Cyber threats and the challenge of de-alerting US and Russian nuclear forces

The NAPSNet Policy Forum provides expert analysis of contemporary peace and security issues in Northeast Asia. As always, we invite your responses to this report and hope you will take the opportunity to participate in discussion of the analysis.

Recommended Citation

Andrew Futter, "Cyber threats and the challenge of de-alerting US and Russian nuclear forces", NAPSNet Policy Forum, June 15, 2015, https://nautilus.org/napsnet/napsnet-policy-forum/cyber-threats-and-the-challenge-of-de-alerting-us-and-russian-nuclear-forces/

by Andrew Futter

15 June 2015

I. Introduction

Andrew Futter writes ‘A quarter of a century after the end of the Cold War, both the United States and Russia retain a significant number of nuclear weapons … capable of inflicting almost unimaginable damage, death and devastation.’

Futter argues that ‘the logic of de-alerting these nuclear forces and enhancing the safety and security of nuclear systems is becoming increasingly persuasive and urgent….. [T]his appears to be becoming particularly pronounced as we move into a era increasingly dominated by the threat of “cyber attacks”.’

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

The views expressed in this report do not necessarily reflect the official policy or position of the Nautilus Institute. Readers should note that Nautilus seeks a diversity of views and opinions on significant topics in order to identify common ground.

II. Policy Forum by Andrew Futter

Cyber threats and the challenge of de-alerting US and Russian nuclear forces

A quarter of a century after the end of the Cold War, both the United States and Russia retain a significant number of nuclear weapons on "hair-trigger" alert, able to launch up to 1,800 warheads towards their designated targets in a matter of minutes.[1] In fact, and despite the widespread and substantial cuts that have been made to US and Russian nuclear forces over the previous three decades, and the many systems that have been removed from service, retired or dismantled, the weapons currently on continuous alert remain capable of inflicting almost unimaginable damage, death and devastation. In an era where it is becoming increasingly possible that "hackers" might steal sensitive nuclear-related operational or design information, "spoof" early warning systems, sabotage weapons and associated infrastructure, command and control facilities or critical communications, potentially cause a nuclear launch or explosion, and in a worst case scenario trigger nuclear war, the logic of de-alerting these nuclear forces and enhancing the safety and security of nuclear systems is becoming increasingly persuasive and urgent. While there has always been a chance that keeping nuclear systems at such a high state of readiness could lead to miscalculation, accidental or unauthorized launches, and the past is littered with examples of nuclear near misses and narrowly averted nuclear crises[2], this appears to be becoming particularly pronounced as we move into a era increasingly dominated by the threat of "cyber attacks".

While all nuclear armed states must be conscious of the new challenges and vulnerabilities to their nuclear forces as a result of developments in cyber, the threat is particularly acute for the large number of nuclear forces primed for launch 24 hours a day by the United States and Russia. Indeed, in the past few years, numerous reports and articles, most notably by the "Global Zero Commision" have championed the idea of de-alerting the many hundreds of US and Russian nuclear weapons that remain on hair-trigger alert[3]; a posture seen by many as an anachronistic hangover from the Cold War. While this has been partly driven by a belief that the US-Russian relationship has changed considerably since the darkest days of the Cold War, and that a nuclear exchange between the two is very hard to envisage, it has also been shaped by a growing concern about the impact of cyber attacks. Essentially, the worry is that new cyber capabilities – spanning a wide gamut of weapons, devices, methods and tools – are exacerbating existing problems and tensions within an already complex nuclear enterprise and creating new challenges that need to be addressed.[4] Foremost amongst these is the nightmare scenario that a terrorist group, other third party or even a nation state might somehow cause a nuclear explosion either directly or indirectly through hacking or other interference with nuclear systems.[5] Such actors might also "spoof" early warning systems into thinking an attack was underway, interrupt vital communications between the weapons and commanders or send false signals and "go codes", and even sabotage the weapons or the systems themselves so that they don't work, or at least don't work as planned. In the words of Franz-Stefan Gady:

> "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 or dismantling it on site (a highly unlikely scenario)."[6]

These challenges are sizeable enough during peacetime, but they will intensify considerably during a

crisis, where confidence in being able to use and control tightly coupled nuclear forces is central to the credibility of deterrence, escalation control and crisis management. With US and Russian forces ready to be used within minutes and even seconds of receiving the order, the possibility that weapons might be used by accident (such as the 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, third party or a rogue commander) is growing. Consequently, in this new nuclear environment, 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.

However, and while this logic is certainly persuasive, it seems unlikely that any significant moves towards de-alerting Russian and US nuclear forces will be made any time soon. Indeed, the cyber challenge may paradoxically help cement rather than undermine the current nuclear status quo in Washington and Moscow and provide a strong rationale for retaining a diverse nuclear force structure including weapons held on high alert. The reasons for this include a mixture of political, technical and strategic dynamics, but above all, are a reflection of the current state of distrust between the two erstwhile Cold War adversaries, particularly in light of recent events in Ukraine. In the United States for example, it would be politically very difficult and costly for the current Obama administration to propose to de-alert the 450 Minuteman III ICBM's fielded in silo's in the American Midwest, or to introduce new measures of reduced readiness for the current fleet of Ohio class SSBNs; especially, if these measures were to be taken unilaterally. It would also be difficult to see how this might be done in practice, without the weapons losing all strategic value – this is particularly the case for non-mobile US ICBMs. In fact, as the threat that weapons or systems might be compromised by cyber attack continues to grow and expand, even the perception of this threat is likely to reinforce the logic of retaining a sophisticated triad of US nuclear forces, with many weapons held on alert, in order to avoid strategic surprise.

These pressures to maintain nuclear weapons on high-alert are perhaps felt even more acutely in Russia, where the need to deploy sophisticated nuclear forces ready to be fired at short notice appears to be increasing rather than decreasing, especially given advances in US conventional weaponry, particularly ballistic missile defence and global prompt strike. As such, and even though the Russian ICBM force could probably be made entirely mobile and include increased penetration aids, and according to Bruce Blair, the Russian high command needs only seconds to fire rockets out of their silos as far away as Siberia,[7] the risk that these forces could be held vulnerable is likely to increase given the new suite of technological capabilities being developed by the US – not least the threat of US cyber "weapons" - and this will remain a significant barrier to de-alerting. In fact, according to Greg Austin and Pavel Sharikov, "Russia now sees U.S. plans to disrupt the command and control of its nuclear weapons as the only actual (current) threat at the strategic level of warfare."[8] The net result is that Russia has little current incentive to de-alert its nuclear forces, or to entertain any further moves on nuclear arms control given this new and emerging threat spectrum, and the perceived challenge to the efficacy of its nuclear weapons and deterrent. The problem is that while Russia is no longer believed to operate the "Dead Hand" semi-autonomous nuclear retaliatory system[9] – a likely disaster waiting to happen in the cyber age for reasons discussed above – the desire to retain a credible nuclear force structure, and therefore manageable strategic balance with the US, is creating considerable new vulnerabilities for cyber intrusion and attack. These vulnerabilities are exacerbated by the fact that Russian command and control facilities, and particularly early warning systems are deteriorating, which makes retaining these weapons on high-alert increasingly dangerous and risky, and intensifies the chances of third party cyber interference, miscalculations and accidents.

Without question, de-alerting Russian and US nuclear forces and securing them against various types of cyber attacks and vulnerabilities should be a pressing priority in both Washington and Moscow, and the centerpiece of future discussions on strategic stability. In fact, it may well be time to replace the long-established overarching focus on strategic arms control and nuclear cuts with more attention on security, safety and the danger of cyber attacks and interference; moreover, it may be that the closer nuclear armed actors move toward "minimum deterrence postures" the more significant the threat of cyber attack or interference becomes.[10] As such, any further arms reductions between the US and Russia will almost certainly have to include discussion if not agreement on the broader suite of capabilities effecting the US-Russian strategic balance, foremost amongst them, cyber. One place to start might be an agreement or moratorium for the US and Russia (and indeed other nuclear powers) not to target each other's vital C2 nuclear systems with cyber attacks[11] (or other forces), although this would be very hard to verify and monitor, and of course would not preclude actions by third party actors or terrorist groups. Another, more extensive option might be to discuss the whole gamut of challenges increasingly shaping the US-Russian strategic balance, and see whether some type of workable agreement including nuclear weapons, advanced conventional systems and cyber might be negotiated that would allow for reducing nuclear alert times. This would undoubtedly be a difficult task, and perhaps impossible in the short term, but it is imperative that this new dynamic isn't simply ignored, and it is at least possible that such moves can be made while retaining a level of stability and confidence in nuclear forces for both sides. Ultimately, the failure to address the increased uncertainty about the efficacy and surety of nuclear forces in a cyberized world, particularly the growth of an array of new vulnerabilities and dangers, may mean we are moving towards a new era of US-Russian nuclear instability and danger not seen since nadir of the 1980s.

III. References

[1] "De-alerting and stabilizing the world's nuclear force postures", Global Zero Commission on Nuclear Risk Reduction, (April 2015), p.1, http://www.globalzero.org/files/global_zero_commission_on_nuclear_risk_reduction_report0.pdf
http://www.globalzero.org/files/global_zero_commission_on_nuclear_risk_reduction_report0.pdf

[2] For a good overview of this see, Eric Schlosser, *"Command and control"*, (London, Allen Lane: 2013)

[3] See for example, "De-alerting and stabilizing the worlds nuclear force postures", and Robert Burns, "Former US commander: take nuclear missiles off high alert", *Washington Post,* (29 April 2015), http://www.washingtonpost.com/pb/world/national-security/former-us-commander-take-nuclear-missiles-off-high-alert/2015/04/29/b253b78e-eea2-11e--8050-839e9234b303_story.html?resType=accessibility

[4] On this see, Andrew Futter, "Hacking the bomb: nuclear weapons in the cyber age", Paper presented at the International Studies Annual Conference, New Orleans, (23-27 February 2015), https://www2.le.ac.uk/departments/politics/people/afutter/copy_of_AFutterHackingtheBombISAPaper2015.pdf

[5] See Bruce Blair, "Could terrorists launch America's nuclear missiles?", *TIME,* (11 November 2010), http://content.time.com/time/nation/article/0,8599,2030685,00.html

[6] Franz-Stefan Gady, "Could cyber attacks lead to nuclear war?", *The Diplomat,* (4 May 2015), http://thediplomat.com/2015/05/could-cyber-attacks-lead-to-nuclear-war/

[7] 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), http://www.thesimonsfoundation.ca/sites/all/files/Presentation%20by%20Bruce%20Blair%20at%20the%20Vienna%20Conference%20on%20the%20Humanitarian%20Impact%20of%20Nuclear%20Weapons,%20Dec%208,%202014.pdf

[8] Quoted in Franz-Stefan Gady, "Could cyber attacks lead to nuclear war?", *The Diplomat,* (4 May 2015), http://thediplomat.com/2015/05/could-cyber-attacks-lead-to-nuclear-war/

[9] On this see, David Hoffman, *"The dead hand: Reagan, Gorbachev and the untold story of the Cold War arms race"*, (Icon: 2011)

[10] Stephen Cimbala & Roger McDermott, "A new Cold War? Missile defenses, nuclear arms reductions, and cyber war", *Comparative Strategy,* 34:1 (2015) p.104

[11] 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.6 & 26, http://www.cnas.org/sites/default/files/publications-pdf/CNAS_PoisonedFruit_Danzig_0.pdf

---

View this online at: https://nautilus.org/napsnet/napsnet-policy-forum/cyber-threats-an--the-challenge-of-de-alerting-us-and-russian-nuclear-forces/

Nautilus Institute
608 San Miguel Ave., Berkeley, CA 94707-1535 | Phone: (510) 423-0372 | Email: nautilus@nautilus.org