Hacking the Bomb: Nuclear Weapons in the Cyber Age

Andrew Futter[1]

The development and spread of cyber weapons, information warfare capabilities and the new dynamics of the so-called "cyber age" are providing a considerable – albeit nuanced – challenge to the management, thinking and strategy that underpins nuclear weapons. While Cyber will not supersede nuclear as the ultimate symbol of national security any time soon, the challenges of the digital age range and impact right across the nuclear weapons enterprise from safe, secure and reliable command and control to new problems for proliferation, espionage, sabotage, and deterrence, and will undoubtedly complicate future crisis management between nuclear-armed rivals. The main aim of this paper therefore is to unpack this challenge, debunk any myths, and provide a framework through which to understand, evaluate, and ultimately address the emerging cyber-nuclear nexus.

Key words: nuclear weapons, nuclear strategy, cyber, normal accidents, espionage and sabotage, deterrence, crisis stability

Introduction: cyber hype and the bomb

The hype surrounding the threat of "cyber attack" has become particularly pervasive in recent years with concerns abounding about a possible "digital Pearl Harbor"[2] or a "cyber 9-11"[3], and in this new computer-based environment it has become vogue to assume that cyber will increasingly impact every aspect of national security thinking and strategy. Indeed, it is now over two decades since John Arquilla and David Ronfeldt warned in their seminal article that, "cyber war was coming".[4] However, and while the growth of "cyber" and the associated technological dynamics of the information age are increasingly shaping security thinking and strategy, 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" any time soon – even the highly sophisticated Stuxnet virus was limited in its

[1] Dr. Andrew Futter is a Senior Lecturer in International Politics at the University of Leicester, UK. Ajf57@le.ac.uk

[2] See "Remarks by Secretary [of Defense Leon] Panetta on Cybersecurity to the Business Executives for National Security", New York City (11 October 2012), http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136

[3] 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), http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124

[4] John Arquilla & David Ronfeldt, "Cyberwar is coming!" *Comparative Strategy*, 12:2 (1993) pp.141-165

destruction, did not cause any fatalities and took many years and considerable expertise to perfect. Neither are teenage hackers – or terrorists - likely to be able to detonate a nuclear weapon from the comfort of their bedroom, or hack into the Pentagon and begin a nuclear World War Three as in the 1983 film *War Games* – at least, that is, not for the foreseeable future.

That said, the dynamics and developments of the so-called "cyber age" are nevertheless changing, recasting and exacerbating existing tensions right across the nuclear weapons enterprise. These challenges are myriad in their scope, and range from the safe, secure and reliable command and control of nuclear forces – including the threat of nuclear accidents, through new problems for information and systems security, proliferation, and the safeguarding of highly sensitive nuclear secrets, to new complications for strategic deterrence and the emergence of a cyber-nuclear security dilemma that must be factored into future crisis stability and management. In this way, the challenge of the cyber age for nuclear weapons is more nuanced and subtle than perhaps it first appears, complicating and obfuscating the inherent challenges associated with nuclear weapons rather than fundamentally transforming them. While these challenges are far from insurmountable, they do – taken together – represent an important shift in the nature of the environment in which nuclear weapons are thought about, states manage their nuclear forces and nuclear policy and strategy is made. The aim of this paper therefore is to unpack and assess these new challenges, debunk any unhelpful myths, and provide a framework and basis with which to fully understand the nature and implications of the cyber age for nuclear weapons.

To do this, the paper proceeds in six sections; (1) the first seeks to demystify what is meant by the term "cyber" and the concept of a "cyber age" and presents a suitable framework through which to examine the nuclear weapons enterprise; (2) the second looks at how the growing complexity of nuclear systems and reliance on computers more generally may lead to more "normal nuclear accidents" and create new vulnerabilities to be exploited; (3) section three looks at the threat, nature and implications of nuclear espionage and at how the nature of "spying on the bomb" has and will evolve in the cyber age; (4) the fourth section considers the seriousness of cyber-nuclear terrorism and other new forms of sabotage and destruction of nuclear weapons and related facilities; (5) section five examines the link between nuclear and cyber, explains the problems of cyber defence and arms control, and assesses the role of nuclear weapons in deterring cyber attack; (6) finally, section six looks at how cyber weapons and methods of information warfare are complicating future crisis management between nuclear-armed actors

The cyber challenge to nuclear weapons

The nature of the term "cyber" is fundamentally contested, and there exists no one definition that all adhere too when seeking to use and analyse the concept.[5] The natural result is that different analyses come to different conclusions and offer different solutions to different problems – this unfortunately continues to hamstring much cyber analysis, and has undoubtedly complicated the ongoing cyber debate. The fundamental problem is that what constitutes "cyber" remains very much in the eye of the beholder. In fact, "cyber" analyses range in scope from those that use a very narrow definition and that focus primarily on Computer Network Operations (CNO)[6] and attacks over and through the Internet, through a broader concept that tends to see cyber as closer to the field of Information Warfare (IW) – and therefore includes more than just CNOs, up to analyses that treat cyber as a holistic concept effecting every part of national security thinking, and that see the concept as referring to an all-encompassing "cyber age". On a second level, cyber analysis is often hampered by the considerable differences between types of cyber attack, which range across a "cyber spectrum" from simple "hacking", "hactivism" and nuisance – which might be carried out by anyone and be of relatively minimal concern, through denial of service and espionage, up to sabotage, destruction and possibly existential attacks and war – much more likely to be the preserve of powerful nation states.[7] As Thomas Rid and Peter McBurney explain "Cyber weapons span a wide spectrum. That spectrum, we argue, reaches from generic but low potential tools to specific but high potential weaponry."[8] It is this diverse nature of the scope and challenge that creates many of the problems that underpin cyber analysis, and is key reason for continued disagreement about the level and nature of the threat.

Clearly each of these approaches has benefits and drawbacks, but for the type of wide-ranging examination being undertaken here, it makes most sense to look at all aspects of cyber phenomenon and consider it in its broadest scope and across the physical, informational and

[5] Perhaps the best definition is provided by Daniel Kuehl, "… 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." Daniel Kuehl, *"From cyberspace to cyberpower: defining the problem",* chapter in Franklin Kramer, Stuart Starr & Larry Wentz (Eds.), *"Cyberpower and national security",* (Dulles VA, Potomac Books Inc: 2009) p.28

[6] 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 more to hacking and espionage.

[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 but skillful hackers." Mike McConnell, "Cyberwar is the new atomic age", *New Perspectives Quarterly,* 26:3 (2009) p.76

[8] Thomas Rid & Peter McBurney, "Cyber-weapons", *The RUSI Journal,* 157:1 (2012) p.8

cognitive domains as well as just the logical domain of Computer Network Operations (CNO). In this way, the framework adopted here is designed to consider the impact that the increasing digitization of society is having on nuclear thinking and strategy. While the discrete threat of hacking and attacks over the Internet are clearly important, they are far from the only dynamics that will impact the nuclear weapons enterprise. 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.[9]

In this way cyber attacks can 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; carried out through computer networks and the Internet or attacks on software, such as through certain malware, logic bombs and general hacking; and by attacking the information on which the systems and therefore operators act and make their decisions – such as by altering key information sets and data. The cyber challenge therefore also includes the natural problems inherent in increasingly complex computer systems – such as badly written software or programme "bugs"[10] – and the overall uncertainly of whether key systems will always work as expected irrespective of outside interference. In this way the cyber challenge involves both inherent vulnerabilities in nuclear systems as well as the threat from actors seeking to gain access to these systems in order to alter, disable, disrupt or damage them. Finally, perhaps the key components of the cyber challenge are humans: it is people that design systems, write software, and place their faith in computers and machines to carry out tasks as intended. Ultimately, it is important to remember that the human-computer interface remains a key "battlefield" in the cyber age – computers don't think (at least not yet), they do what they are programmed to do.

The result is a cyber-nuclear taxonomy that seeks to consider the challenge in the most holistic manner, and therefore includes not just attacks on nuclear weapons over the Internet, but also broader types of attacks on information and information systems related to the nuclear weapons enterprise, as well as other cyber attacks that might involve – but are not necessarily directed against – nuclear weapons. We can think of classifying this in terms of five sets of descriptors: (1) *broad-based* attacks on civilian or military infrastructure that might have implications for nuclear forces (i.e. deterrence and strategy) and *discrete* attacks directed at nuclear weapons and associated

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

[10] Bugs are unintended errors in software and coding and not "cyber attacks".

components and infrastructure; (2) *physical* attacks on computers, software, hardware, communications or networks related to nuclear weapons (e.g. destroying a satellite, crashing a computer or compromising communications), and *logical* attacks – those conducted at a distance, and through the exploitation of malware, logic bombs and other computer-based attacks, and possibly over a network or the Internet; (3) attacks and vulnerabilities that primarily involve *computers and machines*, those that involve *humans*, and those that involve a combination of the two; (4) problems that are *inherent* in software (or hardware) and technology that could lead to normal accidents and malfunctions as a result of bugs, and attacks that are *deliberate* and carried out intentionally by an adversary – perhaps by exploiting these vulnerabilities; (5) challenges that are *actual* – such as infected software, compromised systems, hardware that has been damaged or destroyed – 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.

The "cyber" challenge to nuclear weapons is therefore multifaceted and impacts across every level of the cyber-nuclear nexus. It ranges from single unit variables and nuclear command and control (such as missiles, warheads, specific computers, or early warning systems) through state level structures and national security thinking (such as about nuclear deterrence, strategy and nuclear posture), right up to international strategic relations, crisis stability and balances. While often discrete, these challenges are of course interlinked and act as a multiplier across the nuclear weapons enterprise. The result is that it makes sense to consider the impact on nuclear weapons and their perceived utility in its 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.

Complexity, normal nuclear accidents and new nuclear vulnerabilities

While the central focus of the cyber challenge and of the burgeoning "cyber age" tends to be about hacking, malware, logic bombs or denial of service attacks, perhaps the subtlest challenge is one that has little to do with attacks or weapons at all. In fact, one of the biggest challenges is the natural and inherent problems and "bugs" that are contained in evermore sophisticated and complex software and coding. Generally speaking complex systems – particularly computer-based systems - are likely to contain more bugs, problems and unforeseen errors, 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.[11]

There is perhaps no better example of a "complex system" than that required for nuclear command and control – that is ensuring that nuclear weapons are safe and secure against unauthorized use or accidents while at the same time ensuring that they can and will be used if and when required. This is known as the "always-never paradox"[12], and is increasingly reliant upon computers and software for all nuclear-armed states. There are three significant implications of this for nuclear weapons management; (1) increasing complexity – particularly computerization – raises the risk of "normal nuclear accidents" within the nuclear enterprise; (2) complex systems used to manage nuclear forces contain inherent vulnerabilities and bugs that might be exploited, and; (3) a growing dependence on computers for society more broadly raises the possibility of large scale cyber attack against non-nuclear systems and critical national infrastructure.

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.[13] This is particularly the case with highly pressurized systems, those that can never be fully tested, or with systems that deal with hazardous technologies. There is perhaps no better example of a complex system than those developed for nuclear command and control, and it should be no surprise that the atomic age is littered with accidents and nuclear near misses – indeed, there are probably many more that we will never know about.[14] In fact, the complexity of the nuclear weapons business means that the likelihood of such accidents has essentially become "normalized" – if things can go wrong they will go wrong![15] Indeed, as Scott Sagan points out "…from a normal accidents perspective, the fact that there has never been an accidental nuclear weapons detonation or an accidental nuclear war is

[11] Martin Libicki, *"Conquest in cyberspace: national security and information warfare",* (New York, Cambridge University Press: 2007) pp.293-294

[12] This phrase was coined by Peter Feaver, see Peter Feaver, *"Guarding the guardians: civilian control of nuclear weapons in the United States",* (London, Cornell University Press: 1992)

[13] On this see Charles Perrow, *"Normal accidents: living with high-risk technologies",* (Princeton NJ, Princeton University Press: 1999)

[14] 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)

[15] In the words of Paul Bracken, "In the world of experience we feel complex systems are bound to go awry precisely because they are so complex." Paul Bracken, *"Instabilities in the control of nuclear forces",* chapter in Anatoly Gromyko & 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

surprising."[16] While not all previous nuclear accidents have involved computers and software, and many have simply involved human error, a significant number of incidents have, and this seems likely to increase as systems for nuclear weapons management become more complex, digitized and intricate.[17]

Perhaps the best examples of computer-induced nuclear accidents are those events that occurred at the US North American Aerospace Defense Command (NORAD) between 1979 and 1984 – although this list is by no means exhaustive.[18] The first took place in October 1979 after computers at NORAD indicated that missile had been launched from a submarine in the waters off the West Coast. A low level state of nuclear war was declared and nuclear-armed missiles across the United States went on alert. The "attack" was later discovered to have been caused by someone accidentally loading a war game onto the computer at the operations centre that simulated a Soviet attack.[19] 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[20], and in 1984, a computer malfunction indicated that a US nuclear-armed missile was about to fire.[21] 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.[22] Data for other nuclear 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.[23] This risk is only likely to grow as nuclear-armed

[16] Scott Sagan, *"The limits of safety: organizations, accidents and nuclear weapons",* (Princeton NJ, Princeton University Press: 1993) p.45

[17] In the words of Soviet physicist Boris Rauschenbach, "In terms of potential nuclear war … the very existence of humankind is becoming dependent on hardware and software." Boris Raushenbach, *"Computer war",* chapter in Anatoly Gromyko & 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.47

[18] While the rise of computer induced problems in military command networks can be traced back to the early 1980s (see for example William Broad, "Computer security worries military experts", *New York Times,* (25 September 1983), http://www.nytimes.com/1983/09/25/us/computer-security-worries-military-experts.html), 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 ICBM's. See Eric Schlosser, "Neglecting our nukes", *Politico,* (16 September 2013), http://www.politico.com/story/2013/09/neglecting-our-nukes-96854.html

[19] William Broad, "Computers and the military don't mix", *Science,* 207:14 (1980) p.1183

[20] 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

[21] Shaun Gregory, *"The hidden cost of nuclear deterrence: nuclear weapons accidents",* (London, Brassey's: 1990) p.97

[22] Eric Schlosser, "Neglecting our nukes", *Politico,* (16 September 2013), http://www.politico.com/story/2013/09/neglecting-our-nukes-96854.html

actors come to rely more on computers and complex systems for nuclear weapons management.[24] Moreover, as Peter Neumann notes, "If an event can happen accidentally, it often could be caused intentionally."[25]

The second implication of a growing reliance on software and computers for nuclear weapons management – both operations and infrastructure - is the natural increase in the number of vulnerabilities in this software that could be exploited by a would-be attacker. Of the two, increased vulnerabilities and "ways in" to operational software used for nuclear command and control is clearly the more serious – although hacking into weapon's software would be very difficult.[26] But software vulnerabilities also make it easier to hack into other 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. Such vulnerabilities or "bugs" as they are known colloquially, are essentially coding errors that allow hackers to break into systems and circumvent their security mechanisms. Vulnerabilities and "zero day exploits" (i.e. vulnerabilities that are yet to be discovered or patched) can now be purchased on the black market[27] – indeed, Stuxnet relied on four of these zero days in order to attack the enrichment plant at Natanz.[28] Moreover, and while former head of US Strategic Command General Robert Kehler has remarked that he "is confident that US command and control systems and nuclear weapons platforms 'do not have significant vulnerability' that cause him to be concerned."[29] He later

---

[23] 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." Eric Schlosser, *"Command and control",* (London, Allen Lane: 2013) p.481

[24] Christopher Stubbs suggest 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." Christopher Stubbs, *"The interplay between cultural and military nuclear risk assessment",* chapter in George Shultz & 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

[25] Peter Neumann, *"Computer related risks",* (New York, Addison-Wesley Publishing Company: 1995) p.126

[26] Although as is noted later in this paper, far from impossible.

[27] Andy Greenberg, "Shopping for zero-days: a price list for hackers secret software exploits", *Forbes,* (23 March 2013), http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

[28] Liam O'Murchu, "Stuxnet using three additional zero-day vulnerabilities", *Symantec Official Blog,* (14 September 2010), http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities

[29] Quoted in Aliya Sternstein, "Officials worry about vulnerability of global nuclear stockpile to cyber attack", *Global Security Newswire,* (14 March 2013), http://www.nti.rsvp1.com/gsn/article/officials-worry-about-vulnerability-global-nuclear-stockpile-cyberattack/?mgh=http%3A%2F%2Fwww.nti.org&mgf=1

remarked in a different interview that "we don't know what we don't know."[30] Likewise the recent decision taken by the UK government to upgrade of the software used for the UK Trident submarines, known as "Windows for Submarines", came under strong scrutiny from the software community who viewed the decision not to purchase the more expensive Linux software as dangerous, suggesting that it could lead to loses in security, reliability and assurance.[31] Interesting, in this way, as Martin 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."[32]

The increasing computerization, digitization and complexity of both nuclear operations and nuclear infrastructure therefore raises the risk of "normal nuclear accidents" and creates new vulnerabilities that can be exploited. 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.[33]

As a result it may be that less sophisticated systems are less vulnerable to cyber attack and normal nuclear accidents, but at the same time, this will limit what they are able to do in terms of command and control.

Stealing secrets: spying, hacking and nuclear espionage

The threat 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

---

[30] Quoted in Eric Schlosser, "Neglecting our nukes", *Politico,* (16 September 2013), http://www.politico.com/story/2013/09/neglecting-our-nukes-96854.html. According to Adam Segal of the Council on Foreign Relations, the US national security enterprise experiences up to 10 million significant cyber events every day … "the majority of these are … looking for vulnerabilities." Quoted in Jason Koebler, "US nukes face up to 10 million cyber attacks daily", *USNews,* (20 March 2012), http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily

[31] Lewis Page, "Royal Navy completes Windows for Submarines rollout", *The Register,* (16 December 2012), http://www.theregister.co.uk/2008/12/16/windows_for_submarines_rollout/. Interesting, the United States decided to drop windows systems for its nuclear subs in favour of Linux. See "US Navy rejects Windows for Linux", *Tech Khabaren,* (24 June 2012), http://techkhabaren.wordpress.com/2012/06/24/us-navy-rejects-windows-for-linux/

[32] Martin Libicki, *"Conquest in cyberspace: national security and information warfare",* (New York, Cambridge University Press: 2007) p.40

[33] Ross Anderson, *"Security engineering: a guide to building dependable distributed systems",* (Indianapolis IN, Wiley Publishing: 2008)

spies sought (and acquired) information on the Manhattan Project and early US nuclear bomb designs, and all aspects of nuclear spying have remained a constant ever since. However, the spread of computers, networks and digitally stored data has created new problems for nuclear secrecy and has changed, expanded and diversified the methods available for nuclear espionage. As Peter 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."[34]

The nature of the challenge is not simply "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, but it is also from the importance of computer and information security in those systems that may already be air-gapped or separated from the Internet. Both are particularly acute issues because of the large amount of information that can be stored on computers and that can therefore also be stolen quickly and with minimal effort. Rather than having to rely on copying by hand, taking photos or risk removing documents, enormous amounts of information can now be (and has been) emailed or removed on a USB drive, a CD or in some other digital format. When such attacks can be carried out over the Internet, the risks are reduced even further so that no human agent needs to be placed in danger. Likewise, these economies of scale also allow widespread "hoovering" espionage attacks that attempt to steal as much information as possible about all things as well as the more targeted attacks on specific and specialized information. Moreover, the very nature of hacking means that some secrets may be stolen 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 probably began in the mid-1980s as computers and networks gradually expanded throughout (particularly US) defence and military establishments, and specifically to the 1986 *"Cuckoo's Egg"* episode. Cuckoo's Egg refers to the discovery by systems administrator Clifford Stoll than a German hacker named Markus Hess had breached numerous research and US military computers in order to find information on topics like nuclear weapons and the Strategic Defense Initiative (SDI).[35] It later turned out that Hess had been working for the Soviet KGB who were desperate to find out about SDI and the Reagan administration's nuclear plans. Since this time the volume and scope of cyber-nuclear espionage has expanded exponentially: in 1991 Dutch hackers broke into US military networks and it was feared they were searching for nuclear secrets and missile data to sell to Saddam Hussein[36]; in 1998 the Cox Report

[34] Peter Singer & Allan Friedman, *"Cybersecurity and cyberwar: what everyone needs to know",* (Oxford, Oxford University Press: 2014) p.92

[35] For the best overview of this see Clifford Stoll, *"The cuckoo's egg: tracking a spy through the maze of computer espionage",* (London, Doubleday: 1989)

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

revealed that the Chinese had stolen a considerable cache of highly sensitive secrets over a number of years, particularly those relating to the W88 nuclear warhead design – Matthew McKinzie later remarked that it was an "unprecedented act of espionage … The espionage in the Manhattan Project [would] pale in comparison"[37], this became known as *Kindred Spirit*[38]; also in 1998 an American teenage hacker broke in to India's Bhabha Atomic Research Centre (BARC) and downloaded passwords and emails[39]; in 1999 the thousands of files stolen and the extent of the infiltration of the *Moonlight Maze* attack on Pentagon and sensitive information held by other US government departments was revealed. The attack was believed to emanate from Russia.[40]

This trend has continued and in fact deepened during the last decade: in 2005 hackers believed to be linked with the Chinese PLA infiltrated numerous US military systems searching for nuclear secrets amongst other defence information in an operation dubbed *Titan Rain*[41]; in 2006 the Israeli Mossad planted a Trojan in the computer of a senior Syrian government official which revealed the extent of the Syrian nuclear programme and led directly to the attacks of 2007[42]; in 2008 an infected USB stick led to *Operation Buckshot Yankee* where US classified networks were breached and the air-gap was jumped – the agent.btz malware was designed by Russia to steal military secrets and contained a beacon to allow mass data exfiltration.[43] In recent years the cyber espionage threat has diversified to include all manner of nuclear related systems: in February 2011 the *Zeus* information stealing Trojan aimed at contractors involved in building the UK Trident Submarine force was discovered[44]; in May 2011 Iran was accused of hacking the IAEA looking for

---

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

[38] On this see 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*, Updated (1 February 2006), RL30143, http://fas.org/sgp/crs/nuke/RL30143.pdf

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

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

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

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

[43] Karl Grindal, *"Operation Buckshot Yankee",* chapter in Jason Healey (Eds.), *"A fierce domain: conflict in cyberspace 1986 to 2012",* (USA, Cyber Conflict Studies Association: 2013) p.208

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

secrets regarding the monitoring of its nuclear programme[45]; in August 2011 the *Shady RAT* malware targeted US government agencies, defence contractors and numerous high-technology companies[46], and in November 2012 the group Anonymous claimed to have hacked the International Atomic Energy Agency (IAEA) and threatened to release the "highly sensitive data" on the Israeli nuclear programme that they had allegedly seized.[47] US nuclear laboratories and defense contractors have remained a primary target for hackers for at least the last decade[48], 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.[49] Hackers have also targeted nuclear-related systems, perhaps most notably the US and Israeli ballistic missile defence programmes, and stolen important and secret data.[50] 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 Iran.[51] Likewise, both the *Flame* and *Duqu* cyber attacks were designed primarily to gain intelligence on systems and infrastructure – likely as precursor to a possible future physical attack or sabotage on the Iranian nuclear programme.[52] Indeed, an incident at the Fordo enrichment plant in 2012 where a suspected monitoring device disguised as a rock blew up, suggested that the US and Israel have continued to spy on the Iranian nuclear programme as negotiations have continued.[53]

---

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

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

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

[48] See for example, "Nuclear security: Los Alamos National Laboratory faces challenges in sustaining physical and cyber security improvements", US Government Accountability Office, (25 September 2008), http://www.gao.gov/assets/130/121367.pdf or more recently, Aliya Sternstein, "Attack on energy lab computers was isolated, officials say", *Global Security Newswire,* (26 April 2011), http://www.nti.org/gsn/article/attack-on-energy-lab-computers-was-isolated-and-limited-officials-say/

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

[50] "Chinese hacking targets US missile defense designs", *Global Security Newswire,* (28 May 2013), http://www.nti.org/gsn/article/chinese-hacking-targets-us-missile-defense-designs/ & Debalina Ghoshal, "China hacking Iron Dome, Arrow missile defense systems", *Gatestone Institute,* (5 August 2015), http://www.gatestoneinstitute.org/4578/china-hacking-missile-defense

[51] Kim Zetter, *"Countdown to zero day: Stuxnet and the launch of the world's first digital weapon",* (New York, Crown Publishers: 2014) p.321

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

[53] Uzi Mahnaimi, "Fake rock spying device blows up near Iranian nuclear site", *The Sunday Times,* (23 September 2012), http://www.thesundaytimes.co.uk/sto/news/world_news/Middle_East/article1131847.ece

While the volume of cyber spying and the theft and attempted theft of a wide variety of nuclear secrets has expanded exponentially in recent years, the implications of this are mixed, and cyber nuclear espionage should not therefore be seen as a homogenous threat. On the lower end of the scale cyber nuclear espionage is primarily about acquiring knowledge and intelligence on what a certain state or actor is doing and the relative capabilities of key programmes. It might even be about showing that it is possible to access these systems and acquire information, albeit for no particular military purpose. On the next level 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 might be the recent attempts to steal Israeli and US missile defence information. Slightly more concerning is that nuclear secrets are stolen to aid proliferation – this was certainly the case with China and the US W88 warhead – or that key nuclear designs could be traded on the nuclear black-market to states or non-state actors looking to acquire nuclear capabilities.[54] Arguably the worst case scenario is that these attacks are used as precursors to sabotage and physical destruction, and are used to find out about key systems and their vulnerabilities, implant logic bombs or simply 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.

Sabotage and destruction

The cyber age and the computerization of society has transformed the scope for sabotage of key systems, both in terms of critical national infrastructure and directly against nuclear weapons and associated systems. In this way the challenge is divided between narrow and discrete attacks directed against nuclear forces and systems – such as in procurement, early warning or the destruction of facilities, and attacks not directed against nuclear weapons but that could effect nuclear thinking – such as a strategic attack against critical national infrastructure (this is considered in more detail in the next section). While key nuclear systems are certainly likely to be far better protected than commercial infrastructure against sabotage and attack, and almost certainly air gapped from the Internet, the threat is real and manifests 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 cyber attacks."[55]

---

[54] See Catherine Collins & Douglas Frantz, "Down the nuclear rabbit hole", *Los Angeles Times,* (3 January 2011), http://articles.latimes.com/2011/jan/03/opinion/la-oe-frantz-khan-20110103

[55] Quoted in Timothy Farnsworth, "Study sees cyber risk for US arsenal", *Arms Control Today,* (April 2013), http://www.armscontrol.org/act/2013_04/Study-Sees-Cyber-Risk-for-US-Arsenal

The procurement of nuclear-related software and components and the need to update and replace systems presents a serious vulnerability for the nuclear weapons complex. The main threat here is that vulnerabilities, problems, logic bombs or even software or hardware Trojans can be inserted into software and systems in the manufacturing and supply stage. Sabotage can come in many guises; it could involve the physical alteration of components so that they don't work or at least not work as expected, or the introduction of malware or 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."[56] But even protecting systems built yourself is not straightforward, and some vulnerabilities may simply be the result of accidents.

The first known example of "cyber-sabotage" can actually be traced back to the 1980s when the CIA began a massive operation to feed modified technical equipment to the Soviet Union. 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"[57], "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."[58] While the extent of the operation remains disputed[59], former Air Force Secretary Thomas Reed would later claim that a huge explosion in Russian gas pipeline in 1982 was a direct result of this sabotage operation.[60] More recently, and while the majority of attention has focused on Stuxnet, it is clear that a widespread sabotage campaign directed against the Iranian nuclear programme has been underway for well over a decade. In fact, 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.[61]

---

[56] Ross Anderson, *"Security engineering: a guide to building dependable distributed systems",* (Indianapolis IN, Wiley Publishing: 2008) p.645

[57] Thomas Reed & Danny Stillman, *"The nuclear express: a political history of the bomb and its proliferation",* (Minneapolis MN, Zenith Press: 2009) p.274

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

[59] See for example, Anatoly Medetsky, "KGB veteran denies CIA caused 82 blast", *The Moscow Times,* (18 March 2004), http://www.themoscowtimes.com/news/article/kgb-veteran-denies-cia-caused-82-blast/232261.html

[60] See Thomas Reed, *"At the abyss: and insiders history of the Cold War",* (New York, Presidio Press: 2007)

[61] Quoted in Eli Lake, "Operation sabotage", *The New Republic,* (14 July 2010), http://www.newrepublic.com/article/world/75952/operation-sabotage

During the 1990s the US and Israel "modified" vacuum pumps purchased by Iran to make them break down[62]; in 2012, Iranian lawmaker Aladedin Boroujerdi accused Germany's Siemens of planting tiny explosives inside equipment the Islamic Republic had purchased for its disputed nuclear programme[63]; and in 2014, Iranian Foreign Minister Mohammed Javad Zarif accused "the West" of "trying to sabotage the heavy water nuclear reactor at Arak by altering components of its cooling system", and a huge explosion at the Parchin military base in October again raised the question of sabotage.[64] Similar techniques have also been used to aid counter-proliferation efforts, especially against terrorist groups. As Eli Lake points out "… the specific benefit of sabotage is that it makes countries wary of purchasing crucial [nuclear-related] materials on the black market."[65]

The threat of sabotage 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, 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 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."[66] As a result, the non-stealthy F-15 and F-16 aeroplanes 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 – developed by BAE – worked, but it is possible that code could have beamed into the radar from above or the system had been hacked by the Israelis prior to

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

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

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

[65] Eli Lake, "Operation sabotage", *The New Republic,* (14 July 2010), http://www.newrepublic.com/article/world/75952/operation-sabotage

[66] David Fulgham, David Fulghum, "Why Syria's air defenses failed to detect Israeli's", *Aviation Week & Space Technology,* (12 November 2013)

the attack.[67] The Syrian radar system was likely purchased from Russia and is currently being used by a number of other states, among them reportedly, Iran.[68] While this attack was fairly limited, it nevertheless provides a stark warning of new types of vulnerability, particularly for key nuclear communications systems.[69] 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.[70] Likewise, the risk of "spoofing" remains ever present – in July 2014 for example an Israeli military twitter account was hacked and an erroneous report published that Dimona had been attacked by rockets and had caused a "radiation catastrophe".[71]

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. There are only a handful of cyber-attacks that have caused physical destruction that are publicly known about[72], and only one – Stuxnet – that has cause direct destruction of a nuclear facility. While these attacks were all limited and highly specialized they do nonetheless show that it is possible to infect and damage physical systems – often not connected to the Internet - by hacking into the computers and networks that

---

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

[68] John Leyden, "Israel suspected of 'hacking Syrian air defences: did algorithms clear path for air raid?", *The Register,* (4 October 2007), http://www.theregister.co.uk/Print/2007/10/04/radar_hack_raid/

[69] 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". Jim Michaels, "US could use cyberattack on Syrian air defenses", *USA Today,* (16 May 2013), http://www.usatoday.com/story/news/world/2013/05/16/syria-attack-pentagon-air-force-military/2166439/. And 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." Eric Schmitt & Thom Shanker, "US debated cyberwarfare in attack plan on Libya", *New York Times,* (17 October 2011), http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=0

[70] 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." Jason Fritz, "Hacking nuclear command and control", *International Commission on Nuclear Non-proliferation and disarmament,* (2009),www.icnnd.org/Documents/Jason_Fritz_Hacking_NC2.doc

[71] "Hacked Israeli military twitter account declared nuclear leak", *Global Security Newswire,* (7 July 2014), http://www.nti.org/gsn/article/hack-israeli-military-account-erroneous-post-announces-nuclear-leak/

[72] The attack on Saudi Aramco in August 2010 and the attack on a German steel mill in December 2014 are the best known. See Christopher Bronk & Eneken Tikk-Ringas, "The cyber attack on Saudi Aramco", *Survival,* 55:2 (2013) pp.81-96 and Kim Zetter, "A cyberatttack has caused confirmed damage for the second time ever", *Wired,* (8 January 2015), http://www.wired.com/2015/01/german-steel-mill-hack-destruction/

control them. The Stuxnet virus – W32.Stuxnet – that was discovered by Belarusian company VirusBlockAda in June 2010 was only one of a number of pieces of malware aimed at the Iranian nuclear enrichment programme at Natanz, which together have been credited with causing significant damage to centrifuges and delaying considerably any Iranian bomb.[73] The Stuxnet viruses were designed to attack the SCADA control systems operating the centrifuges needed to enrich uranium, first by attacking the valves the managed the flow of uranium hexafluoride into the centrifuge, and later more directly by attacking the frequency converters.[74] The thinking, according to David Sanger, "was that the Iranians would blame bad parts, or bad engineering, or just incompetence."[75] However, the success of Stuxnet was dependent upon a considerable amount of prior monitoring and mapping of the system before any attack could take place, this information was integral to its ability to work as planned. It is believed that Stuxnet entered the air-gapped Natanz system through an infected USB drive or other media and probably via an unwitting employee who had access to infection points.[76]

While Stuxnet undoubtedly represented a quantum leap in cyber capabilities and Operation Orchard demonstrated the vulnerabilities of early warning and communications, the threat of cyber sabotage to the nuclear enterprise remains limited – at least for now. That said, recent events have shown that even systems not connected to the Internet as well as those vital for nuclear operations could be compromised in a worst case scenario and that cyber-based weapons offer a useful method of counter-proliferation. Interestingly therefore, it may be that the older and less sophisticated the systems and infrastructure used in nuclear command and control, the more safe and secure against sabotage they will be.

Nuclear strategy and cyber deterrence

The threat of cyber attack and the proliferation of "cyber weapons" have necessarily created a range of new pressures for national security policy and the role of nuclear weapons, and specifically for defence, deterrence and possible retaliation. Formulating a credible and workable way to respond

[73] 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?", *Institute for Science and International Security,* ISIS Reports, (22 December 2010), http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

[74] Kim Zetter, *"Countdown to zero day: Stuxnet and the launch of the world's first digital weapon",* (New York, Crown Publishers: 2014) p.302-303

[75] David Sanger, *"Confront and conceal: Obama's secret wars and surprising use of American power",* (New York, Broadway Paperbacks: 2013) p.188

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

to the cyber challenge has however been far from easy, and this has been greatly complicated by the considerable differences between nuclear and cyber, the problems and limitations of cyber defence and arms control, the likely need for some type of cross-domain deterrence/ retaliation strategy (that may nor may or may not include nuclear weapons) and perhaps above all the uncertainty of the nature and extent of any future cyber attack. These dynamics have made formulating a credible nuclear-cyber strategy very difficult.

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 bracket is fundamentally unhelpful. While there are some similarities; offense appears to trump defence and both often involve delivery vehicles and "payloads", we can think of at least four main differences between cyber and nuclear; (1) the scale and nature of the threat, (2) the types of targets to be attacked, (3) the types of actors involved, and (4) 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[77], and it is difficult to think of cyber weapons as being "strategic" or for that matter as constituting war at least on their own (although this remains the subject for debate, and could change in the future).[78] Martin Libicki sums up this difference nicely; "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."[79] Part of the reason for this is that the intended targets of cyber and nuclear attack tend to be fundamentally different. While it is possible to have limited or focused nuclear attack, nuclear weapons are generally seen as indiscriminate and intended to cause widespread damage to large urban areas, by contrast the most threatening cyber attacks are likely to be highly specialized and target very specific systems or machines – in fact, they often require highly specialized knowledge of the target beforehand to be effective.[80] Nuclear weapons have traditionally been the preserve of nation states and the main actors in the nuclear game have been national governments – partly due to the enormous cost and

[77] 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 cyber attack.

[78] For example, Thomas Ridd and Peter McBurney have suggested that "An act of war must be instrumental, political and potentially lethal, whether in cyberspace or not. No stand alone cyber offense on record on record meets these criteria, so a 'cyberwar' remains a metaphor for the time being." Thomas Rid & Peter McBurney, "Cyber-weapons", *The RUSI Journal,* 157:1 (2012) p.7.

[79] Martin Libicki, *"Conquest in cyberspace: national security and information warfare",* (New York, Cambridge University Press: 2007) p.39

[80] As Dale Peterson explains, "An organization wanting to attack a potential adversary's critical infrastructure must first learn what system that adversary has." Dale Peterson, "Offensive cyber weapons: construction, development and employment", *The Journal of Strategic Studies,* 36:1 (2013) p.121

undertaking involved in producing and fielding nuclear weapons - and this has meant that it has been pretty clear where the threat comes from and who is ultimately responsible. 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 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, Mutual Assured Destruction (MAD), cyber arms control and cyber deterrence in particular are inherently complicated, and there is no established tradition of cyber non-use – in fact, cyber attacks are ongoing pretty much all of the time.[81] 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.[82]

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. William Lynn has argued that "…traditional models of assured destruction do not apply in cyber space … deterrence will necessarily be based more on denying any benefit to attackers than on imposing costs through retaliation."[83] 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, and for states with advanced cyber offense capabilities – and the concept of cyber arms control may be too problematic for anything meaningful to be agreed.[84] 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, perhaps most importantly, whether attacks can be attributed with enough confidence to elicit a response[85], and what form this response might take if it

---

[81] Andrew Krepinevich, *"Cyber warfare: a nuclear option?",* (Washington DC, Centre for Strategic and Budgetary Assessments: 2012) p.iii

[82] Jason Andres & Steve Winterfeld, *"Cyber warfare: techniques, tactics and tools for security practitioners",* (Waltham MA, Syngress: 2011) p.8

[83] William Lynn, "Defending a new domain: the Pentagon's cyber strategy", *Foreign Affairs,* 89:5 (2010) p.99-100

[84] As Paul Meyer explains, "The lack of defined strategies, transparency of operations and verification capacity, as well as then inherent length of the treaty-making and adoption process, render legally based arms control problematic for addressing cyber-security threats." Paul Meyer, "Cyber-security through arms control: an approach to international cooperation", *The RUSI Journal,* 156:2 (2011) p.22

[85] 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 Sanger & Thom Shanker, "In digital combat, US finds no easy deterrent", *New York Times,* (25 January 2010), http://www.nytimes.com/2010/01/26/world/26cyber.html?pagewanted=all&_r=0. See also, Thomas Rid & Ben Buchanon, "Attributing cyber attacks", *The Journal of Strategic Studies,* (2015)

is to be credible and viable. 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.[86] 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. 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."[87]

If the deterrence of cyber attacks must to be "tailored" to the specific types of threat and attack – ranging from hacking and nuisance to those that cause damage, disruption or destruction – and proportional, this raises the question of what types of response might be required.[88] It also suggests that some types of cyber attack might require asymmetric response – including military force – and that therefore cyber might have to be included in cross-domain deterrence planning. As Siobham 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.[89]

Or in the words of one US military official, "If you shut down our power grid, maybe we put a missile down one of your smokestacks."[90] Such thinking necessarily leads to consideration of whether there might be any role for nuclear weapons in "anchoring" the deterrence ladder and being threatened in the event of a cyber attack of an existential nature. As the 2013 US Defense Science Board argued,

---

[86] See Franklin Kramer, *"Cyberpower and national security: policy recommendations for a strategic framework",* chapter in Franklin Kramer, Stuart Starr & Larry Wentz (Eds.), *"Cyberpower and national security",* (Dulles VA, Potomac Books Inc: 2009) p.15

[87] Richard Kugler, *"Deterrence of cyber attacks",* chapter in Franklin Kramer, Stuart Starr & Larry Wentz (Eds.), *"Cyberpower and national security",* (Dulles VA, Potomac Books Inc: 2009) p.310

[88] It is thought that the United States responded to the hacking of Sony pictures in late 2014 – believed to be by North Korea – by launching an "equivalent" response. As Nicole Perlroth & 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." Nicole Perlroth & David Sanger, "North Korea loses its link to the Internet", *New York Times,* (22 December 2014), http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html

[89] Siobhan Gorman & Julian Barnes, "Cyber combat: act of war", *Wall St Journal,* (31 May 2011), http://www.wsj.com/articles/SB10001424052702304563104576355623135782718

[90] Quoted in Siobhan Gorman & Julian Barnes, "Cyber combat: act of war", *Wall St Journal,* (31 May 2011), http://www.wsj.com/articles/SB10001424052702304563104576355623135782718

> 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 nuclear weapons.[91]

In fact, "For a while it was Russian policy to react to strategic cyber attack with the choice of any strategic weapons in its arsenal"[92] 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."[93]

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 Russia and China 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 advantages – even implicitly – by using cyber as a way to deter and even coerce the United States and our allies.[94]

But, the majority of analysis has questioned the logic of commingling nuclear and cyber weapons. Timothy Farnsworth for example has pointed to five main problems of using nuclear weapons to deter cyber: (1) cyber attacks lack the destructive and existential threat of nuclear weapons; (2) a nuclear response to a cyber attack is not proportional; (3) threatening to respond with nuclear weapons lacks credibility in adversaries eyes; (4) cyber deterrence in general is difficult to achieve, and; (5) the policy would provide a new rationale for nuclear proliferators."[95] Steven Andreasen and Richard Clarke go on to say that "It is hard to see how this cyber-nuclear action-reaction

---

[91] United States Department of Defense, Defense Science Board, "Task force report: resilient military systems and the advanced cyber threat", (January 2013), http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf p.15

[92] Martin Libicki, *"Cyberdeterrence and cyberwar",* (Santa Monica CA, The RAND Corporation: 2009) p.69

[93] "International Strategy for Cyberspace", Office of the President of the United States, (May 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[94] Elbridge Colby, "Cyberwar and the nuclear option", *The National Interest,* (24 June 2013), http://nationalinterest.org/commentary/cyberwar-the-nuclear-option-8638

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

dynamic would improve or US or global security."[96] Given the current 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 two "domains" would appear to offer few benefits and numerous problems. However, 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.[97]

A cyber-nuclear security dilemma

In the past decade, cyber weapons and cyber attacks have become an increasingly important and influential component of conflict – most notably they have been used by the US and Israel against Iran and by Russia in Georgia, Estonia and Ukraine[98] – and while the nature and form that these attacks will continue to take remains uncertain, it seems likely that this trend will continue and be exacerbated as we move into the future.[99] An increased role for cyber weapons and attacks – either one their own or in concert with the use of kinetic military force - is therefore likely to have implications for the nature of conflict and particularly future crisis management between nuclear-armed actors, and seems likely to introduce a range of new destabilizing and unhelpful factors to what is already a complicated concept. While it may not be an existential cyber attack against critical infrastructure, or even direct attacks against nuclear weapons themselves, cyber capabilities will almost certainly be used against opposing military forces in future crises and this will have implications for the role and utility of nuclear forces, strategic balances and for escalation.

There are essentially four key areas that cyber weapons might impact crisis stability between nuclear-armed actors[100]: (1) they can potentially disrupt or destroy communications channels,

---

[96] Steve Andreasen & Richard Clarke, "Cyberwar's threat does not justify a new policy of nuclear deterrence", *The Washington Post,* (14 June 2013), http://www.washingtonpost.com/opinions/cyberwars-threat-does-not-justify-a-new-policy-of-nuclear-deterrence/2013/06/14/91c01bb6-d50e-11e2-a73e-826d299ff459_story.html

[97] In an interview with the author, a former senior UK MoD 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."

[98] The use of cyber alongside other forms of attack is increasingly being labeled as "hybrid warfare".

[99] As the US Defense Science Board has pointed out, "The 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.)." United States Department of Defense, Defense Science Board, "Task force report: resilient military systems and the advanced cyber threat", (January 2013) p.5

[100] This list of adopted from that used by Stephen Cimbala. Stephen Cimbala, *"Nuclear weapons in the information age",* (London, Continuum International Publishing: 2012) pp.56-7

making it difficult to manage forces during a conflict and reducing commanders' confidence in their systems, because "only a small number of attacks would have to be successful to plant seeds of doubt in any information coming from a computer"[101] – or they might include Distributed Denial of Service attacks (DDoS)[102]; (2) they can increase perceived time pressures to act/ respond or to act pre-emptively, 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.[103]

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.[104]

(3) They may reduce the search for viable alternatives, and; (4) they may cause flawed images of intentions and capabilities, exacerbate concerns of "strategic surprise, and create considerable problems for successful "signaling."[105] Taken together these dynamics raise the likelihood of (unintended) and potentially uncontrollable escalation and make the management of such crises more complicated and dangerous.[106] 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. Haim Assa, the designer of the game, later remarked "What we all

---

[101] Peter Singer & Allan Friedman, *"Cybersecurity and cyberwar" what everyone needs to know",* (Oxford, Oxford University Press: 2014) p.129

[102] 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…" Jason Fritz, "Hacking nuclear command and control", *International Commission on Nuclear Non-Proliferation and Disarmament,* (2009), www.icnnd.org/Documents/Jason_Fritz_Hacking_NC2.doc p.2

[103] Stephen Cimbala, *"Nuclear weapons in the information age",* (London, Continuum International Publishing: 2012) p.206

[104] David Gompert & Martin Libicki, "Cyber warfare and Sino-American crisis instability", *Survival,* 56:4 (2014) pp.11-12

[105] According to one senior British Government Official, the ability to clearly signal intentions could be one of the biggest challenges created by cyber for nuclear crisis management. Interview with the author.

[106] Stephen Cimbala, *"Nuclear weapons in the information age",* (London, Continuum International Publishing: 2012) p.205

learned was how quickly localized cyber events can turn dangerously kinetic when leaders are ill-prepared to deal in the cyber domain."[107]

This new cyber-nuclear security dilemma seems most likely to play out in the near future between the United States and NATO, Russia and China. Perhaps the most likely future cyber-nuclear dilemma is between the United States and China in the Asia-Pacific, where both nations have been pretty open about the importance of cyber capabilities and attacks on information systems. As David Gompert and Martin Libicki explain, "China and the US both recognize that an armed conflict with the other would include cyber warfare."[108] More specifically, the US "Air-Sea battle plan "makes no bones about conducting cyber warfare against Chinese kill-chain networks in the event of a conflict,"[109] while at the same time,

> Many analysts now believe that the PLA has already acquired, through its development of strong cyberwar force capabilities, the means to asymmetrically challenge the United States in the event of a kinetic conflict between the two states.[110]

The second potential cyber-nuclear dilemma, especially given their recent and very obvious use of cyber capabilities, is likely to be between the US, its NATO allies and Russia. In fact, as part of its 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,

> … the alliances hallowed article 5 – which says an attack on one member is an attack against all – applies equally to virtual attacks as to physical ones … NATO is now taking cyber threats as seriously as the Russian tanks and nuclear weapons it was created to deter.[111]

---

[107] Barbara Opall-Rome, "Israeli cyber game drags US, Russia to brink of Mideast war", *Defense News,* (14 November 2013), http://www.defensenews.com/article/20131115/C4ISRNET07/311150020/Israeli-Cyber-Game-Drags-US-Russia-Brink-Mideast-War

[108] David Gompert & Martin Libicki, "Cyber warfare and Sino-American crisis instability", *Survival,* 56:4 (2014) p.10

[109] David Gompert & Martin Libicki, "Cyber warfare and Sino-American crisis instability", *Survival,* 56:4 (2014) p.16

[110] George Patterson Manson, "Cyberwar: the United States and China prepare for the next generation of conflict", *Comparative Strategy,* 30:2 (2011) p.122. Moreover, as David Gompert and Martin Libicki points out, "The Chinese know that computer networks are crucial to US capabilities and strategy in the Western Pacific, and that targeting them could have decisive effects on a conflict." David Gompert & Martin Libicki, "Cyber warfare and Sino-American crisis instability", *Survival,* 56:4 (2014) p.16

[111] Sidney Freedberg, "NATO hews to strategic ambiguity on cyber deterrence", *Breaking Defense,* (7 November 2014), http://breakingdefense.com/2014/11/natos-hews-to-strategic-ambiguity-on-cyber-deterrence/

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."[112] While it remains unclear at "what threshold collective defense will be triggered, and how this threshold will be measured"[113], current NATO thinking appears to suggest "that some cyber attacks could have the same level of disruption on Nato countries and economies as conventional warfare."[114] It is important to remember that NATO deterrence thinking remains "anchored" by nuclear weapons.

While the emergence of cyber weapons and attacks in these strategic nuclear relationships does not necessarily mean the next crisis will become unmanageable and lead to disaster, it clearly will make a safe and peaceful resolution more complicated. As Ashton Carter has 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."[115]

Conclusion: putting the cyber risk in perspective

Cyber weapons will not supersede nuclear weapons or become strategic tools of warfare any time soon, but this does not mean that new technological developments are not having a significant impact across the nuclear weapons enterprise. If we take cyber as a holistic concept that includes not just the Internet, but also software, hardware, other infrastructure and the people that operate these systems, then the challenge of the cyber age is in fact multifaceted, albeit in some cases more subtle and exacerbating rather than transforming established nuclear tensions and problems. One notable dynamic here is the inherent complications of relying upon increasingly sophisticated and complex technology in nuclear management, and particularly in nuclear command and control. The nuclear past is littered with examples of near misses and accidents – many of which can be either directly or indirectly attributed to computers and software – and this seems only likely to increase as nuclear-armed states strive for more sophisticated and complex management systems. Normal

---

[112] Sam Jones, "Nato holds largest cyber war games", *Financial Times,* (20 November 2014), http://www.ft.com/cms/s/0/9c46a600-70c5-11e4-8113-00144feabdc0.html#axzz3NIsB8FG2

[113] Sidney Freedberg, "NATO hews to strategic ambiguity on cyber deterrence", *Breaking Defense,* (7 November 2014), http://breakingdefense.com/2014/11/natos-hews-to-strategic-ambiguity-on-cyber-deterrence/

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

[115] Ashton Carter, *"Sources of error and uncertainty",* chapter in Ashton Carter, John Steinbruner & Charles Zraket (Eds.), *"Managing nuclear operations",* (Washington, DC, Brookings Institution Press: 1987) p.612

nuclear accidents – without the need for any attack – must therefore remain a key topic of study in the cyber age, and more complex systems mean more potential vulnerabilities that could be exploited by a would-be attacker.

Cyber nuclear espionage is a significant problem that has grown considerably over the past two decades and clearly has implications not just for proliferation of nuclear knowhow, but also for the efficacy of systems (nuclear and non-nuclear) in any future crisis scenario. Given the enormous amounts of data involved, it is most likely that this problem can really only be managed rather than eradicated. Likewise, the Stuxnet virus demonstrated just how real the threat of sabotage and destruction is, although this was a highly complex piece of malware that took many years to develop and required considerable prior knowledge. As such, the strategic sabotage of critical infrastructure or of the nuclear weapons enterprise remains very difficult to mount, and perhaps impossible in reality at the time of writing. That said, Stuxnet is likely just the tip of the iceberg and the development of new technologies that might compromise and even destroy systems will undoubtedly improve in time. The threat of a terrorist attack on a nuclear weapon or weapons facility in this manner is an ever-present possibility – although power plants or key infrastructure may prove more attractive targets. While mechanisms to protect key nuclear infrastructure against cyber attack can certainly be enacted, these are not foolproof and are likely to be costly.

Given the current shape of the cyber challenge, using nuclear weapons to deter a cyber attack is neither an attractive nor useful idea, although it could prove to be so in the future. Part of the reason for this is that cyber and nuclear are fundamentally different, and while the difficulties of cyber defence and cyber arms control mean that some type of deterrence should almost certainly be used, this does not currently need to include nuclear weapons. Doing so would probably lack credibility and would do little for wider non-proliferation and arms control efforts given the nature of the current threat. That said, cyber will undoubtedly further muddy the waters of crisis stability between nuclear-armed actors, and present new challenges for risk management, communication and signaling. The development of a new "cyber-nuclear security dilemma" could therefore be one of the most dangerous developments in the cyber-nuclear nexus in the coming years.