nations have been pretty open and transparent about the importance of cyber capabilities and attacks on information systems.[7] As Gompert and Libicki explain, both China and the US 'have recognised that an armed conflict with the other would include cyber warfare'.[8] The US Air-Sea battleplan 'makes no bones about conducting cyber warfare against Chinese kill-chain networks in the event of a conflict'.[9] While at the same time,

> Many analysts now believe that the PLA has already acquired, through its development of strong cyberwarfare capabilities, the means to asymmetrically challenge the United States in the event of a kinetic conflict between the two states.[10]

1. According to one senior former British government official, 'the ability to clearly signal intentions could be one of the biggest challenges created by cyber for nuclear crisis management'. Confidential interview with the author.
2. Richard J Danzig, 'Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies,' Center for a New American Security, July 2014, p. 6.
3. Cimbala, *Nuclear Weapons in the Information Age,* p. 205.
4. Barbara Opall-Rome, 'Israeli Cyber Game Drags US, Russia to Brink of Mideast War', *Defense News*, 14 November 2013.
5. *Ibid.*
6. Blair, 'Could Terrorists Launch America's Nuclear Missiles?'.
7. See, for example, US Department of Defense, 'The Department of Defense Cyber Strategy', April 2015.
8. Gompert and Libicki, 'Cyber Warfare and Sino-American Crisis Instability', p. 10.
9. *Ibid.*, p. 16.
10. George Patterson Manson, 'Cyberwar: The United States and China Prepare For The Next Generation of Conflict', *Comparative Strategy* (Vol. 30, No. 2, 2011), p. 122. Moreover, as Gompert and Libicki point out, 'The Chinese know that computer networks are critical to US capabilities and

The primary concern here is that a low-key conventional conflict or skirmish 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 (at least in part) through cyber means. This is a particular concern given the fact that China is thought to share some parts of its C2 system for both nuclear and conventional forces.[11] This risk is, in turn, likely to have implications for China's 'No First Use' nuclear posture, particularly when cyber is combined with US ballistic missile defence plans and conventional global strike capabilities.[12] In fact, the nature of a possible US–China conflict involving the use of cyber-attacks has already been explored in the futuristic novel *Ghost Fleet* – although in this scenario nuclear systems were not attacked.[13]

The second potential cyber-nuclear security dilemma is likely to be between the US, its NATO allies and Russia, especially given their recent and very conspicuous use of cyber capabilities.[14] In fact, as part of the Wales summit in September 2014, and almost certainly in part as a response to Russian activities in Ukraine, NATO made it clear that cyber-attacks were a major challenge and concern for the Alliance. As Sidney Freedberg explains,

> NATO is now taking cyber threats as seriously as the Russian tanks and nuclear weapons it was created to deter… [it declared that] the alliance's hallowed Article 5 – which says an attack on one member is an attack against all – applies equally to virtual attacks as to physical ones.[15]

A few months later, in November 2014, NATO held its largest ever cyber war game just outside the city of Tartu in Estonia. As Sam Jones commented, 'In reality, the scenario was a thinly disguised version of the threats confronting the alliance as a result of the crisis in Ukraine. Russia, though never mentioned, loomed large'.[16] While it remains unclear at what threshold collective defense will be triggered, and how this threshold will be measured,[17] current NATO thinking appears to suggest, according to Warwick Ashford, 'that some cyber attacks could have the same level of disruption on Nato countries and economies as conventional warfare'.[18] Indeed in June 2016, NATO Secretary General Jens Stoltenberg announced that a major cyber-

---

strategy in the Western Pacific, and that targeting them could have decisive effects on a conflict'. See Gompert and Libicki, 'Cyber Warfare and Sino-American Crisis Instability', p. 16.

11. Joshua Pollack, 'Emerging Strategic Dilemmas in U.S.-China Relations,' *Bulletin of the Atomic Scientists* (Vol. 65, No. 4, 2009), p. 56. Under modernisation plans, to be completed in 2020, it is likely that the US will also share parts of its C2 infrastructure between nuclear and conventional weapons systems, see Futter, 'The Double-Edged Sword'.
12. Taylor Fravel and Evan Medeiros, 'China's Search for Assured Retaliation: the Evolution of Chinese Nuclear Strategy and Force Structure', *International Security* (Vol. 35, No. 2, 2010), pp. 48–87.
13. PW Singer and August Cole, *Ghost Fleet: a Novel of the Next World War* (Boston MA: Houghton Mifflin Harcourt, 2015).
14. Stephen Cimbala and Roger McDermott, 'A New Cold War? Missile Defenses, Nuclear Arms Reductions, and Cyber War', *Comparative Strategy* (Vol. 34, No. 1, 2015), pp. 95–111.
15. Sidney J Freedberg Jr, 'NATO Hews to Strategic Ambiguity on Cyber Deterrence', *Breaking Defense*, 7 November 2014.
16. Sam Jones, 'NATO Holds Largest Cyber War Games', *Financial Times*, 20 November 2014.
17. Freedberg, 'NATO Hews to Strategic Ambiguity on Cyber Deterrence'.
18. Warwick Ashford, 'NATO to Adopt New Cyber Defence Policy', *ComputerWeekly.com*, 3 September 2014.

attack could trigger an Article V collective response.[19] It is important to remember that NATO deterrence thinking – and for that matter, Russian thinking too – remains anchored by nuclear weapons, and that a significant number of these weapons remain on high alert.[20]

While the threat of (unintended) escalation driven by cyber is also clearly an important aspect of the East–West strategic balance, the direct and indirect cyber threat to US and Russian nuclear forces is also particularly pressing. These challenges include either attacks designed to neuter, interfere with or compromise nuclear C2 systems so that they do not work properly or do not work as expected (likely perpetrated either by the US or Russia), or attacks by third parties (for example terrorist groups) 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 retained by both parties, and particularly by the several hundred intercontinental ballistic missiles (ICBMs) that both sides keep on high alert. As Franz-Stefan Gady explains:

> First, sophisticated attackers from cyberspace could spoof U.S. or Russian early warning networks into reporting that nuclear missiles have been launched, which would demand immediate retaliatory strikes according to both nations' nuclear warfare doctrines. Second, online hackers could manipulate communication systems into issuing unauthorized launch orders to missile crews. Third, and last, attackers could directly hack into missile command and control systems launching the weapon … (a highly unlikely scenario).[21]

These challenges would become magnified considerably during a possible future crisis. Somewhat paradoxically, these new cyber-enabled threats also make nuclear arms control and possible reductions between the US and Russia less rather than more likely.[22]

While the increasing importance of cyber dynamics in these strategic nuclear relationships does not necessarily mean that the next crisis will become unmanageable and lead directly to disaster, clearly it will make a safe and peaceful resolution harder to achieve. As current US Secretary of Defense Ashton Carter previously pointed out, 'one must face the fact that specific instances of error and uncertainty almost always look improbable and absurd, which tends to discredit them as subjects for serious study'.[23] Moreover, with many nuclear systems remaining on high alert, the possibility of accidents or miscalculation resulting from cyber-enabled disinformation, outsider interference, or a perceived pressure to act will remain a significant challenge.[24]

---

19. Andrea Shalal, 'Massive Cyber Attack Could Trigger NATO Response: Stoltenberg', *Reuters*, 16 June 2016.
20. For a discussion of the problems of cyber during US–Russian crises, see Andrew Futter, 'Cyber Threats and the Challenge of De-Alerting US and Russian Nuclear Forces', *Nautilus Institute NAPSANet Policy Forum*, 15 June 2015.
21. Franz-Stefan Gady, 'Could Cyber Attacks Lead to Nuclear War?', *The Diplomat*, 4 May 2015.
22. Futter, '*War Games* Redux?'.
23. Ashton B Carter, 'Sources of Error and Uncertainty' in Ashton B Carter, John D Steinbruner and Charles A Zraket (eds), *Managing Nuclear Operations* (Washington DC: Brookings Institution Press, 1987), p. 612.
24. Futter, '*War Games* Redux?'.

Nuclear Strategy and Cyber Deterrence

In addition to the new challenges for international stability and crisis management, the threat of a broad-based cyber-attack and the proliferation of cyber-attack capabilities have also necessarily created a range of new pressures for national security policy and the role of nuclear weapons, specifically for defence, deterrence and possible retaliation. Formulating a credible and workable way to respond to the cyber challenge has, however, been far from easy, and this has been greatly complicated by the considerable differences between nuclear weapons and cyber threats, the problems and limitations of cyber defence and arms control, the likely need for some type of cross-domain deterrence/retaliation strategy (that may or may not include nuclear weapons), the inherent difficulties of attribution, and perhaps above all the uncertainty of the nature and extent of any future cyber threat or attack. These dynamics make formulating a credible national nuclear-cyber strategy difficult and problematic.

The rise of the cyber challenge has necessarily led to comparisons with nuclear weapons, but the two are profoundly different, and putting them in the same conceptual bracket is largely unhelpful. While there are some similarities (for example, offence appears to trump defence[25] and both often involve 'delivery vehicles' and 'payloads'), there are at least four main differences between cyber and nuclear weapons: first, the scale and nature of the threat in terms of physical destruction and long-term effects; second, the types of targets to be attacked; third, the types of actors involved; and fourth, the rules and conventions which govern their use.

In terms of the scale and nature of the threat, even the most sophisticated cyber-attacks are highly unlikely to cause the enormous physical destruction, damage and death that just one nuclear bomb can and has done,[26] and it is difficult to think of cyber weapons as being of strategic importance or, for that matter, as being the sole or primary means of waging war (of course this remains subject to debate, and the situation could change in the future).[27] As Libicki puts it, 'Nuclear war creates firestorms, destroying people and things for miles around. By contrast even a successful widespread information attack has more the character of a snowstorm'.[28] Part of the reason for this is that the intended targets of cyber and nuclear attacks tend to be different. While it is (theoretically) possible to have limited or focused nuclear attacks, nuclear weapons are generally seen as indiscriminate and intended to cause widespread damage to large urban areas. In contrast, the most threatening cyber-attacks are likely to be highly specialised and target very specific systems or machines – in fact, they often require knowledge of the target beforehand to be effective (notwithstanding distributed denial of service (DDoS) attacks which are often indiscriminate).[29]

25. Erik Gartzke and Jon R Lindsay, 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace', *Security Studies* (Vol. 24, No. 2, 2015), pp. 216–348.
26. Approximately 200,000 people died as a result of the two atomic bombs dropped on Hiroshima and Nagasaki in 1945. So far no-one has died as a direct result of a cyber-attack.
27. For example, Thomas Rid and Peter McBurney have suggested that 'an act of war must be instrumental, political and potentially lethal, whether in cyberspace or not. No standalone cyber offense on record meets these criteria, so a 'cyberwar' remains a metaphor for the time being'. See Rid and McBurney, 'Cyber-weapons', p. 7.
28. Libicki, *Conquest in Cyberspace*, p. 39.
29. Such DDoS cyber-attacks were directed against Estonia in 2007, Georgia in 2008, and purportedly by Iran against US banks in 2013. As Dale Peterson explains, 'An organization wanting to attack a

Nuclear weapons have also traditionally been the preserve of nation states and the main actors in the nuclear game have been national governments, which is partly due to the enormous cost and undertaking involved in producing, managing and fielding nuclear weapons. This has meant that it has been pretty clear where the threat has come from and who has been ultimately responsible for any attack. While sophisticated cyber-attacks are probably also likely to be state sponsored, the range of actors is multifaceted and it has become far less clear how to attribute who is ultimately responsible for these attacks.

Finally, the rules and conventions which have governed the use and role of nuclear weapons are difficult to apply to the realm of cyber – the notions of mutually assured destruction (MAD), cyber arms control and cyber deterrence in particular are inherently complicated, and there is no established tradition of cyber non-use or taboo.[30] In fact, cyber-attacks, in one form or another, are underway pretty much all of the time.[31] The net result is that using nuclear as a model for cyber is flawed; although some have suggested that biological or chemical weapons might provide a better comparison.[32]

While the cyber challenge may be intrinsically different from that posed by nuclear weapons, it nonetheless requires concerted thinking about how to defend, deter and potentially respond to cyber-attacks in all their different guises. But this is unlikely to be straightforward. As former US Deputy Secretary of Defense William Lynn has argued 'traditional Cold War deterrence models of assured retaliation do not apply in cyber space … deterrence will necessarily be based more on denying any benefit to attackers than on imposing costs through retaliation'.[33] But cyber-security and defence, and the broader notion of deterrence by denial, is far from a panacea – even for supposedly air-gapped, highly redundant and well-protected systems. Likewise, the concept of cyber arms control may be too problematic for anything meaningful to be agreed. As Paul Meyer explains:

> The lack of defined strategies, transparency of operations and verification capacity, as well as the inherent length of the treaty-making and adoption process, render legally based arms control problematic for addressing cyber-security threats.[34]

As a result, a significant component of any strategy to engage the cyber threat will probably need to be deterrence by punishment and through the threat of retaliation. However, deterring cyber-attacks through the threat of punishment raises other significant questions and complications,

---

potential adversary's critical infrastructure must first learn what system that adversary has'. Dale Peterson, 'Offensive Cyber Weapons: Construction, Development and Employment', *Journal of Strategic Studies* (Vol. 36, No. 1, 2013), p. 121.

30. Paul Meyer, 'Cyber-Security through Arms Control: an Approach to International Cooperation', *RUSI Journal* (Vol. 156, No. 2, April 2011), pp. 22–7.
31. Andrew Krepinevich, 'Cyber Warfare: a "Nuclear Option"?', (Washington DC: Center for Strategic and Budgetary Assessments, August 2012), p. iii.
32. Andres and Winterfeld, *Cyber Warfare*, p. 8; David Fidler, 'The Relationship between the Biological Weapons Convention and Cybersecurity', *Council on Foreign Relations Net Politics Blog*, 26 March 2015.
33. William J Lynn III, 'Defending a New Domain: the Pentagon's Cyberstrategy', *Foreign Affairs* (Vol. 89, No. 5, 2010), pp. 99–100.
34. Meyer, 'Cyber-Security Through Arms Control', p. 22.

perhaps most importantly whether attacks can be attributed with enough confidence to elicit a response,[35] and what form this response might take if it is to be credible, proportional, legal and viable.[36]

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 too.[37] 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, ranging from hacking, nuisance and exploitation to those that cause damage, disruption or destruction. As Richard Kugler explains, 'A one-size fits all approach to deterrence will not work because of the multiplicity and diversity of potential adversaries and cyber attacks'.[38]

As deterrence of cyber-attacks must be tailored to the specific types of threat and attack and must also be proportional to them, there are a number of different options available.[39] We should also bear in mind 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. As Siobhan Graham and Julian Barnes explain:

> If a cyber attack leads to the death, damage, destruction or high-level of disruption that a traditional military attack would cause, then it would be the candidate for a "use of force" consideration.[40]

Or in the words of one US military official, 'If you shut down our power grid, maybe we will put a missile down one of your smokestacks'.[41] Such thinking necessarily leads to a consideration

35. In a simulated cyber-attack in 2010 'no one could pinpoint the country from which the attack came, so there was no effective way to deter further damage by threatening retaliation'. See John Markoff, David E Sanger and Thom Shanker, 'In Digital Combat, US Finds No Easy Deterrent', *New York Times*, 25 January 2010 and Thomas Rid and Ben Buchanon, 'Attributing Cyber Attacks', *Journal of Strategic Studies* (Vol. 38, No. 1–2, 2015), pp. 4–37.
36. For an interesting discussion of the possibilities of cyber deterrence, see Jason Rivera, 'Achieving Cyberdeterrence and the Ability of Small States to Hold Large States at Risk' in M Maybaum, A-M Osula and L Lindstrom (eds), *Architectures in Cyberspace: 7th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE Publications, 2015).
37. Franklin Kramer, 'Cyberpower and National Security: Policy Recommendations for a Strategic Framework', in Kramer, Starr and Wentz (eds), *Cyberpower and National Security*, p. 15.
38. Richard Kugler, 'Deterrence of Cyber Attacks', in Kramer, Starr and Wentz, *Cyberpower and National Security*, p. 310.
39. It is thought that the US responded to the hacking of Sony pictures in late 2014 – believed to be by North Korea – by launching an 'equivalent' response. As Nicole Perlroth and David Sanger explain, 'While perhaps a coincidence, the failure of the country's computer connections began only hours after President Obama declared Friday that the United States would launch a 'proportional response' to what he termed an act of 'cybervandalism' against Sony Pictures'. See Nicole Perlroth and David E Sanger, 'North Korea Loses its Link to the Internet', *New York Times*, 22 December 2014. That said, the identity of the perpetrators of the attack remains a matter of debate, see Kim Zetter, 'The Evidence that North Korea Hacked Sony is Flimsy', *Wired*, 17 December 2014.
40. Siobhan Gorman and Julian E Barnes, 'Cyber Combat: Act of War', *Wall Street Journal*, 31 May 2011.
41. *Ibid*.

of whether there might be any role for nuclear weapons in 'anchoring' the deterrence ladder. However, this strategy would also lead, in the event of a cyber-attack, to a potential existential threat. As the 2013 US Defense Science Board argued:

> There is no silver bullet that will reduce DoD cyber risk to zero. While the problem cannot be eliminated, it can and must be determinedly managed through the combination of deterrence and improved cyber defense. Deterrence is achieved with offensive cyber, some protected-conventional capabilities, and anchored with U.S. nuclear weapons.[42]

Indeed, Martin Libicki points out that 'for a while it was Russian policy to react to strategic cyber-attack with the choice of any strategic weapons in its arsenal'[43] and the US International Strategy for Cyberspace has declared that it 'reserve[s] the right to use all necessary means – diplomatic, informational, military and economic – as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests'.[44]

There is certainly some logic in including nuclear forces as part of a cross-domain cyber-deterrence strategy – especially given the problems of cyber-defence. As Elbridge Colby explains,

> if China or Russia knows that we would never consider using nuclear weapons in response to even a massive cyber attack, then that gives them a strong incentive to try to exploit that advantage – even implicitly – by using cyber as a way to deter and even coerce the United States and our allies.[45]

Yet the majority of analysis has questioned the logic of commingling nuclear and cyber weapons. Timothy Farnsworth, for example, has pointed to a number of problems with using nuclear weapons to deter cyber: first, cyber-attacks lack the destructive and existential threat of nuclear weapons, meaning that a nuclear response to a cyber-attack is not proportional; second, threatening to respond to a cyber-attack with nuclear weapons lacks credibility in adversaries' eyes; third, cyber-deterrence in general is difficult to achieve; and finally, the policy would provide a new rationale for nuclear proliferators.[46] Former US governmental officials Steven Andreasen and Richard Clarke remark that 'it's hard to see how this cyber-nuclear action-reaction dynamic would improve U.S. or global security'.[47]

Given the existing nature of the cyber threat, it is probably fair to say that nuclear weapons are not currently a good option for addressing and deterring cyber challenges – and linking the

42. US Department of Defense, Defense Science Board, 'Task Force Report', p. 15.
43. Martin C Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica CA: RAND Corporation, 2009), p. 69.
44. Office of the President of the US, 'International Strategy for Cyberspace: Prosperity, Security and Opennesss in a Networked World' (May 2011).
45. Elbridge Colby, 'Cyberwar and the Nuclear Option', *National Interest*, 24 June 2013.
46. Timothy Farnsworth, 'Is There a Place for Nuclear Deterrence in Cyberspace?', *Arms Control Now*, 30 May 2013. Farnsworth also comments, 'the threat of nuclear retaliation to a major cyber attack is neither proportional, nor credible, in stopping (deterring) high-level catastrophic cyber attacks against a nation's critical infrastructure by other states, including the nuclear weapons complexes'.
47. Steven Andreasen and Richard A Clarke, 'Cyberwar's Threat Does Not Justify a New Policy of Nuclear Deterrence', *Washington Post*, 14 June 2013.

two domains would appear to offer few benefits and numerous problems, at least conceptually. However, in reality they are of course intrinsically linked, and should the nature of the cyber threat change and evolve – which it arguably will – then it is certainly not impossible that nuclear weapons could have a role to play in the future.[48]

48. In a confidential interview with the author, a former senior UK official remarked, 'Nukes have a limited role in deterring that form of asymmetric warfare, but never say never, if nukes were a proportionate response to a verified, attributed cyber assault'.

Conclusion: New Challenges for Old Dynamics

IN THE NEAR future, cyber will neither supersede nuclear weapons as the ultimate guarantor of national security nor represent a strategic or existential threat. To believe so would be to misunderstand both the nature and scope of the challenge posed by cyber, as well as the fundamental differences between cyber-attacks and nuclear weapons. But the developing relationship between cyber and nuclear technologies certainly represents an important shift in the context in which we think about nuclear weapons and nuclear security, manage nuclear relationships and strategic stability, and regulate the global nuclear order. If we understand cyber as a holistic concept that includes not just the internet, but also the software, hardware, other infrastructure and people that operate and interact with these systems, then the challenge to nuclear weapons in the cyber age is in fact multifaceted.

This challenge is more nuanced in some cases than in others. But in general it both exacerbates and transforms established nuclear tensions, problems and challenges. Indeed, the cyber challenge builds upon the existing challenges that have always been part of nuclear weapons management, especially the antagonistic demands of positive and negative nuclear command and control (C2), the protection of sensitive information, and the ability to guard against outside interference. Cyber is essentially presenting new ways into these systems, and new opportunities to interfere with their functioning, rather than shifting the basic tenets of nuclear weapons management. Nevertheless, the emergence and spread of cyber-interference and -attack capabilities is changing, recasting and exacerbating existing tensions right across the nuclear weapons enterprise, and providing new dynamics and challenges that must be understood and addressed.

The cyber threat to nuclear weapons is not homogenous, and systems and associated infrastructure are vulnerable in different ways (and this varies for different systems and actors too). Importantly, it is not just the danger of hacking directly into a weapons system over the internet and causing a launch or detonation that should be the main focus – although this remains a possibility. Instead, the overwhelming majority of attacks on nuclear-related systems are simply hacking or espionage, and while these clearly do have implications for the credibility or efficacy of weapons systems, proliferation and possible future sabotage (as discussed in Chapter II), we should be clear about the nature of this challenge.

Only a handful of cyber-attacks have successfully caused major disruption and damage, most notably Stuxnet, although the potential for this number to increase in the future is obvious. In this way, the most likely implication of the cyber challenge is that weapons will be compromised due to espionage. More worrying is that systems might be sabotaged or compromised, and

the least likely but worst-case scenario is that attacks could somehow facilitate a nuclear launch or explosion.

It is equally important to understand that the nature of the cyber threat to nuclear weapons varies between nation states and terrorists and between *enabling* and *disabling* attacks. The main goal of a nation-on-nation cyber-attack (aside from espionage) is likely to be to disable an opponent's nuclear forces or C2, or at least erode confidence that these systems will work. Hopefully, no rational actor is likely to take this risk unless the situation is already dire. Terrorists or other third parties are more likely to seek to use cyber as a means to precipitate a crisis and/or facilitate miscalculation and possible nuclear use. Cyber-attacks may also be used alongside other military domains, especially if the goal is sabotage or major interference. As such, they are likely to act as a force multiplier. The balance between the threat of enabling versus disabling attacks is therefore a fundamental part of the emerging cyber–nuclear security dilemma, and of the possibility that cyber could escalate towards nuclear use (either through outside interference or miscalculation). Finally, and in addition to discrete and focused attacks on nuclear weapons systems, widespread attacks against society and critical infrastructure also have implications for nuclear weapons, and particularly for the question of whether nuclear weapons can or should play a role in deterring such attacks. While nuclear retaliation may not currently represent a particularly credible or proportionate response to cyber-attack, the two domains are intrinsically linked, and this could become more important in the future.

As well as creating numerous new challenges for nuclear C2 and associated infrastructure, cyber threats will also have a variety of knock-on implications on a much larger scale. First, the possibility (and even the perception) that nuclear systems might be compromised or attacked, and therefore not work as intended, seems likely to hinder the push for global nuclear reductions.[1] It may be cited as a strong reason for nuclear modernisation, sophistication and diversity by nuclear-armed states. As such, it seems likely that cyber will affect both current (bilateral) arms control agreements and broader global nuclear regimes (notably the Nonproliferation Treaty – NPT), and provide another barrier to further nuclear cuts and the ultimate goal of disarmament. In fact, the various challenges and threats of cyber-attack may need to be included as part of future nuclear dialogue and strategic discussions.

Perhaps more troubling is the fact that this may also create incentives to retain nuclear forces on high levels of alert – especially when cyber is combined with other potentially destabilising dynamics such as missile defence and prompt strike capabilities, which taken together could constitute a serious threat to assured retaliation or be viewed as a first-strike capability. As has been explained above, such moves are likely to undermine strategic stability and greatly enhance the likelihood of interference by third parties (such as terrorists), leading to an increased chance of miscalculation and possibly even nuclear use. Ultimately, while the implications are of course different for different actors, and much depends on the posture and requirements

1. While it is certainly true that for many analysts and anti-nuclear campaigners cyber threats have made the need for nuclear disarmament more urgent, evidence suggests that the opposite view is being taken by the nuclear armed states. See, for example, Futter, '*War Games* Redux'.

placed on nuclear forces by individual states, these new dynamics together clearly do represent a challenge to the nuclear orthodoxy.

There are no easy fixes to mitigate these various new challenges, but there are some options that could be considered and pursued to help minimise the impact and risks of cyber for nuclear weapons. A potentially propitious starting point is a need to properly understand the nature of the challenge (and come to agreement on what the term means) and how new cyber dynamics might play out. It is too easy to misunderstand the cyber challenge, either by focusing too narrowly or too broadly, and doing so makes it harder to formulate methods and mechanisms of protection or a productive way forward. Cyber threats vary markedly and it is important to be clear about exactly what is at stake and about what its implications are, especially as states seek to modernise their nuclear infrastructure.[2] In doing this it might become easier to establish certain norms or rules of the road in the nuclear-cyber domain, and to pursue certain confidence-building measures, such as sharing data on non-state or third-party threats, and even sharing good practice.

A second set of recommendations would be for all nuclear-armed states to work to protect nuclear systems against direct cyber-attack through better network defences, firewalls and physical security. This may involve embracing measures to minimise the implications of indirect cyber interference, such as using upgraded infrastructure[3], and highly redundant communications systems, better training and screening of operators, and perhaps even reducing the alert levels of forces and the time it takes for weapons to be fired. It might also involve a concerted effort to keep nuclear C2 systems relatively simple and separate from the C2 systems used for conventional operations. Keeping nuclear systems simple, separate and secure would appear to be another sensible way to help mitigate some of the new dangers posed by cyber.

Finally, the leaders of nuclear-armed states desperately need to start a discussion about the nature and implications of the emerging cyber–nuclear nexus, and begin to think about pursuing certain confidence-building measures at the strategic level. Such dialogue may help provide the basis for more concrete mechanisms of protection and control, such as a set of moratoria or agreements between states not to target each other's nuclear C2 systems with cyber, for example.[4] This in turn may help lay the foundations for broader bilateral or even multilateral arms control agreements in the cyber–nuclear realm in the future, and even for talks that address the whole range of emerging technological challenges to nuclear orthodoxy.[5] While none of this will be easy or straightforward, it is imperative to act now, and to guard against the new and growing challenges to nuclear weapons presented by the cyber age.

---

2. It is equally important not to let nuclear systems simply erode.
3. Although not necessarily more complex or digitised, as discussed in Chapter I.
4. Danzig, 'Surviving on a Diet of Poisoned Fruit', p. 26, Recent moves to consider using cyber-attacks on C2 systems as part of a US 'full-spectrum missile defense' concept are certainly not a welcome development in this regard, see Andrew Futter 'The Danger of Using Cyber Attacks to Counter Nuclear Threats', *Arms Control Today*, July/August 2016.
5. Such as the spread and increasing sophistication of ballistic missile defences and various new prompt global conventional strike weapons systems.

About the Author

Andrew Futter is a senior lecturer at the University of Leicester, UK, a member of the Cyber-Nuclear Security Threats Task Force, run by the Nuclear Threat Initiative, an Honorary Fellow at the Institute for Conflict, Cooperation and Security at the University of Birmingham, a member of the Euro-Atlantic Security Next Generation Working Group, and the co-founder of the BISA Global Nuclear Order Working Group. He is the author of three books: *Ballistic Missile Defence and US National Security* (2013), *The Politics of Nuclear Weapons* (2015), and *Reassessing the Revolution in Military Affairs* (2015). His fourth book, *The United Kingdom and Nuclear Weapons*, will be published later this year. He has written widely on nuclear strategy, proliferation, missile defence and deterrence, and is currently working on an ESRC-funded Future Research Leader's project looking into the impact of cyber on nuclear weapons (grant number ES/K008838/1). More information about his research can be found at: <http://www2.le.ac.uk/departments/politics/people/afutter>, and he can be contacted at Ajf57@le.ac.uk.