The Cyber-Nuclear Nexus and Threats to Strategic Stability

Muhammad Shoaib

Introduction

Cyber-attacks have become a threat to both national and international security as the number and sophistication of such attacks have increased due to open access to cyber technology. The perpetrators are not only private hackers or criminals but also nation states. Cyber-attacks are not limited against computer systems and networks but they can also target instruments and control systems making them equally vulnerable to damage from such attacks. Nuclear facilities have become heavily dependent on digital control systems or computer based information systems (IS). This is because digitalisation of operational functions and working processes increases the quality and efficiency of these facilitites. This development raises new threats for nuclear facilities as they still remain vulnerable in the area of process control and automation systems.

According to observers, the nexus of cyber and nuclear technologies creates challenges related to the security of nuclear weapons. This in turn impacts strategic stability.[1] For example, in July 2017, the US Department of Homeland Security and the Federal Bureau of Investigation issued a report stating that hackers have been targeting US' nuclear facilities.[2] Similarly, in 2010, the 'Stuxnet' computer worm damaged uranium enrichment centrifuges at Iran's Natanz nuclear site.[3]

The dynamics of and developments in cyberspace are changing and aggravating tensions across the nuclear domain, through both threats and challenges. These

include threats to safe, secure and reliable command and control of nuclear forces, the threat of nuclear accidents, as well as proliferation. Cyber-power poses challenges to the safeguarding of highly sensitive nuclear secrets and may result in complications for strategic deterrence. Therefore, the emergence of a cyber-nuclear security dilemma must be considered when examining future crisis stability and management. Cyber-attacks pose different challenges to nuclear weapons enterprise including espionage and threats to systems and information security, to sabotage and the risk of interference, destruction or even unauthorised nuclear use. The actors involved, and their intentions, also vary, particularly with regard to the differences between the dangers posed by non-state actors and by nation states.
The growing rhetoric highlights challenges and threats due to increasing dependency on cyber technology and has started perturbing nuclear strategists and policy makers.[4] Both nuclear and conventional weapons systems of today are complex and interconnected while depending on digital technologies for the management and functioning of these systems. This means the systems remain vulnerable to digital interference due to their reliance on digital transmission, reception and management of data. Cyber threat in the nuclear domain can be studied at two levels: one, security of nuclear weapons and facilities; and two, threats to strategic stability.

This study would examine the implications of cyber threats to nuclear weapons and related systems. It would include two dimensions of cyber-nuclear nexus: firstly, the challenges to nuclear security in the cyber-age; and secondly the impact of cyber-technology on strategic stability. In order to elaborate on these dimensions, this paper would address the following questions: What are the effects of cyber technology on nuclear security?;

Does cyber technology pose a threat to strategic stability and do nuclear weapons provide effective deterrence against cyber threats? What could be done to strengthen deterrence against cyber threats?

Secondary sources of data collection would be used, primarily from published journals, books and newspaper articles, from both print and online publications. The study would only focus on the challenges related to nuclear weapons in the cyber-age including impact on strategic stability and nuclear security. The concepts of cyberspace, cyber-war, and cyber-weapons etc. would not be explained as they were explained in a previous study.[5] Western perspective dominates the existing literature on the subject.

Understanding Threats and Challenges

During the last few years, negative uses and effects of cyberspace have become more recognisable. Cyber risks should be considered one of the most rapidly evolving global threats today. Information and Communication Technologies (ICTs) have become a fundamental part of daily life for a majority of the people, as well as a basis for innovation and economic growth. These technologies have enormous benefits in the nuclear field. However, they also entail substantial risks, as the information they contain or convey can be accessed and used for criminal purposes. The number, scale, and impact of cyber-attacks is on the rise. Due to the reliance of all economic activities on the internet, the level of concern about the high vulnerability of this domain has also increased.

For states, preventing cyber-attacks has become an important and strategic challenge as well as a national security issue that could potentially impact not only the nuclear sector, but all societal sectors. There is a

possibility of deliberate or unintended cyber-attacks by state or non-state actors which raises concerns about current and future risks in the cyber domain. Potential risks include: the risk of disruption in facility operation; damage to physical facilities; espionage (commercial and political); interference with critical infrastructure ("CI")[6]; potential radiological incident; erosion of public confidence in nuclear energy; and theft of nuclear or other radioactive material.[7]

Moreover, the lack of information and accurate attribution in the event of successful cyber-attacks could spark bilateral, regional or international conflict among states. Even more seriously, such an attack could potentially develop into a conflict between or among nuclear-weapon states. Developments in ICTs also increase cyber vulnerabilities. Cyber-attacks could be very complex and dynamic. Malware[8] can go through extensive evolution over time and can be reused, resulting in new vulnerabilities. Cyber-attacks involving malware can often reach beyond the target for which they were intended, easily spreading into public networks. Such malware could fall into the hands of different users and could be used for the development of other new malware.[9]

Although the distinct threat of hacking and attacks through the internet are important, they do not present the only dynamics that would 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.[10] More importantly, this approach also allows for a consideration of what is new and what is not when understanding the cyber phenomenon. In

this way cyber-attacks on nuclear weapons infrastructure could 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 information.[11] 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] by those with close physical access to systems. This could be done either intentionally or unknowingly. Cyber-attacks could also be directed against the information on which these systems and human operators act and make their decisions, such as by altering key information sets and data.[13]

The cyber challenge therefore also incorporates natural problems inherent in increasingly complex computer systems, such as badly written software or programme 'bugs'[14], and the overall uncertainty and risk of whether key systems will always work as expected. Therefore, 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 and people 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 and computers do not behave independently but what they are programmed to do. As human beings are complex having their own agendas or can be influenced in terms of their beliefs, loyalties and

priorities, they cannot always be trusted. Therefore, nuclear weapons systems and their functioning remain vulnerable to human interference.

Challenges to Nuclear Weapons

In order to comprehend the challenges to nuclear weapons enterprise, it is necessary to look at all aspects of the cyber phenomenon and consider it in its broadest scope and across all the domains, in addition to the primarily logical domain of Computer Network Operations (CNOs).[16] Therefore it is important to consider the impact that the broader cyber environment is having on nuclear thinking and strategy by treating cyber as an operational domain, an offensive capability, and a societal development.

Nuclear Command and Control (C2) systems have always been susceptible to outside interference, attack and possible sabotage, and there have been abundant cases where miscalculations, accidents and near misses (many of which were caused by computers and electronic systems) were observed. 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).[17] As Peter Feaver, Professor of Political Science and public policy at Duke University, explains, "At the heart of nuclear command and control lies the always / never dilemma.[18] 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 authorised 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 unauthorised people to detonate them."[19]

Despite many protective mechanisms (such as, among others, Permissive Actions Links, dual phenomenology, encryption, redundancy, and in some cases a 'two-man rule'[20]), this central problem of nuclear C2 means that weapons would never be invulnerable, and would always be susceptible to attackers 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.[21] 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.[22] 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 digitalisation, 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.

The vulnerabilities and problems that are inherent within nuclear C2 systems are best demonstrated by the number of accidents, near misses and miscalculations in the past.[23] The 'normal accidents' theory posits that complex systems, particularly computer systems, would not

always work as intended and naturally go wrong some of the time,[24] 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, a Professor of Political Science and Business at Yale University, "In a world of experience we feel complex systems are bound to go awry precisely because they are so complex".[25] 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. As Ross Anderson, a Professor of Security Engineering at the Computer Laboratory, University of Cambridge, 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."[26]

According to Scott Sagan, a professor of Political Science at Stanford University and Senior Fellow at Stanford's Centre for International Security and Cooperation, 'from a normal accidents perspective, the fact that there has never been an accidental nuclear weapons detonation or an accidental nuclear war is surprising'.[27] 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 and digitised. As Soviet physicist Boris Rauschenbach said, 'In terms of potential nuclear war, the very existence of mankind is becoming dependent on hardware and software'.[28] Perhaps the most notable normal accidents

in the nuclear realm occurred at the US North American Air/Aerospace Defence Command (NORAD)[29] between 1979 and 1984.[30] 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.[31]

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.[32] In 1984, a computer malfunction indicated that a US nuclear-armed missile was about to fire.[33] 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.[34] This risk of accidents and other problems is only likely to grow as nuclear-armed actors come to rely more on computers and complex systems for nuclear weapons management.[35]

Perhaps more importantly, they also provide an insight into how systems might be hacked. According to Peter Neumann, an expert on terrorism and political violence, 'If an event can happen accidentally, it often could be caused intentionally.'[36] 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.[37] 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. Martin Libicki, a scholar and Professor at the Frederick S. Pardee RAND Graduate School in Santa Monica, California 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."[38]

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'[39], can now be purchased on the black market.[40] 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.[41] 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.

While nuclear systems and especially C2 are among the best protected against cyber threats and almost certainly air-gapped[42] from the wider internet, they are by no means invulnerable. 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 procedures. This is the natural result of an increase in the number of vulnerabilities in nuclear related software that could be exploited by an attacker, both directly within nuclear C2 systems, and indirectly inside the various systems and infrastructure that supports nuclear weapons management. Although hacking into weapons software directly would probably be very difficult, the increase in the number of vulnerabilities and ways in to operational software and the systems used for nuclear C2 is a serious threat.

While the cyber challenge varies across nuclear actors and systems, the less sophisticated a system is, the less vulnerable it would be to cyber-attack.[43] 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.[44] These new challenges associated with cyber have considerable implications across the nuclear weapons domain, as well as for the global nuclear order.

Threats to Nuclear Security

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. 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. The biggest challenge of the cyber age is the threat of espionage, and the new measures that are required to protect sensitive nuclear information, such as weapons designs or operational procedures.[45] Another challenge 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[46], Aurora Generator Test[47], Operation Orchard[48] and Stuxnet all demonstrate the possibility of interfering with, or damaging, nuclear systems through cyber means.

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. The importance of nuclear espionage can be traced as far back as the early 1940s as Soviet spies sought information on the Manhattan Project and early US nuclear bomb designs.[49] 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.

The nature of the threat posed not only involves hacking into secret systems and downloading and copying information over the internet and from remote locations, but also compromising the computer and information

security in those systems that may already be air-gapped, or separated from the internet. Both issues are serious 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 using a USB drive or in some other digital format. 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.

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 defence and military establishments.[50] 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 Defence Initiative (SDI).[51] It later transpired that Hess had been working for the Soviet KGB.

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.[52] 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.[53] The activity was termed as an act of espionage.

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.[54] In 2008 an infected USB memory stick 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.[55] In February 2011, the Zeus was discovered, an information-stealing Trojan aimed at contractors involved in building the UK Trident nuclear-armed submarine force.[56]

Operation Olympic Games, which produced the Stuxnet, began primarily as an intelligence-gathering and espionage operation against Iranian nuclear activities.[57] 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.[58]

While the volume of cyber spying and the attempted theft of a wide variety of nuclear secrets has increased manifold 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 weapons programmes. Moving 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. 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.[59] 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 a classic example of this. 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.

Threat of Sabotage and Spoofing

The cyber age 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.[60] 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.[61] While nuclear weapons systems are certainly likely to be far better protected against sabotage and attack than commercial infrastructure, the threat is real manifesting across the nuclear weapons domain. As a US Defence Science Board report warned in 2013, 'US nuclear weapons may be vulnerable to highly sophisticated cyberattacks'.[62]

Ultimately, this is also likely to be true for other nuclear-armed actors.[63]

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 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 also 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.[64] That said, even protecting systems built 'in house' are not straightforward, and some vulnerabilities may simply be the result of accidents, bugs or unanticipated circumstances.

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.[65] 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',[66] 'contrived computer chips found their way into Soviet military equipment' and the 'Pentagon introduced misleading information pertinent to stealth aircraft, space defence and tactical aircraft'.[67] While the extent of the operation remains disputed,[68] 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.[69] More recently, and while the majority of attention remains 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, an expert on Iran's nuclear programme at the Woodrow Wilson International Center for Scholars in Washington, it seems to be clear that there is an active and imaginative sabotage programme 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.[70]

During the 1990s, the US and Israel 'modified' vacuum pumps purchased by Iran to make those pumps break down;[71] in 2012, Iranian lawmaker Alaeddin Boroujerdi accused the German company Siemens of planting tiny explosives inside equipment that Iran had purchased for its disputed nuclear programme;[72] 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';[73] and a huge explosion at the Parchin military base in October 2014 again raised the question of sabotage.[74] Similar techniques have also been used by various governments to bolster counter-proliferation efforts against certain states seeking nuclear capabilities.
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,[75] but the nature of this challenge is also changing in the cyber age. A good example of this is 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.[76] 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'.[77] 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. 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.[78] The Syrian radar system was likely purchased from Russia and is currently being used by a number of other states including Iran.[79] While this attack was fairly limited, it nevertheless provides a stark warning of new types of vulnerabilities, particularly for key nuclear communications and early-warning systems.[80] 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.[81] 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'.[82]

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 have only been a handful of cyber-attacks that have caused physical destruction and are publicly known,[83] and only one – Stuxnet – that has caused direct damage to a nuclear facility.[84] The Stuxnet worms were designed to attack the Supervisory Control and Data Acquisition (SCADA)[85] 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.[86] According to one of the architects of the attack, speaking to Chief Washington correspondent for The New York Times David Sanger, 'the thinking was that the Iranians would blame bad parts, or bad engineering, or just incompetence'.[87] 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.[88] Stuxnet has been credited with causing damage to centrifuges and delaying any Iranian bomb,[89] 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.

Even as Stuxnet represented a major development in cyber capabilities and the Operation Orchard demonstrated the vulnerabilities of early warning and communications, the direct threat of cyber sabotage to the nuclear enterprise remains limited. Certain 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. 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. 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."[90]

Implications for Strategic Stability

The various dynamics and challenges to nuclear security and command and control that are being driven, shaped and aggravated by the growth of cyber threats would also have implications for strategic stability, nuclear strategy and crisis management. This can be observed on two levels. First, discrete and focused cyber-attacks against nuclear systems and associated infrastructure may ultimately impact strategic stability and crisis management.[91] In part this is due to the emergence of a cyber-nuclear security dilemma whereby the challenges described in the previous sections must be considered important in how future crises are managed and how unintended escalation 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 of states. While a policy seeking to deter cyber-attacks through nuclear retaliation is 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 would remain linked.[92]

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 would take in the future remains unclear, it is likely that this trend would continue and develop. While cyber may be viewed by some as a separate domain from other forms of military power, and especially with regard to nuclear weapons, in reality cyber cannot be separated from these other dynamics and it will therefore play a role in future nuclear-related decisions and strategic balances.

This increased role for cyber-attacks, either on their own or in combination with the use of traditional kinetic military force, would probably alter the nature of conflict, strategic stability and particularly future crisis management between nuclear-armed actors.[93] This will likely introduce a range of new destabilising factors to strategic stability. 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, would have implications for the role and perceived utility of nuclear forces, strategic balances, perceptions and risks, as well as having potential force multiplier implications.

Several key areas can be identified where cyber-attacks may influence crisis stability between nuclear-armed actors. First, during a crisis, a hacker could potentially disrupt or destroy communications channels,[94] making it difficult to manage nuclear forces and reducing commanders' confidence in their systems. According to authors 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'.[95] 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.[96] 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, Professor of Political Science at Penn State Brandywine, explains, "A nuclear-armed state faced with a sudden burst of holes in its vital warning and response systems might, for example, press the pre-emption button instead of waiting to ride out the attack and retaliate."[97]

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 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 further concerns over strategic surprise. It is quite understandable to see this as the beginning of a possible transition to a condition of mutually unassured destruction (MUD): where states may no longer feel that they would always be able to threaten nuclear retaliation to deter nuclear attack.[98] Taken together, these dynamics raise the likelihood of unintended and potentially uncontrollable escalation and

make the management of nuclear crises more complicated and dangerous.[99]

Conclusion

Cyber weapons alone would not supersede nuclear weapons as strategic tools of deterrence and warfare. However, cyber in combination with nuclear weapons poses threats and also makes latter more vulnerable in terms of its security and strategic stability. Cyber-nuclear espionage is a significant problem that has implications not just for nuclear proliferation, but also for the efficacy of weapons systems in any crisis scenario. This problem can only be managed and not eradicated due to the involvement of enormous amounts of data. With improvements overtime, the development of new cyber technologies might compromise and even completely destroy systems. Therefore, the threat of a terrorist attack on a nuclear weapon or weapons facility also remains a possibility. While mechanisms to protect key nuclear infrastructure against cyber-attack can certainly be enacted, these are not fool proof and are likely to be costly.

Offensive cyber operations against nuclear C2 can raise the risks of nuclear war. This is because of the informational properties of both cyber operations and nuclear weapons. Offensive cyber operations rely on secrecy. Nuclear deterrence, however, relies on transparency. In a brinksmanship crisis, the former undermines the latter. For many years, the high cost of nuclear war and the distinctive transparency of the nuclear balance ensured that nuclear weapons were not used. To maintain this nuclear stability, it would be necessary to find ways to maintain transparency. New cyber technologies are undermining this transparency, as offensive cyber operations offer a means to covertly

defeat an adversary's deterrent capabilities. Nuclear C2 would remain a particularly attractive counterforce target because disruption can render the enemy's arsenal less effective without having to destroy individual platforms.

Using nuclear weapons to deter a cyber-attack is not useful because cyber and nuclear are fundamentally different. Therefore, arms control agreements to curtail offensive cyber operations against nuclear C2 might not work, due to the dependence of cyber on secrecy and deception making monitoring and enforcement difficult. There are a few options that could be considered and pursued to help minimise the impact and risks of cyber for nuclear weapons and strategic stability. Cyber threats vary in nature 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. Following this, it might become easier to establish certain norms or rules in the cyber-nuclear domain, and to pursue certain confidence-building measures, such as sharing data on non-state or third-party threats, and even sharing good practice. Another recommendation for all nuclear-armed states would be to work to protect nuclear systems against direct cyber-attack through better network defences, firewalls and physical security. This may include upgrading nuclear infrastructure, developing secure 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 include efforts to keep nuclear C2 systems relatively simple and separate from the C2 systems used for conventional operations.

The leaders of nuclear-armed countries should 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 agreements between states not to target each other's nuclear C2 systems with cyber weapons.

References

1. Erik Gartzke and Jon R. Lindsay, "Thermonuclear Cyberwar," June 15, 2016, http://dx.doi.org/10.2139/ssrn.2836208.
2. Nicole Perlroth, Hackers are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say, *The New York Times,* July 6, 2017, https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html?mcubz=0&module=ArrowsNav&contentCollection=Technology&action=keypress&region=FixedLeft&pgtype=article.
3. James P. Farwell, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (February-March 2011), quoted in Muhammad Shoaib, "Conceptualising Cyber-Security: Warfare and Deterrence in Cyberspace," *Journal of Strategic Affairs* 2, no. 1 (Summer 2017).
4. Andrew Futter, "Cyber Threats and Nuclear Weapons," Occasional Paper, *Royal United Services Institute for Defence and Security Studies,* July 2016, https://rusi.org/sites/default/files/cyber_threats_and_nuclear_combined.1.pdf.
5. See: Muhammad Shoaib, "Conceptualising Cyber-Security: Warfare and Deterrence in Cyberspace," *Journal of Strategic Affairs* 2, no. 1 (Summer 2017).
6. "Critical infrastructure" refers to essential services and sectors that are the backbone of every nation's economy, security and health.
7. Vesselin Giaurov, The Cyber-Nuclear Security Threat: Managing the Risks, Vienna Centre for Disarmament and Non-Proliferation, January 2017, http://nonproliferation.eu.

8. Malware (Malicious software) is a software programme specifically designed to disrupt, damage, or gain authorised access to a computer system. It includes computer viruses, worms, Trojan horses and spyware.
9. Alexander Klimburg, National Cyber Security Framework Manual, CCDCOE, 2012, https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.
10. Jason Andres & Steve Winterfield, "Cyber warfare: techniques, tactics and tools for security practitioners", (Waltham MA: Syngress, 2011), 167.
11. Andrew Futter, "Hacking the Bomb: Nuclear Weapons in the Cyber Age," Working paper for ISA Annual Conference, New Orleans, February 2015. https://www2.le.ac.uk/.../afutter/copy_of_AFutterHackingtheBombISAPaper2015.pdf.
12. In computing, a Trojan horse, or Trojan, is any malicious computer programme which misleads users of its true intent.
13. Futter, "Hacking the Bomb."
14. Bugs are unintended errors in software and coding and not "cyber-attacks".
15. Futter, "Hacking the Bomb".
16. Computer network operation (CNO) is a broad military computing concept that encompasses tools, processes and methodologies to utilise, optimise and gain strategic advantages from computer networks.
17. Futter, "Cyber Threats".
18. 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).
19. Peter Feaver, "Command and Control in Emerging Nuclear Nations," *International Security* 17, no. 3 (1992), http://www.jstor.org/stable/2539133.
20. Gerald Johnson, "Safety, Security and Control of Nuclear Weapons" in *Technology and the Limitation of International Conflict* ed. Barry Blechman (Washington DC: Foreign Policy Institute, Johns Hopkins University, 1989), 145, http://bupytuu.ru/gekukov.pdf.

21. 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'.
22. US Department of Defence, Office of the Assistant Secretary of Defence for Nuclear, Chemical, and Biological Defence Programmes, *The Nuclear Matters Handbook 2011*, https://fas.org/man/eprint/NMHB2011.pdf.
23. Shaun Gregory, *The Hidden Cost of Nuclear Deterrence: Nuclear Weapons Accidents* (London: Brassey's, 1990).
24. Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (Princeton NJ: Princeton University Press, 1999), http://www.jstor.org/stable/j.ctt7srgf.
25. Paul Bracken, "Instabilities in the Control of Nuclear Forces" in *Breakthrough: Emerging New Thinking: Soviet and Western Scholars Issue a Challenge to Build a World Beyond War*, eds. Anatoly Gromyko and Martin Hellman (New York: Walker & Company Inc, 1988), 23.
26. Ross Anderson, *Security Engineering: a Guide to Building Dependable Distributed Systems* (Indianapolis IN: Wiley Publishing, 2008), http://www.cl.cam.ac.uk/~rja14/book.html.
27. Scott Sagan, *The Limits of Safety: Organizations, Accidents and Nuclear Weapons* (Princeton NJ: Princeton University Press, 1993), 45, www.mwftr.com/CS2/The%20limitation%20of%20Safety-Chapter%201.pdf.
28. Boris Raushenbach, "Computer War" in *Breakthrough* eds. Anatoly Gromyko and Martin Hellman (New York: Walker & Company Inc, 1988), 47, https://www-ee.stanford.edu/~hellman/Breakthrough/book/pdfs/breakthrough.pdf.
29. In 1981, NORAD was renamed, and Air Defence became Aerospace Defence.
30. Gordon Corera, *Intercept: The Secret History of Computers and Spies* (London: Weidenfeld and Nicholson, 2015), 71-72, smtp.nist.pk/intercept-by-gordon-corera.pdf; 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.

31. William Broad, "Computers and the Military Don't Mix," *Science* 207, no. 14 (1980): 1183, http://science.sciencemag.org/content/207/4436/1183.
32. US General Accounting Office, *NORAD's Missile Warning System: What Went Wrong?*, May 5, 1981, 13, http://www.gao.gov/assets/140/133240.pdf.
33. Gregory, *The Hidden Cost*, 97.
34. Eric Schlosser, "Neglecting our Nukes," Politico, September 16, 2013, https://www.politico.com/story/2013/09/neglecting-our-nukes-096854; 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*, November 11, 2010, http://content.time.com/time/nation/article/0,8599,2030685,00.html.
35. Christopher Stubbs, "The Interplay between Cultural and Military Nuclear Risk Assessment" in *The Nuclear Enterprise: High Consequence Accidents: How to Enhance Safety and Minimize Risks in Nuclear Weapons and Reactors*, eds. George Shultz and Sidney Drell (Stanford CA: Hoover Institution Press, 2012), 228.
36. Peter Neumann, *Computer Related Risks* (New York NY: Addison-Wesley Publishing Company, 1995), 126.
37. Martin C Libicki, *Conquest in Cyberspace* (New York: Cambridge University Press, 2007), 40.
38. Ibid.
39. Zero-day expoits are vulnerabilities that are yet to be discovered.
40. Andy Greenberg, "Shopping for Zero-Days: a Price List for Hackers' Secret Software Exploits," *Forbes*, March 23, 2013, https://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/#62ec71c62660.
41. Liam O'Murchu, "Stuxnet Using Three Additional Zero-Day Vulnerabilities," *Symantec Official Blog*, September 14, 2010, https://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities.

42. 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.
43. John Reed, "Keeping Nukes Safe from Cyber Attack," *Foreign Policy*, September 25, 2012, http://foreignpolicy.com/2012/09/25/keeping-nukes-safe-from-cyber-attack/.
44. Peter Hayes, "Nuclear command-and-control in the Millennials era," NAPSNet Special Reports, Nautilus Institute for Security and Sustainability, February 17, 2015, https://nautilus.org/napsnet/napsnet-special-reports/nuclear-command-and-control-in-the-millenials-era/.
45. Futter, "Cyber Threats".
46. It was a campaign by the CIA where computer sabotage resulted in a huge explosion in Siberia in 1982. See The Farewell Dossier, *The New York Times*, February 2, 2004, http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html.
47. It was a demonstration test in 2007 using computer programme to show how cyber technology can be used to destroy physical components of an electric grid. See Jeanne Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid," *CNN*, September 26, 2007, http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html.
48. In 2007, Israeli jets conducted airstrikes against a suspected Syrian nuclear reactor. Israel used its electronic warfare capabilities to take over Syrian air defence systems and fed them false information. See David Cenciotti, "Syria Never Stood A Chance Against Israel's Electronic Warfare," February 3, 2013, http://www.businessinsider.com/israeli-electronic-warfare-in-syria-2013-2.
49. Mike Rossiter, *The Spy Who Changed the World* (London: Headline, 2015).
50. 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* 27, no. 5 (2012): 784, https://doi.org/10.1080/02684527.2012.708530.

51. Clifford Stoll, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage (London: Doubleday, 1989).
52. Dorothy Denning, *Information Warfare and Security* (Reading, MA: Addison-Wesley, 1999).
53. Select Committee US House of Representatives, "Report of the Select Committee on US National Security and Military/Commercial Concerns with the Republic of China," May 25, 1999, https://www.gpo.gov/fdsys/pkg/GPO-CRPT-105hrpt851/html/ch2bod.html#anchor4311396.
54. Eric Follarth and Holger Stark, "The Story of Operation Orchard: How Israel Destroyed Syria's Al Kibar Nuclear Reactor," *Spiegel Online*, November 2, 2009, http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html.
55. Karl Grindal, "Operation Buckshot Yankee" in *A Fierce* Domain ed. Jason Healey (Vienna, VA: Cyber Conflict Studies Association, 2013), 208.
56. Richard Norton-Taylor and Julian Borger, "Chinese Cyber-Spies Penetrate Foreign Office Computers," *The Guardian*, February 4, 2011, https://www.theguardian.com/world/2011/feb/04/chinese-super-spies-foreign-office-computers.
57. Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York, NY: Crown Publishers, 2014), 321.
58. Uzi Mahnaimi, "Fake Rock Spying Device Blows up Near Iranian Nuclear Site," *Sunday Times*, September 23, 2012, https://www.thetimes.co.uk/article/fake-rock-spying-device-blows-up-near-iranian-nuclear-site-5l6wqt3z27z.
59. Catherine Collins and Douglas Frantz, "Down the Nuclear Rabbit Hole," *Los Angeles Times*, January 3, 2011,

http://articles.latimes.com/2011/jan/03/opinion/la-oe-frantz-khan-20110103.

60. Futter, "Cyber Threats."
61. Ibid.
62. Timothy Farnsworth, "Study Sees Cyber Risk for U.S. Arsenal," *Arms Control Today*, April 2, 2013, Timothy Farnsworth, 'Study Sees Cyber Risk for U.S. Arsenal', Arms Control.
63. 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," *The Nonproliferation Review* 23, no. 5-6 (2016), https://doi.org/10.1080/10736700.2017.1346834.
64. Anderson, *Security Engineering*, 645.
65. Alec Russell, "CIA plot led to huge blast in Siberian gas pipeline," *The Telegraph*, February 28, 2004, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html.
66. Thomas Reed and Danny Stillman, *The Nuclear Express: A Political History of the Bomb and Its Proliferation* (Minneapolis, MN: Zenith Press, 2009), 274.
67. Gus Weiss, "Duping the Soviets: the Farewell Dossier," *Studies in Intelligence* 39, no. 5 (1996): 125, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm.
68. See, for example, Anatoly Medetsky, "KGB Veteran Denies CIA Caused 82 Blast," *Moscow Times*, March 18, 2004, http://oldtmt.vedomosti.ru/sitemap/free/2004/3/article/kgb-veteran-denies-cia-caused-82-blast/232261.html.
69. Thomas Reed, *At the Abyss: an Insider's History of the Cold War* (New York, NY: Presidio Press, 2007).
70. Eli Lake, "Operation Sabotage," *New Republic*, July 14, 2010, https://newrepublic.com/article/75952/operation-sabotage.

71. David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York NY: Broadway Paperbacks, 2013), 194.
72. Iran accuses Siemens of nuclear sabotage, *The Times of Israel*, September 22, 2012, https://www.timesofisrael.com/iran-accuses-siemens-of-nuclear-sabotage/.
73. David Sanger, "Explosion at Key Military Base in Iran Raises Questions About Sabotage," *New York Times*, October 9, 2014, https://www.nytimes.com/2014/10/10/world/explosion-at-key-military-base-in-iran-raises-questions-about-sabotage.html.
74. Ibid.
75. 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.
76. David Fulghum, "Why Syria's Air Defences Failed to Detect Israelis," *Aviation Week*, November 12, 2013, https://www.strategypage.com/militaryforums/512-40367.aspx#startofcomments.
77. Ibid.
78. Richard Clarke and Robert Knake, *Cyber War: the Next Threat to National Security and What to Do About It* (New York, NY: HarperCollins, 2010).
79. John Leyden, "Israel Suspected of "Hacking" Syrian Air Defences: Did Algorithms Clear Path for Air Raid?," *The Register*, October 4, 2007, https://www.theregister.co.uk/2007/10/04/radar_hack_raid/.
80. Jim Michaels, "US Could Use Cyberattack on Syrian Air Defenses," *USA Today*, May 16, 2013, https://www.usatoday.com/story/news/world/2013/05/16/syria-attack-pentagon-air-force-military/2166439/.
81. Jason Fritz, "Hacking Nuclear Command and Control," *International Commission on Nuclear Non-proliferation and disarmament*, 2009, www.icnnd.org/Documents/Jason_Fritz_Hacking_NC2.pdf.
82. "Hacked Israeli Military Twitter Account Declared Nuclear Leak," *Global Security Newswire*, July 7, 2014,

http://www.nti.org/gsn/article/hack-israeli-military-account-erroneous-post-announcesnuclear-leak/.

83. Christopher Bronk and Eneken Tikk-Ringas, 'The Cyber Attack on Saudi Aramco," *Survival* 55, no. 2 (2013), https://doi.org/10.1080/00396338.2013.784468; and Kim Zetter, "A Cyberattack Has Caused Confirmed Damage for the Second Time Ever," *Wired*, anuary 8, 2015, https://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

84. Salvador Rodriguez, "US Tried, Failed to Sabotage North Korea Nuclear Weapons Programme with Stuxnet-Style Cyber Attack," *International Business Times*, May 29, 2015, http://www.ibtimes.com/us-tried-failed-sabotage-north-korea-nuclear-weapons-program-stuxnet-style-cyber-1945012.

85. SCADA is an industrial automation control system at the core of many modern industries. Multiple software and hardware elements are deployed to monitor, gather, and process data and to connect to and control machines etc, See https://inductiveautomation.com/what-is-scada.

86. Zetter, *Countdown to Zero Day*.

87. Sanger, *Confront and Conceal*, 188.

88. Jon Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 381, https://doi.org/10.1080/09636412.2013.816122.

89. 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, December 22, 2010, http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.

90. 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 Authorisation Request For Fiscal Year 2014 and the Future Years Defence Programme," 113th Congress, March 12, 2013, https://www.armed-services.senate.gov/hearings/15-03-

19-us-strategic-command-us-transportation-command-and-us-cyber-command.

91. Futter, "Cyber Threats."
92. Ibid.
93. Ibid.
94. 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*, April 29, 2015, https://apnews.com/2ae0a33fa1c7402999afb6d55046e2cc
95. PW Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 155.
96. 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."
97. Stephen Cimbala, *Nuclear Weapons in the Information Age* (London: Continuum International Publishing, 2012).
98. Richard J Danzig, "Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies," *Centre for a New American Security*, July 2014, https://www.cnas.org/publications/reports/surviving-on-a-diet-of-poisoned-fruit-reducing-the-national-security-risks-of-americas-cyber-dependencies.
99. Cimbala, *Nuclear Weapons in the Information Age*.