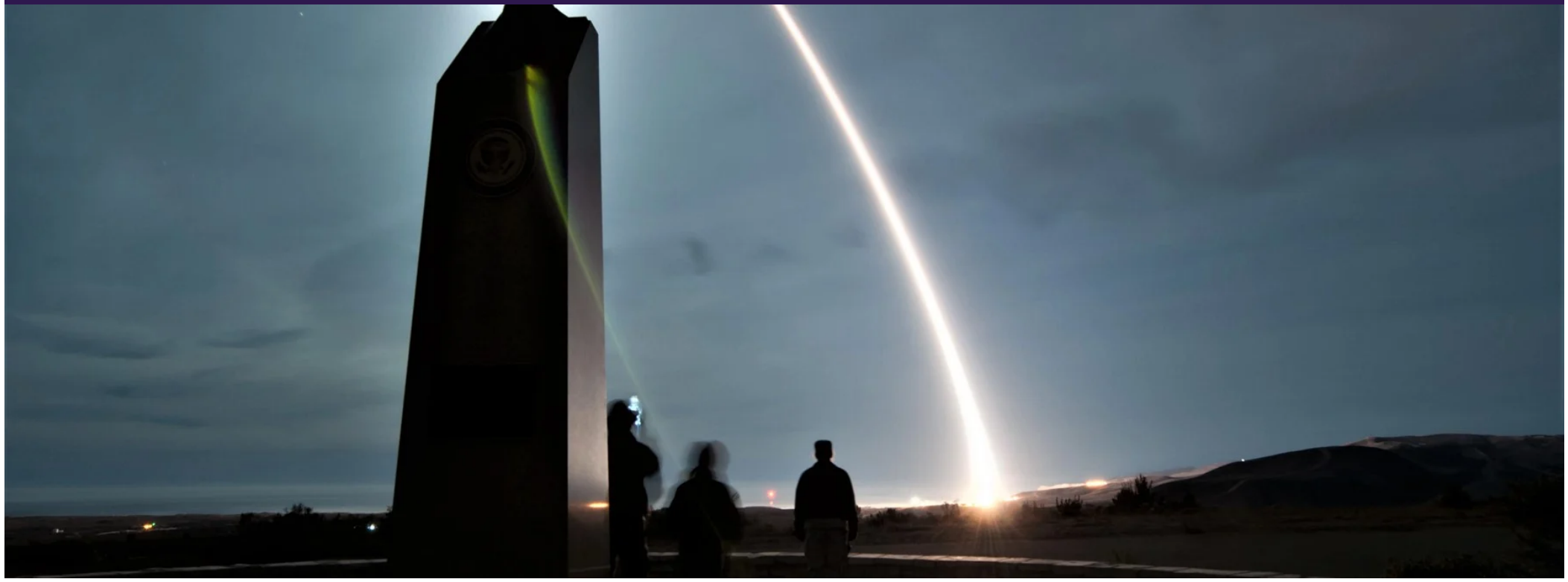

Cyber Threats and Nuclear Weapons

Andrew Futter

29 August 2018

The increasing sophistication of hacking and cyber-attacks is challenging the security of nuclear weapons systems.

There is a real and growing possibility that a sophisticated hacker could break into a nuclear weapons system and its associated infrastructure. Nuclear systems are of course well protected and wherever possible air-gapped from the wider internet and unsecured networks, but they are not -- and probably never will be -- invulnerable. Even the nuclear-armed submarine on patrol somewhere under the surface of the ocean is not beyond the range of skilful "cyber"-attackers who could implant malware during the vessel's manufacture or maintenance. The Stuxnet attack against the Iranian nuclear plant at Natanz, where attackers managed to install malware that disrupted the computer systems that controlled the centrifuges needed to enrich uranium, shows that hackers can find ways to "jump the air gap". It also shows that breaching computer systems often involves humans rather than sophisticated malware.

An evolving threat

In the past, the greatest fear in the "cyber"-nuclear realm was that a lone-wolf hacker could somehow break in and cause a nuclear launch, essentially re-enacting the plot of the 1983 Hollywood film *WarGames*. But today, the use of so-called Computer Network Operations (CNO) capabilities against an adversary's most sensitive military systems seems to have become an important component of military planning. Most notably, such operations underpin a new "full spectrum missile defence" mission adopted by the United States, where kinetic interceptors will be augmented by "left-of-launch" digital

Latest

An Update on the Security Policy Change Programme

Chances for Peace in the Third Decade

A Story of ORG: Oliver Ramsbotham

A Story of ORG: Gabrielle Rifkind

Related

Neither MAD Nor Even: Looking Beyond Trump's Missile Defense Review

ORG Explains #5: NATO Nuclear Sharing

technologies, as well as the broader global strike mission, where the intention is to be able to hit targets anywhere in the world at very short notice (in this case milliseconds). The result is an emerging norm that interfering in sensitive systems and critical national infrastructure to "prepare the battlefield" and prevent systems from working is an acceptable part of military strategy.

There is undoubtedly some logic in seeking new means to counter nuclear threats before they can fully materialise, with both Iran and North Korea being the obvious examples (and perhaps the first proper test cases). And of course, in not relying solely on kinetic ballistic missile defence systems to prevent the weapons, if launched, from striking their targets.

But such developments are also fraught with danger. Unlike kinetic missile interceptors and radar, which can be seen, and to some extent quantified, new electronic and digital methods of attack are by their very nature far more intangible. A missile deployed in a certain location will only be able to hit or intercept certain targets in a geographical area. "Cyber" capabilities, on the other hand, could be deployed against anyone at any time. Likewise, a Ballistic Missile Defence (BMD) system is only used once a missile has been launched. Computer Network Operations will likely have to take place before a launch, lacing systems and deploying malware "pre-emptively" to be effective.

The implication is that US adversaries will naturally worry that the same capabilities designed for "rogue states" could also be used against them, and even that their systems might already be compromised in some way. Thus, even without any attacks taking place or being discovered, such actions increase suspicion and tensions, undermine stability, and perhaps also increase nuclear risks. If a hacker was discovered inside the computer systems used to manage nuclear weapons, this could well lead to dangerous

The Kim/Trump Summit and Implications for Iran

Nuclear weapons x~20

Most read

The Role of Youth in Peacebuilding: Challenges and Opportunities

Making Bad Economies: The Poverty of Mexican Drug Cartels

ORG's Vision

Remote Warfare: Lessons Learned from Contemporary Theatres

knee-jerk responses, creating a diplomatic crisis, and maybe even pressure for some sort of military response. If the systems have been successfully compromised, it could mean that nuclear weapons don't work as expected or might even be used without authorisation or unintentionally.

New uncertainties about nuclear surety and security are playing out against an already worrying backdrop. US-Russia nuclear relations are at a nadir for a generation, and strategic stability across the globe is becoming increasingly clouded by an ever-more complex techno-political nuclear environment. The likelihood that more states will follow the US in developing and planning for new ways to target an adversary's nuclear weapons systems (and other military systems too) will do little to increase confidence, predictability or encourage a measure of calm in the global nuclear order. It may easily drive renewed arms racing in both nuclear and non-nuclear weaponry as states rush to make sure they are not at a (perceived) strategic disadvantage.

Add to this the potential for third party and non-state actors to utilise digital means as a mechanism for attacking nuclear systems or exacerbating a nuclear crisis, and we have a context shaped by myriad new dangers and dynamics. While "cyber-terrorism" as a concept and threat is much debated, nuclear systems kept on high alert and reliant upon ever more sophisticated coding for their operation are clearly an obvious target for a group bent upon causing mass casualties. That said, terrorist groups are likely to be less capable in this realm, and may instead opt for indirect attack vectors, such as clouding the information space, spoofing and even "fake news" to cause or deepen a crisis.

Managing the threat

There are no easy fixes to this emerging problem, and history does not offer much reassurance when it comes to managing the impact of new technology on warfare. But two pathways stand out when it comes to thinking about how to survive and mitigate the most worrying aspects of this threat.

The first is the development of new constraints in the use of CNO against nuclear systems. This might involve trying to get ahead of the threat by negotiating new forms of arms control in this space, and specifically through an agreement not to target nuclear weapons systems in this way. It might also involve new declaratory policy foreswearing such options by states. Clearly neither will be verifiable in the traditional sense, nor stop non-state actors, but it is a start, and states would be unlikely to want to run the risk of being caught in violation of stated policy or agreements.

The second is better security, policy and cooperation in this space, specifically reducing alert times of nuclear systems (to minimise the ability of non-state hackers to cause a launch or explosion), working to keep these systems separate from other non-nuclear weaponry and command and control apparatus (to reduce the risk of attackers inadvertently hitting the wrong systems), and keeping the command and control infrastructure as simple as possible (so it is understandable and offers less vulnerabilities for attackers to exploit). This might also involve other confidence building measures and sharing of good practice between governments, particularly regarding non-state threats.

The current geopolitical climate may not seem very conducive to new bilateral or multilateral nuclear agreements–indeed, many pillars of the past decades such as the New START, Intermediate-Range Nuclear Forces and Non-proliferation Treaties are all in danger. Whilst the Joint Comprehensive Plan of

Action (JCPOA) with Iran isn't dead, US participation is. But we have a chance now to get ahead of a serious development that will likely have negative implications for all nuclear-armed states, and thus by implication, all of us. New arms control agreements may not necessarily look like those of the past, or be quick to design and implement, but this does not make the need any less. It took the best part of two decades to begin to codify the nuclear revolution, and we have arguably been refining this ever since.

Conclusion

In the past, new military capabilities have had to be built (usually at enormous costs) and the threat realised before agreements could be made, but we may not be so lucky in the new techno-political context. If we can somehow come together and agree on the things that we as a society-and as nation states-most want to avoid, then perhaps we can begin to piece together frameworks to prevent this and begin to work backwards. Surely, we can all agree that hackers messing around in nuclear control systems primed for quick launch, and a general fear that nuclear weapons might not work if needed, isn't good for anyone.

Due in no small part to the latest computer and information revolution, where all aspects of our everyday lives are becoming digitised and reliant on computer technology that very few people can fully comprehend, we stand on the cusp of a very different global nuclear order, where the challenges of managing nuclear weapons will change. Our approach to making sure that nuclear weapons are never used again, must therefore change with it.

Image of ICBM test. Credit: US Air Force/public domain

Dr Andrew Futter is an Associate Professor of International Politics at the University of Leicester and the author of 'Hacking the Bomb". He can be contacted at: ajf57@le.ac.uk.

Share this page