War Games Redux? Cyber Threats, U.S.-Russian Strategic Stability and Future Nuclear Reductions*

Andrew Futter

In the 1983 Hollywood blockbuster, *War Games,* a teenage hacker sitting in his bedroom in Seattle, broke into a Pentagon supercomputer, managed to initiate a nuclear attack plan, and almost started World War Three between the United States and the Soviet Union. Such a scenario may have seemed somewhat far-fetched at the time and more science fiction than scientific reality. Indeed, most people didn't own a personal computer in the early 1980s, let alone have access to the Internet. But some thirty years later, with the ubiquitous spread of computers, hi-tech systems and software, digital networks and general interconnectedness, the possibility that hackers – be they state or non-state actors – might break into, interfere with, or sabotage nuclear command and control (C2) facilities, "spoof" or compromise early warning systems or components of the nuclear firing chain or, in a worst case scenario, even cause a nuclear explosion or launch, has become disconcertingly real. As the Global Zero Commission has mused:

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

Given the current downturn in east-west strategic relations and the significant amount of nuclear weapons still deployed by the United States and Russia – a surprisingly large number of which remain on hair-trigger alert and ready to be fired at very short notice – the potential for accidents, miscalculation or unauthorized nuclear use appears to be growing.[2] Worryingly however, in this increasingly unstable strategic context, the focus of U.S. and Russian officials seems likely to be more on making sure that nuclear forces cannot be *compromised* or *undermined* though hacking or other strategic developments (a focus on credibility) rather than taking various measures to reduce the risk of accidental or unauthorized use – most notably perhaps, through de-alerting and reducing their nuclear forces (a focus on surety). Consequently, it seems that cyber will become a significant impediment for the nuclear disarmament agenda and that the nightmare scenario depicted in *War Games* three decades ago is gradually becoming a feasible political reality that must be recognized, understood and addressed.

Cyber and U.S.-Russia Strategic Instability

Barack Obama entered office in 2009 determined to repair the bilateral relationship with Russia that he felt had been left to slide and become increasingly toxic under his predecessor, George W Bush. At the centre of the so-called "reset" was the desire to re-engage Russia on nuclear arms control and, if possible, to agree to make further reductions beyond those agreed upon since the end of the Cold War. While this was designed primarily to ensure that some type of agreement would be in place to supersede the expiring START and SORT treaties signed in 1991 and 2002 respectively, it was also, perhaps, seen as a first tentative step towards further reductions between the two erstwhile Cold War adversaries and possibly as a catalyst for multilateralizing and expanding the nuclear reductions agenda.

Despite the successful negotiation and agreement of the New START treaty in 2010, U.S.-Russian strategic relations have deteriorated markedly over the subsequent years, reaching a nadir not seen since the Cold War. The push for further nuclear cuts has, therefore, naturally stalled. One author has even suggested that we may have reached the "end of history" for nuclear arms control.[3]

Despite occasional up-turns, such as the 2009 "reset", the deterioration of U.S.-Russian strategic relations is a long-term trend that can probably be traced back to the late 1990s.[4] But while distrust and suspicion has always underpinned the east-west nuclear balance, over the past two decades, bilateral relations have become increasingly strained due to the continued expansion of NATO eastwards towards Russia, the growth of U.S. advanced non-nuclear weaponry and, particularly, the deployment of ballistic missile defence (BMD) systems in the United States, Europe and elsewhere, intensifying anti-Americanism in Russia, especially since the re-election of Vladimir Putin to the presidency in 2012, and the mounting concerns about purported Russian violations of the 1987 Intermediate-range Nuclear Forces (INF) treaty.[5]

These tensions have been compounded and exacerbated in recent months in the wake of the on-going war in Ukraine. Perhaps the most notable development has been an amplification of bellicose nuclear rhetoric, increasingly hostile posturing and threats, and "sabre rattling" from both parties, reminiscent of the 1980s. Indeed, in March 2015, Vladimir Putin revealed that he had considered putting Russian nuclear forces on alert in the wake of the Ukraine crisis[6] and, in response, the Obama administration allegedly considered re-deploying nuclear-armed ballistic missiles to Europe.[7] The result has been a notable descent toward greater nuclear instability and distrust and recognition that any further nuclear reductions are unlikely any time soon. In fact, both the United States and Russia currently appear more interested in modernizing their nuclear forces rather than cutting them back (although both continue to implement New START).[8]

This downturn in relations is happening at the same time as developments in cyber are creating various new vulnerabilities and problems to be addressed for both the safe and secure management of nuclear forces and for the U.S.-Russia strategic balance more generally. The cyber threat to U.S. and Russian nuclear forces and stability is twofold and nuanced, with each possibility representing different challenges and signifying different implications and problems. The first is the possibility that outsiders, third parties or terrorist groups might seek to cause a nuclear explosion, launch or try to precipitate or exacerbate a crisis – these can be thought of as *enabling* cyber attacks. The second is the possibility that the United States and Russia – or other states – will carry out cyber attacks against each other's nuclear systems in order to compromise communications, prevent weapons working as required or disrupt and undermine nuclear C2. These can be thought of as cyber attacks intended to *disable* or incapacitate nuclear systems. Taken together, these new cyber threats are both exacerbating the already strained U.S.-Russia strategic balance – particularly the perceived surety of nuclear forces – and, at the same time, creating new vulnerabilities and problems that might be exploited by a third party.

Accordingly, they add another major complication for future arms control agreements and possible significant nuclear cuts and also seem likely to increase the possibility of accidents, miscalculation and potentially unauthorized use – especially given the large number of nuclear weapons that remain on high alert. In this way, even though cyber may not be the main cause of the current instability – or, for that matter, supersede nuclear weapons as the ultimate symbol of national security – it is poised to further aggravate current tensions and add to the increasingly risky and delicate management of NATO-Russian nuclear relations.

Cyber Threats and the Logic of De-alerting

While all nuclear-armed states must be conscious of the new challenges presented to their nuclear forces by the various new tools, techniques and dynamics associated with cyber, the threat appears to be particularly acute for the United States and Russia. This is partly because these two states account for over 90% of the world's nuclear forces, but primarily because a considerable number – approximately 1,800 – are kept on hair-trigger alert.[9] The majority of these weapons are heavily-armed Intercontinental Ballistic Missiles (ICBMs) deployed in silos far removed from central command and control facilities, are tightly coupled with warning networks, and can be fired towards their targets at very short notice.

While such a posture is seen by many as an anachronistic legacy of the Cold War, it has, nevertheless, endured, and has been sustained primarily by "a circular (though flawed) logic, whereby U.S. nuclear forces are maintained on alert because Russian nuclear forces are on alert, and vice versa."[10] Given the current state of U.S.-Russian relations, this is unlikely to be reversed any time soon. The result, as the Global Zero Commission points out, is that:

> vulnerability to cyber attack [...] is the new wild card. Having many far-flung missiles controlled electronically through an aging and flawed command and control network and ready for launch upon receipt of a short stream of computer signals is a nuclear (surety) risk of the first order.[11]

In fact, it is at least possible that terrorist groups or other unauthorized actors could have taken advantage of the loss of control over 50 Minuteman missiles at FE Warren Air Force Base in Wyoming during October 2010 and facilitated a launch[12] – and it is highly likely that there are close calls we don't know about (particularly in other nuclear-armed states).

The nightmare scenario is that a terrorist group, a so-called "lone-wolf hacker", or even potentially a nation state, might somehow directly or indirectly hack into or interfere with these weapons and cause them to be launched. There are a variety of ways that such actors might seek to do this. It could be carried out *directly* by acquiring (possibly through cyber espionage) and sending false launch codes to the weapons, sabotaging the weapons and causing them to blow up or malfunction, or they might seek to precipitate a nuclear crisis *indirectly* by interfering with or "spoofing" early warning or other C2 systems into thinking an attack was underway.

With the United States and Russia deploying forces ready to be used within minutes of receiving the order, the possibility that weapons might be used by accident (such as a belief that an attack was underway due to spoofed early warning or false launch commands), by miscalculation (by compromised communications or through unintended escalation), or by people without proper authorization (such as a terrorist group, lone-wolf hacker or rogue commander) appears to be growing. As Franz-Stefan Gady explains:

> First, sophisticated attackers from cyberspace could spoof U.S. or Russian early-warning networks into reporting that nuclear missiles have been launched, which would demand immediate retaliatory strikes according to both nations' nuclear warfare doctrines. Second, online hackers could manipulate communication systems into issuing unauthorized launch orders to missile crews. Third, and last, attackers could directly hack into missile command and control systems launching the weapon [...] (a highly unlikely scenario).[13]

The result is that it is becoming progressively important to secure nuclear forces and associated computer systems against cyber attack, guard against nefarious outside influence and hacking and, perhaps most crucially, to increase the time it takes and the conditions that must be met before nuclear weapons can be launched. While this threat is particularly acute for U.S. and Russian forces deployed on hi-alert status and with weapons that cannot be called back (such as ICBMs), it will increasingly impact all nuclear forces – and those held by other nuclear-armed states – particularly during a crisis. In fact, certain other nuclear-armed states are also dispersing their forces and raising alert levels - increasing exponentially the pressures on C2 systems – and therefore magnifying the risk and possible implications of cyber attack.[14]

While there are numerous measures in place to guard against the unauthorized use of these weapons during "peacetime" and periods of strategic stability, such as Permissive Action Links (PALs), dual phenomenology, sophisticated encryption for communications, and various other safety features, the stress on C2 systems becomes particularly acute during a crisis where time pressures and perceived incentives may change. Moreover, complete trust in the dependability of these protective measures may also naturally reduce over time.

In this way, while indirect outsider interference (such as spoofing early warning) is likely to be manageable in times of stability and peace, in crisis situations, "cyber terrorists" would only need their interference to be believable for a short period of time to have considerable implications, perhaps even leading to miscalculation and nuclear use.[15] Given the possibility that certain actors wanting to cause mass destruction, equipped with the right tools, might have both the *intention* and *ability* to target these weapons, logic would suggest that de-alerting U.S. and Russian nuclear forces, hardening nuclear security systems against cyber attack, and perhaps expediting nuclear cuts are all pressing priorities. Ultimately, as former STRATCOM Commander General James Cartwright has said, "taking U.S. and Russian missiles off high-alert could keep a possible cyber attack from starting a nuclear war."[16]

New Barriers to De-alerting and Nuclear Reductions

Unfortunately decisions about nuclear weapons are not made in a political vacuum and, while new cyber challenges undoubtedly increase the risks associated with highly alerted U.S. and Russian nuclear weapons, they are also compounding and complicating U.S.-Russian strategic stability. Essentially, while the threat that a third party or terrorist group might seek to cause the launch or explosion of U.S. or Russian nuclear weapons appears to dominate the debate, cyber capabilities may also be used by the United States and Russia to hinder, disable or prevent each other's nuclear forces from operating as they should. This clearly has implications for the credibility and surety of nuclear forces on both sides and, consequently, for the strategic nuclear balance and mutual deterrence.

The result, especially given the current climate of distrust, is that neither party is likely to make any moves – such as de-alerting or reducing nuclear forces – that might potentially make them more vulnerable or susceptible to cyber attacks aimed at undermining their nuclear command and control systems.

While terrorists or other actors might wish to cause a nuclear launch, it is also possible that the United States and Russia might seek to use cyber capabilities against each other – likely in conjunction with other forces, or as a potential precursor to other kinetic forms of attack – in order to undermine or weaken each other's nuclear systems. This might be achieved by interfering with early warning systems – such as Israel is alleged to have done against Syria in 2007 – preventing, blocking or jamming communications and "go-codes", hacking into weapons and delivery systems themselves (possibly in advance), and generally placing doubt in an adversary's mind about whether their nuclear systems might possibly not work as intended when needed. The worst case scenario, as Martin Libicki explains, is that:

> Conceivably, one state could hack into the nuclear command and control system of another, render its weapons unusable, and use the temporary monopoly of power to coerce its target.[17]

While neither the United States nor Russia is likely to feel sufficiently confident that their cyber attacks have fully disabled the other's command and control systems "to the point at which they can act with impunity"[18], the perception that systems could be compromised or undermined is raising the perceived level of risk. This pressure is likely to become particularly acute during any future crisis, where both the United States and Russia will want to be sure of the credibility of their nuclear deterrent capabilities.

Both parties are increasingly cognizant of these potential new challenges to their nuclear forces, but the threat of cyber interference or disablement is perhaps most acute for Russia. Moscow has become deeply aware of the risk that its nuclear command and control systems could be compromised or disrupted by U.S. hackers and sees this as an increasingly serious challenge at the strategic level.[19]

But it is not just the threat of cyber on its own that is the problem, but rather how cyber might be used alongside other emerging U.S. technological capabilities – notably ballistic missile defences and advanced conventional strike systems. These concerns are compounded by the fact that Russian command and control infrastructure and particularly, its early warning systems are deteriorating (these malfunctioned in 2014 and, as of February 2015, Russia has had no nuclear warning space satellites[20]). Purported U.S. plans to target enemy air defence networks and warning sensors with cyber attacks early on in any future conflict are not helping assuage this concern.[21] A worst-case scenario is that Russian nuclear C2 could be penetrated by U.S. hackers, various systems and weapons might not work or not work as expected, other assets might be targeted by conventional precision strike forces and missile defence systems would nullify the rest.

The result is that the perceived requirement to deploy varied and sophisticated nuclear forces – a significant proportion of which are ready to be fired at short notice – appears to be increasing rather than decreasing in Moscow. Unfortunately, this desire to retain a credible nuclear force structure, and therefore an ostensibly manageable strategic balance with the United States, is compounding vulnerability to cyber intrusion and attack from outsiders.

While the possibility that nuclear forces may be compromised is perhaps slightly less acute for the United States, it has been recognized as a significant and growing challenge. In fact, the Defense Science Board reported in 2013 that U.S. nuclear weapons might be vulnerable to highly sophisticated cyber attack.[22] The primary concern for the United States is the exponential increase in hackers trying to gain access to systems and key (quite often nuclear-related) secrets. For example, the Buckshot Yankee attack of 2008 is believed to have been designed by Russia to steal sensitive U.S. defence information[23] and U.S. nuclear research and weapons laboratories remain key targets for hackers looking for sensitive secrets.[24]

While information security is one risk (and a possible proliferation concern), the greater anxiety is that such attacks may be used to "map out" systems or implant logic bombs and other malware for future sabotage. Discriminating between intrusions designed to steal information and those designed for more sinister purposes is very difficult to do. However, while such possible concerns present a growing barrier to nuclear cuts and de-alerting, and a strong rationale for the retention of a strategic nuclear triad to guard against a technological breakthrough in cyber counterforce capabilities, U.S. thinking is arguably more driven by political than by strategic dynamics. Essentially, it would be politically very difficult and costly for the current Obama administration to propose to de-alert the Minuteman III ICBMs fielded in silos in the American Midwest or to introduce new measures of reduced readiness for the current fleet of nuclear armed submarines, especially if these were to be taken unilaterally. It would also be difficult to see how this might be done in practice, without these weapons losing all strategic value.

While it is unlikely that either the United States or Russia has plans to fully undermine the other's nuclear command and control systems as a precursor to some type of disarming first strike, the perception that forces and key systems *could* be vulnerable or compromised is persuasive. The net result, especially given the current downturn in U.S.-Russian strategic relations and the way cyber exacerbates other strategic dynamics, is that it seems highly unlikely that either party will make the requisite moves to de-alert nuclear forces that the new cyber challenge appears to necessitate or, for that matter, to embrace the agenda of further significant cuts any time soon.

Options for Arms Control?

Given the new challenges presented by cyber to U.S. and Russian nuclear forces and U.S.-Russian strategic stability, it is important to consider what might be done to help mitigate and guard against these threats and thereby, help minimize the risks of unintentional launches, miscalculation and accidents, and perhaps create the conditions for greater stability and further nuclear cuts. While there is unlikely to be a panacea that will reduce the risk of cyber attacks on U.S. and Russian nuclear forces to zero – be they designed to launch nuclear weapons or compromise the systems that support them – there are a number of options that might be considered and pursued in order to address these different types of threats and vulnerabilities.

The most obvious and immediate priority for both the United States and Russia is working (potentially together) to harden and better protect nuclear systems against possible cyber attack, intrusion or cyber-induced accidents.

In fact, it was announced in October 2013 that Russian nuclear command and control networks would be protected against cyber threats by special units of the Strategic Missile Forces.[25] Other measures will include better network defences and firewalls, more sophisticated cryptographic codes, upgraded communications systems, extra redundancy, and better training and screening for the practitioners who operate these systems.

However, while comprehensive reviews are underway to assess the vulnerabilities of current U.S. and Russian nuclear systems to cyber attack, it may well be that C2 infrastructure becomes more vulnerable as it is modernized and old analogue systems are replaced with hi-tech digital platforms. As a result, while nuclear weapons and command and control infrastructure are likely to be the best protected of all computer systems and "air-gapped" from the wider Internet, this does not mean they are invulnerable or will continue to be in the future, particularly as systems are modernized or become more complex. Or as Peggy Morse, ICBM systems director at Boeing, put it, "while it's old it's very secure."[26]

Another set of options involves examining the potential for cyber arms control or cooperative agreements, both bilaterally between the United States and Russia and multilaterally.

The first option would be the pursuit of some type of international agreement on the prohibition of cyber attack capabilities, possibly under the auspices of the United Nations, which would build upon the joint Russian-Chinese proposal to ban cyber weapons, outlined in 2011. The idea would be for this to mirror previous arms control treaties – and perhaps draw upon the thinking, methods and mechanisms of the 1972 Biological Weapons Convention[27] or the now-defunct Anti-Ballistic Missile Treaty. Such an agreement might include limits on what is acceptable state behaviour in cyberspace, duties for monitoring private actors within state borders, mechanisms of cooperation and clarification of definitions thereby, possibly laying the basis for an international regime to govern this.[28] However, as the time of writing such a treaty remains a long way off and is hampered by a number of substantial problems and challenges, among them, issues of verification, attribution, and accepted definitions and demarcations.[29] That said, in 2013 the United States and Russia did agree to establish a "cyber hotline".[30]

The second would be to consider something more discrete, focused primarily on the cyber threat to nuclear weapons and C2. This might be a specific agreement or moratoria between the United States and Russia not to target each other's (and indeed other nuclear powers') nuclear forces and associated command and control infrastructure.[31] Such an agreement might be pursued through the auspices of the P5 dialogue or the broader framework of the Treaty on the Non-proliferation of Nuclear Weapons (NPT). In fact, given that other states are also suspected of drawing up plans to target adversaries' nuclear weapons infrastructure, it would make sense to involve other parties too.[32] Again, this would be very hard to verify and monitor and would not, of course, address actions by third party actors or terrorist groups. That said, this could be an area in which to build confidence between nuclear-armed states and enhance stability.

A third, more comprehensive option would be to include cyber – alongside other dynamics, such as sub-strategic nuclear forces, BMD and (advanced) conventional weapons – in a holistic U.S.-Russian strategic stability dialogue. While this would unquestionably be the most comprehensive and difficult option, any further nuclear reductions talks between the United States and Russia will have to at least address, if not formally include discussion about the emerging challenges beyond nuclear weapons. There are considerable political and strategic barriers to this, particularly in the United States where any future arms control agreement that includes limits on other U.S. systems is unlikely to fare well in the Senate, but it would appear to be the most credible way forward. Essentially, it is very difficult to see any further progress on significant nuclear reductions or arms control between the United States and Russia and, therefore, potentially including other nuclear armed states, if the whole gamut of technological and military dynamics effecting U.S.-Russian relations and strategic stability is not addressed holistically.

Ultimately, given the problems inherent in combating the new challenges associated with cyber, it may be, that for the time being, we have to accept that the drive for significant nuclear cuts in the short to medium term will need to be temporarily shelved and attention instead be focused on U.S.-Russian strategic stability and confidence building. This is likely to mean including cyber, alongside other emerging techno-military dynamics, in U.S.-Russian strategic dialogue and as part of any future formal agreements. Without addressing these concerns now, it is difficult to see a credible and efficacious pathway back towards meaningful disarmament measures in the medium and longer term. Essentially, the threat of cyber *disablement* of U.S. and Russian nuclear forces needs to be prioritized and addressed before measures can be taken to mitigate and minimize the possibility that hackers might facilitate a nuclear launch or explosion.

Conclusions

The development of offensive cyber capabilities is creating a range of new challenges and problems for the safe, secure and reliable management of U.S. and Russian nuclear forces, and for the U.S.-Russian strategic relationship more broadly. In particular, they increase the risk that hackers might gain access to nuclear C2 systems and either spoof them into believing an attack is underway or, in a worst case scenario, facilitate the launch/detonation of a nuclear weapon.

While the most logical response to this challenge would appear to be de-alerting and reducing U.S. and Russian nuclear forces, so as to minimize the risk of terrorists or non-state actors breaking into C2 systems and precipitating a launch, this is unlikely to happen any time soon. Essentially this is because, in the current toxic political climate, neither the United States nor Russia feels inclined to take any measures to move away from launch-on-warning modes. This is particularly acute for Russia, especially when U.S. cyber capabilities are combined with concerns about the deployment of ballistic missile defences, new conventional precision strike technologies and the increasing problems in the Russian command and control infrastructure. In this way, cyber is not the main cause of the current instability, but rather another factor exacerbating insecurity and making it more difficult to rebuild trust and confidence.

While the direct threat to the credibility of U.S. nuclear forces might be comparably less severe than for Russia, a mixture of political and strategic reasons makes it unlikely that any significant unilateral moves will be made by Washington either. The implications for nuclear arms control and further nuclear reductions are, therefore, not particularly encouraging, but it is imperative that both the new challenges presented by cyber and the way that cyber is exacerbating other dynamics undermining U.S.-Russia relations be addressed. Indeed, while there may be a number of options to help mitigate the cyber threat – primarily through arms control, moratoria or better security and cooperation – it is difficult to envision any progress without considerable improvement in the overall U.S.-Russian strategic relationship.

In this light, in order to take the necessary measures to protect nuclear systems from outside interference and safeguard against miscalculation and unauthorized use, we must first focus on U.S.-Russian strategic stability and, particularly, on the new gamut of techno-military challenges – including cyber – that are transforming and, in some cases, undermining the nuclear relationship. While this will undoubtedly not be easy, it does appear to be the only credible way to reinvigorate any serious nuclear disarmament agenda in the medium to long term which, in turn, will provide the best defence against cyber attack.

* * *

The views expressed are those of the author and do not necessarily reflect the views of Deep Cuts Commissioners or organizations associated with the Deep Cuts project.

About the Author

Andrew Futter is a Senior Lecturer in International Politics at the University of Leicester (United Kingdom), where his research focuses on nuclear weapons issues. He is the author of three books *Ballistic Missile Defence and U.S. National Security Policy* (2013), *The Politics of Nuclear Weapons* (2015) and *Reassessing the Revolution in Military Affairs* (2015), and has written widely on nuclear proliferation, strategy, deterrence, and missile defence. He is a member of the Euro-Atlantic Security Initiative (EASI) next generation working group and an Honorary Fellow at the Institute for Conflict, Cooperation and Security at the University of Birmingham. His current research into cyber threats and nuclear strategy is funded by the UK Economic and Social Research Council (ESRC) Future Research Leader's scheme (grant number ES/K008838/1).

Contact: ajf57@le.ac.uk

Disclaimer

Contact: info@deepcuts.org

References

[*] This paper builds on ideas previously published in "Cyber threats and the challenge of de-alerting US and Russian nuclear forces", Nautilus Institute NAPSNet Policy Forum, (15 June 2015) | Link.
I would like to thank Ulrich Kühn, Heather Williams and Ben Zala for their thoughts and comments on this piece.

[1] Global Zero Commission on Nuclear Risk Reduction, "De-alerting and stabilizing the world's nuclear force postures", (April 2015), p. 29 | Link.

[2] Ibid.

[3] Alexei Arbatov, "An unnoticed crisis: the end of history for nuclear arms control?", *Carnegie Moscow Center,* (16 June 2015) | Link.

[4] See Dmitri Simes, "Losing Russia: the costs of renewed confrontation", *Foreign Affairs,* 86:6 (2007) pp. 36-52.

[5] See Oliver Meier, Greg Thielmann & Andrei Zagorski, "Saving the INF Treaty", *Deep Cuts Commission Issue Brief 3,* (February 2015) | Link.

[6] Adam Withnall, "Vladimir Putin says Russia was preparing to use nuclear weapons 'if necessary' and blames US for Ukraine crisis", *The Independent,* (15 March 2015) | Link.

[7] Rhys Blakely & Tom Coghlan, "US considers sending missiles to Europe", *The Times,* (6 June 2015) | Link.

[8] See John Mecklin, "Disarm and modernize", *Foreign Policy,* (24 March 2015) | Link.

[9] Global Zero Commission, *"De-alerting and stabilizing the worlds nuclear forces",* p. 1.

[10] Hans Kristensen & Matthew McKinzie, "Reducing alert rates of nuclear weapons", *United Nations Institute for Disarmament Research,* (Geneva, 2012), p. viii | Link.

[11] Global Zero Commission, *"De-alerting and stabilizing the world's nuclear force postures",* p. 8.

[12] For a detailed explanation, see Bruce Blair, "Could terrorists launch America's nuclear missiles?", *TIME,* (11 November 2010) | Link.
Franz-Stefan Gady, "Could cyber attacks lead to nuclear war?", *The Diplomat,* (4 May 2015) | Link.

[14] Bruce Blair, "Lowering the nuclear threshold: the dangerous evolution of world nuclear arsenals toward far-flung dispersal, hair-trigger launch readiness, and First Use Doctrines", Remarks given at the Vienna conference on the Humanitarian Impact of Nuclear Weapons, Vienna, Austria, (8-9 December 2014) | Link.

[15] Jason Fritz, "Hacking nuclear command and control", *International Commission on Nuclear Non-proliferation and disarmament,* (2009) | Link.

[16] Quoted in Robert Burns, "Former US commander: take nuclear missiles off high alert", *Associated Press,* (29 April 2015) | Link.

[17] Martin Libicki, *"Crisis and escalation in cyberspace",* (Santa Monica CA, The RAND Corporation: 2012) p. 128.

[18] Ibid, p. xvii.

[19] Gady, "Could cyber attacks lead to nuclear war?"

[20] Kris Osborn, "Russia's satellite nuclear warning system down until November", *Defense Tech,* (20 June 2015) | Link.

[21] Philip Ewing, "The Pentagon's new cyber attack plan: 'Blunt force trauma'", Politico, (18 April 2015) | Link.

[22] See United States Department of Defense, Defense Science Board, "Task force report: resilient military systems and the advanced cyber threat", (January 2013) | Link.

[23] Ellen Nakashima, "Cyber-intruder sparks response debate", *The Washington Post*, (8 December 2011) | Link.

[24] See for example, "US nuclear weapons researchers targeted with Internet Explorer virus", *Russia Today*, (7 May 2013) | Link.

[25] "Cyber security units to protect Russia's nuclear weapons stockpiles", *Russia Today*, (17 October 2014) | Link.

[26] Quoted in John Reed, "Keeping nukes safe from cyber attack", *Foreign Policy,* (25 September 2012) | Link.

[27] For a discussion see David Fidler, "The relationship between the Biological Weapons Convention and Cybersecurity", *Council on Foreign Relations Net Politics Blog,* (26 March 2015) | Link. See also Kenneth Geers, "Cyber weapons convention", *Computer Law & Security Review*, 26:5 (2010) pp. 547-51.

[28] This builds on the list outlined in Jack Goldsmith, "Cybersecurity treaties: a skeptical view", *Koret-Taube task force on national security and law*, Hoover Institution, Stanford University, (March 2011), p. 2 | Link.

[29] Christopher A Ford, " The trouble with cyber arms control", *The New Atlantis,* 29 (Fall 2010), pp. 52-67 | Link.

[30] Ellen Nakashima, "US and Russia sign pact to create communication link on cyber security", *The Washington Post,* (17 June 2003) | Link.

[31] This a proposal discussed by Richard Danzig in, "Surviving on a diet on poisoned fruit: reducing the national security risks of America's cyber dependencies", Center for a New American Century, (July 2014), p. 26 | Link.

[32] See Fritz, *"Hacking command and control"*, and Zachary Keck, "S. Korea seeks cyber weapons to target North Korea's nukes", *The Diplomat,* (21 February 2014) | Link.