



# War Games redux? Cyberthreats, US–Russian strategic stability, and new challenges for nuclear security and arms control

Andrew Futter

To cite this article: Andrew Futter (2015): War Games redux? Cyberthreats, US–Russian strategic stability, and new challenges for nuclear security and arms control, European Security, DOI: [10.1080/09662839.2015.1112276](https://doi.org/10.1080/09662839.2015.1112276)

To link to this article: <http://dx.doi.org/10.1080/09662839.2015.1112276>



© 2015 The Author(s). Published by Taylor & Francis.



Published online: 21 Dec 2015.



Submit your article to this journal [↗](#)



Article views: 275



View related articles [↗](#)



View Crossmark data [↗](#)

## War Games redux? Cyberthreats, US–Russian strategic stability, and new challenges for nuclear security and arms control

Andrew Futter

Department of Politics & International Relations, University of Leicester, Leicester, UK

### ABSTRACT

Some 30 years since the release of the Hollywood blockbuster *War Games*, the possibility that hackers might break into nuclear command and control facilities, compromise early warning or firing systems, or even cause the launch of a nuclear weapon has become disturbingly real. While this challenge will impact all nuclear-armed states, it appears particularly acute for the USA and Russia given their large, diverse, and highly alerted nuclear forces. The fact that east–west relations have deteriorated to a nadir perhaps not seen since the 1980s, strategic instability has increased – particularly in the wake of the Ukraine and now Syria crises – and that the nuclear arms reductions agenda appears to have reached a standstill makes this challenge particularly pressing. In this discouraging milieu, new cyberthreats are both exacerbating the already strained US–Russia strategic balance – particularly the perceived safety and security of nuclear forces – and at the same time creating new vulnerabilities and problems that might be exploited by a third party. Taken together, these dynamics add another major complication for current arms control agreements and possible future nuclear cuts, and also seem likely to increase the possibility of accidents, miscalculation, and potential unauthorised nuclear use, especially given the large number of nuclear weapons that remain on “hair-trigger” alert.

### ARTICLE HISTORY

Received 11 September 2015

Accepted 21 October 2015

### KEYWORDS

Cyber; nuclear weapons; strategic stability; arms control; nuclear reductions; United States; Russia; nuclear command and control

### Introduction: when science fiction becomes reality

In the 1983 Hollywood blockbuster *War Games*, a teenage hacker sitting in his bedroom in Seattle, WA, broke into a Pentagon supercomputer, managed to initiate a nuclear attack plan, and almost started the Third World War between the USA and the Soviet Union. Such a scenario may have seemed somewhat far-fetched to viewers at the time, and a work of science fiction rather than scientific reality; indeed, most people didn’t own a personal computer in the early 1980s, let alone have access to the Internet.<sup>1</sup> But some 30 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

**CONTACT** Andrew Futter  [ajf57@le.ac.uk](mailto:ajf57@le.ac.uk)

© 2015 The Author(s). Published by Taylor & Francis.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

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 on Nuclear Risk Reduction (2015) 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? (p. 29)

Given the current downturn in east–west strategic relations, and the significant amount of nuclear weapons still deployed by the USA and Russia – a surprisingly large number of which remain on high alert and ready to be fired at very short notice<sup>2</sup> – the potential for accidents, miscalculation, or unauthorised nuclear use appears to be growing. Worryingly however, in this increasingly unstable strategic context, the focus of US and Russian officials seems likely to be more on making sure that nuclear forces cannot be *compromised* or *undermined* through hacking or other strategic developments (a focus on credibility), rather than taking various measures to reduce the risk of accidental or unauthorised use – most notably perhaps through de-alerting, securing, and potentially reducing their nuclear forces (a focus on security and safety). Or, more succinctly, the perceived requirement to fire nuclear weapons seems likely to supersede the desire to keep them safe and secure for the foreseeable future (Blair 2010). Consequently, it seems that cyber will become a significant impediment for bilateral arms control and the nuclear reductions agenda, and that the nightmare scenario depicted in *War Games* over three decades ago is gradually becoming a feasible political reality that must be recognised, understood, and addressed.

Given this disconcerting strategic context and outlook, and in order to consider, examine, and suggest some possible ways forward out of this current impasse, this paper proceeds in four sections: (1) first, it charts the deterioration in US–Russian strategic relations and explains how new cyber challenges are both exacerbating existing tensions between the two states and causing new issues for nuclear safety and security; (2) second, it considers perhaps the most alarming emerging risk that hackers might somehow directly or indirectly cause a nuclear explosion or precipitate the launch of US or Russian strategic forces (especially the several hundred Intercontinental Ballistic Missiles (ICBMs) that both states maintain on high alert); (3) third, it examines the possibility that the USA and Russia might use cyber capabilities against each other’s nuclear systems, and why this is causing added nuclear instability, complicating nuclear arms control, and undermining prospects for future nuclear cuts and stronger nuclear security; (4) lastly, the article considers various different options that might be taken to address and mitigate the undesirable and increasingly worrying impact of these new cyber dynamics on US and Russian nuclear forces, strategic stability, and on bilateral relations more broadly.

## An unholy alliance: cyberthreats and US–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 nuclear security, and if possible to work towards making further nuclear reductions beyond those agreed since the end of the Cold War. While this was designed primarily to ensure that some type of binding agreement would be in place to supersede the expiring START and SORT treaties signed in 1991 and 2002, respectively (and especially the New START verification regime<sup>3</sup>), it was also, perhaps, seen as a first tentative step towards deeper cuts between the two erstwhile Cold War adversaries, and potentially as a catalyst for multilateralising and expanding the nuclear reductions and nuclear security agenda. As then President-elect Obama explained in late 2008,

The United States and Russia should seek real, verifiable reductions in all US and Russian nuclear weapons ... I am committed to working with Russia and other nuclear weapons states to make deep cuts in global stockpiles by the end of my first term. (Obama 2008)

However, and despite the successful negotiation and agreement of the New START treaty in 2010, US–Russian strategic relations have declined markedly over the subsequent years, reaching a nadir perhaps not seen since the Cold War. As a result, trust and cooperation have slowly evaporated and the push for further bilateral nuclear cuts has therefore naturally stalled. One author has even suggested that we may have reached the “end of history” for nuclear arms control (Arbatov 2015).

Despite occasional up-turns such as the 2009 “reset”, the deterioration of US–Russia strategic relations is a long-term trend that can probably be traced back to the late 1990s (see Simes 2007). Indeed, for some “cold warriors” on both sides, the antagonism and competition that shaped the past remain central to the modern relationship, particularly with regard to global and strategic issues. But while distrust and suspicion have always underpinned the east–west nuclear balance, over the past two decades, US–Russian bilateral relations have become increasingly strained due to a mixture of political, diplomatic, and strategic reasons. In particular, four main drivers of this instability stand out: (1) the continued expansion of the North Atlantic Treaty Organisation (NATO) eastwards towards Russia, and especially into former Soviet states (see Mearsheimer 2014); (2) the growth of US advanced non-nuclear weaponry, and particularly the deployment of ballistic missile defence (BMD) systems in the USA, Europe, and elsewhere (see Futter and Zala 2013); (3) the growth of anti-American and anti-Western sentiment in Russia, particularly following the re-election of Vladimir Putin to the presidency in 2012 (see Remnick 2014); and (4) mounting concerns about purported Russian violations of the 1987 Intermediate Range Nuclear Forces treaty (see Sokov and Pomper 2014). Taken together these dynamics have driven a return to the type of antagonistic US–Russian relations not seen since the 1980s, which in turn has led to increasing concern in both countries, within NATO, and across Europe. Some have even warned of about the emergence of a “new Cold War” (see Krickovic and Weber 2015).

These tensions have been compounded and exacerbated in recent months in the wake of the ongoing war in Ukraine, and now increasingly by events in Syria as well. Perhaps the most notable development has been an amplification of bellicose (nuclear) rhetoric, hostile posturing and threats, and “sabre rattling” from both parties, in some ways reminiscent of the 1980s (see Ewing 2015a, Shapiro 2015). Indeed, in March 2015, Russian President Vladimir Putin revealed that he had considered putting Russian nuclear forces on

alert in the wake of the Ukraine crisis (Withnall, 2015), and in response the Obama administration allegedly considered redeploying nuclear-armed ballistic missiles to Europe (Blakeley and Coghlan 2015). The result has been a notable descent towards greater nuclear instability and distrust, the suspension of bilateral cooperation on nuclear security issues (see Bender 2015), and the recognition that any new arms control measures or further nuclear reductions are unlikely any time soon. In fact, the USA and Russia currently appear more interested in modernising their nuclear forces rather than cutting them back (Wolfsthal *et al.* 2014, Mecklin, 2015), although both continue to implement the arms control measures agreed under the New START treaty (Rose 2015). At least that is for the time being.

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 US–Russia strategic balance more generally (see Futter 2015b). Indeed, and while cyber remains a contested and somewhat nebulous concept, and perhaps too often a universal catch-all prefix for “anything bad that involves a computer” (Yadron and Valentio-Devries 2015), it is clear that the cyber challenge to all facets of the US and Russian nuclear security enterprise and associated infrastructure is real and growing. In 2012, for example, Thomas D’Agostino, former US Under Secretary for Nuclear Security (2007–2012) and Administrator of the National Nuclear Security Administration, warned that US nuclear weapons and associated systems “are under constant attack” from a “full spectrum of hackers” (Koebler 2012), and more recently former head of US Strategic Command (2004–2007) General James Cartwright noted that “The sophistication of the cyber threat has increased exponentially ... It is reasonable to believe that the threat has extended itself into nuclear command and control systems” (quoted in Burns 2015). The nature of this challenge is multifaceted and varied and ranges across a broad spectrum from simple hacking and nuisance, through accessing and stealing information, right up to attacks designed to cause physical damage (see Futter 2015a). As such, and given the diverse nature of nuclear weapons management, in this case the cyber challenge is perhaps best 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 who engage with them.<sup>4</sup> New cyberthreats therefore impact right across and within the US and Russian nuclear relationship, and include attacks on nuclear command and control systems, communications links, weapons, and delivery systems; attacks on computers, hardware, and software used to manage and operate nuclear forces; and attempts to provide false or misleading information to these systems and to decision-makers.<sup>5</sup>

The cyberthreat to US and Russian nuclear forces and stability is not homogenous, but rather is twofold and nuanced, with each possibility representing different challenges and signifying different implications and problems. The first is the prospect that outsiders, third parties, or terrorist groups might seek to cause a nuclear explosion, launch, or try to precipitate or exacerbate a crisis between nuclear-armed states (potentially through a so-called false-flag operation<sup>6</sup>). These can be thought of as *enabling* cyberattacks. The second is the possibility that the USA and Russia – or other states – might carry out cyberattacks against each other’s nuclear systems in order to compromise communications, prevent weapons working as required, or disrupt and undermine the opponent’s nuclear C2. These can be thought of as cyberattacks intended to *disable* or incapacitate

nuclear systems. Taken together, these new cyberthreats are both exacerbating the already strained US–Russia strategic balance – particularly the perceived surety of nuclear forces – and at the same time creating new vulnerabilities and security problems that might be exploited by a third party. Accordingly, they add another major complication for both current arms control agreements and the possibility of future nuclear cuts, and also seem likely to increase the chance of accidents, miscalculation, and potentially unauthorised use, especially given the large number of nuclear weapons that remain on high alert. As Cimbala and McDermot (2015) point out, the result is that “neither nuclear deterrence nor cyber war will be able to live in distinct policy universes for the near or distant future” (p. 103).

In this way, and even though cyber may not be the main cause of current US–Russian strategic instability – or for that matter supersede nuclear weapons as the ultimate symbol or guarantor of national security – it is poised to further aggravate current tensions and add to the increasingly risky and delicate management of east–west nuclear relations. The net result, as a recent report by the Nuclear Threat Initiative argues, is that “The risk of nuclear weapons use in the Euro-Atlantic region is on the rise — and it is higher than it has ever been since the end of the Cold War” (Berls & Ratz 2015, p. 1).

### **“Cyberterrorism” and the logic of de-alerting US and Russian nuclear forces**

While all nuclear-armed states must be conscious of the new challenges presented to their nuclear forces and infrastructure by the various new tools, techniques, and dynamics associated with cyber, the threat appears to be particularly acute for the USA and Russia. This is partly because these two states account for over 90% of the total global nuclear weapons stockpile,<sup>7</sup> but primarily because a considerable number of these weapons – approximately 1800 – are kept on hair-trigger alert and primed for launch within minutes of receiving the order (Global Zero Commission 2015, p. 1). The majority of these weapons are heavily armed ICBMs deployed in silos far away from central command and control facilities, that are tightly coupled with warning networks and sensors, and can be fired towards their targets at very short notice. In fact, according to Blair (2014), the Russian high command needs only seconds to fire rockets out of their silos as far away as Siberia.

While a posture of maintaining nuclear forces at such high levels of alert is seen by many as an anachronistic legacy of the Cold War, it has however endured, and has been sustained primarily by what Kristensen and McKinzie (2012) refer to as “a circular (though flawed) logic, whereby US nuclear forces are maintained on alert because Russian nuclear forces are on alert, and vice versa” (p. viii). Nevertheless, and particularly given the current state of US–Russian strategic relations, this potentially very dangerous posture is unlikely to be reversed any time soon. The result, as the Global Zero Commission (2015) 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. (p. 8)

In fact, as Blair (2010) has pointed out, it is at least possible that terrorist groups or other unauthorised 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 nuclear launch. Moreover, given the number of nuclear accidents and nuclear near misses that are only now coming to light (see Lewis *et al.* 2014), it should be assumed that there have been many other times when “hackers” could have interfered with nuclear systems in the recent past. This is particularly the case for other nuclear-armed states, and not just the USA. As Schlosser (2013a) notes,

I have no doubt that America’s nuclear weapons are among the safest, most advanced, most secure against unauthorized use that have ever been built ... other countries with less hard-earned experience in the field may not be so fortunate. (p. 481)

Worryingly, according to General Robert Kehler, former head of US Strategic Command (2011–2013), it remains unknown whether Russia or China could prevent hackers from launching their nuclear missiles (quoted in Schlosser 2013b).

The nightmare scenario is that a terrorist group, a so-called lone-wolf hacker, or even potentially a nation state, might somehow either directly or indirectly hack into or interfere with US or Russian nuclear C2 systems and potentially cause nuclear weapons to be launched or to detonate (see Blair 2010). There are a variety of ways that such actors might seek to do this; attacks could be carried out *directly* by acquiring (possibly through cyberespionage) 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 (a so-called false positive). With the USA and Russia deploying forces ready to be used within minutes and perhaps even seconds 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 (due to compromised communications links or through unintended escalation), or by people without proper authorisation (such as a terrorist group, lone-wolf hacker, or rogue commander) appears to be growing. As Gady (2015) 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).

That said, as Fritz (2009) notes,

A sophisticated all encompassing combination of traditional terrorism and cyber terrorism could be enough to launch nuclear weapons on its own, without the need for compromising command and control centres directly.

Either way, the result is that it is becoming progressively important to secure nuclear forces and associated computer systems and infrastructure against cyberattack, guard against nefarious outside influence and hacking, and perhaps most crucially, 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 US and Russian forces deployed at a status of high alert and that cannot be called back (such as ICBMs), it will increasingly impact all nuclear forces – as well as those held by other nuclear-armed states – particularly during crises and periods of heightened tension. In fact, it is believed that 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 potential implications of a possible cyberattack (Blair 2014).

While there are numerous measures in place to guard against the unauthorised use of US and Russian nuclear weapons during “peacetime” and periods of strategic stability, such as Permissive Action Links, dual phenomenology, sophisticated encryption for communications,<sup>8</sup> and other various safety features,<sup>9</sup> these tensions become particularly acute during a crisis where time pressures and perceived incentives may change.<sup>10</sup> Complete trust in the dependability of these protective measures may also naturally reduce over time as components age and new vulnerabilities and glitches that can be exploited are discovered. In this way, while indirect outsider interference (such as spoofing early warning or sending false commands) is likely to be manageable in times of relative 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 (Fritz 2009). Given the possibility that certain actors wanting to cause mass destruction, equipped with the right tools, might have both the *intention* and the *capability* to target nuclear weapons and associated systems, logic would suggest that de-alerting US and Russian nuclear forces, expediting nuclear cuts, and hardening nuclear facilities against cyberattack are all pressing priorities. Ultimately, as General James Cartwright has said, “Taking US and Russian missiles off high alert could keep a possible cyber attack from starting a nuclear war” (quoted in Burns 2015).

### Cyber and the US–Russia nuclear balance: prioritising assurance over security

Unfortunately decisions about nuclear weapons are not made in a political vacuum, and while new cyberthreats undoubtedly increase the risks associated with highly alerted US and Russian nuclear weapons, and exacerbate the challenges of nuclear security more broadly, they are also compounding and complicating US–Russian strategic stability. Essentially, while the threat that a third party or terrorist group might seek to cause the launch or explosion of US or Russian nuclear weapons appears to dominate the current debate, cyber capabilities could also be used by the USA and Russia *against each other* in order 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 accordingly, for the strategic nuclear balance and mutual (assured) deterrence too. The result, especially given the current climate of political distrust, is that neither party is likely to take any moves – such as de-alerting or reducing nuclear forces – that might potentially make them more vulnerable or susceptible to cyberattacks, or attacks that include a cyber-component, aimed at compromising their vital nuclear command and control systems. As Austin (2012) notes, “Strategic nuclear stability may be at risk because of uncertainty about innovations in cyber attack capability”. This is



particularly the case when uncertainties about cyber are added to other destabilising strategic dynamics.

While terrorists or other actors might wish to cause a nuclear launch or explosion, it is also possible that the USA 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 the opponent's nuclear capability. This might be achieved by interfering with early warning systems – such as Israel is alleged to have done against Syria in 2007 (see Fulgham 2013); preventing, blocking, or jamming communications and “go-codes”; hacking into weapons and delivery systems themselves (possibly in advance, and through the imposition of certain logic bombs and backdoors<sup>11</sup>); and generally by placing doubt in an adversary's mind that their nuclear systems may not work as intended when needed. The worst-case scenario, as Libicki (2012) 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.  
(p. 128)

While neither the USA nor Russia are likely to feel sufficiently confident that their cyberattacks have fully disabled the other's command and control systems “to the point at which they can act with impunity” (Libicki 2012, p. xvii), or for that matter be willing to carry out such a potentially catastrophic move in anything but the most extreme circumstances, 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, and especially one that escalates rapidly, where both the USA and Russia will want to be sure of the credibility of their nuclear deterrent capabilities, and particularly the ability to carry out retaliatory nuclear strikes in the face of possible cyber interference (Danzig 2014, p. 26).

Both parties are increasingly cognisant of these new potential vulnerabilities to the surety of their nuclear forces, but the threat of cyber interference or disablement is perhaps most acute in Russia. Moscow has become deeply aware of the risk that its nuclear command and control systems could be compromised or disrupted by US hackers, and sees this as an increasingly serious challenge at the strategic level (Gady 2015). This concern has been magnified by the reported success of the Stuxnet cyberattacks against the Iranian nuclear programme (see Zetter 2014) and rumours of similar operations conducted against North Korea (Rodriguez 2015). But it is not just the threat of cyber on its own that is the problem, but rather how cyber might be used alongside and in conjunction with other emerging US technological capabilities – notably BMDs and advanced conventional strike systems. Such concerns are compounded by the fact that Russian command and control infrastructure, and particularly its early warning systems, are deteriorating (Osborn 2015).<sup>12</sup> Overhauling and upgrading Russia's nuclear C2 and deploying a new fleet of early warning satellites are also considered essential short-term priorities to help eliminate and guard against nuclear false alarms (Sputnik News 2015). Purported US plans to target enemy air defence networks and warning sensors with cyberattacks early on in any future conflict are not helping to assuage this concern (Ewing 2015b). A worst-case scenario therefore is that Russian nuclear weapons, C2, and associated infrastructure could be penetrated by US hackers, various

systems and weapons might not work or work as expected, other assets might be targeted by conventional precision strike forces, and missile defence systems could potentially nullify the retaliatory capability of those weapons that remain usable. While this might seem a highly unlikely future scenario at the time of writing, the result is nevertheless 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.<sup>13</sup> Unfortunately, this desire to retain a credible nuclear force structure, and therefore an ostensibly manageable strategic balance vis-à-vis the USA and NATO, is compounding the vulnerability of Russian nuclear systems to cyber-intrusion and attack by others.

While the possibility that nuclear forces and associated infrastructure may be compromised is perhaps slightly less acute for the USA, it has been recognised as a significant and growing challenge. In fact, the US Defense Science Board reported in 2013 that US nuclear weapons might be vulnerable to highly sophisticated cyberattack in extreme circumstances, and that the full extent of the cyber challenge to US nuclear forces remains unknown (see US Department of Defense 2013, see also Farnsworth 2013). A key concern for the USA 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 US defence information (Nakashima 2011), and US nuclear research and weapons laboratories remain key targets for hackers looking for sensitive secrets (*Russia Today* 2013). As Adam Segal puts it,

Hacking into the Department of Energy and looking for nuclear secrets – how to build a bomb, is probably much easier than trying to take over a bomb or a launch code, and probably of more interest to the Russians or the Chinese or the Iranians. (quoted in Koebler 2012)

However, and while information security is one risk (and a possible proliferation concern), the greater anxiety is that similar attacks may be used to map out nuclear C2 and related systems or to 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 determine, as attackers often use very similar techniques and “delivery vehicles” for their different malware. That said, and while such possible concerns undoubtedly present a growing barrier to US nuclear reductions and the possibility of de-alerting nuclear forces, and a strong rationale for the retention of a strategic nuclear triad to guard against a technological breakthrough in cyber or other counterforce capabilities (see Huessey 2015, Futter and Williams, forthcoming), US thinking is arguably driven more by political rather than strategic dynamics. Essentially, it would be politically very difficult and costly for the current Obama administration (or its successor) to propose to de-alert the 450 Minuteman III ICBMs fielded in silos in the American Midwest, or to introduce new measures of reduced readiness for the current fleet of Ohio class nuclear-armed submarines, especially if these actions 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.

It is of course highly unlikely that either the USA or Russia has plans – or perhaps more importantly, the desire – to fully undermine the other’s nuclear command and control systems as a precursor to some type of disarming first strike, but the *perception* that

nuclear forces and associated systems *could* be vulnerable or compromised is persuasive. Or as Hayes (2015) puts it, “The risks of cyber disablement entering into our nuclear forces are real”. While the growing possibility of “cyber disablement” should not be overstated (notions of a “cyber-Pearl Harbor” (Panetta 2012) or “cyber 9–11” (Charles 2013) have done little to help understand the nature of the challenge), cyberthreats are nevertheless an increasingly important component of the contemporary US–Russia strategic context. This is particularly the case when they are combined with other emerging military-technical developments and programmes. The net result, especially given the current downturn in US–Russian strategic relations, and the way cyber is exacerbating the impact of other problematic strategic dynamics, is that it seems highly unlikely that either the USA or Russia will make the requisite moves to de-alert nuclear forces that the new cyber challenges appear to necessitate, or for that matter to (re)embrace the “deep nuclear cuts” agenda any time soon.

### Assessing the options for arms control and enhancing mutual security

Given the new challenges presented by cyber to both US and Russian nuclear forces and to US–Russia strategic stability, it is important to consider what might be done to help mitigate and guard against these threats, and thereby help minimise the risks of unintentional launches, miscalculation, and accidents, and perhaps create the conditions for greater stability, de-alerting, and further nuclear cuts. While there is unlikely to be a panacea or “magic bullet” that will reduce the risk of cyberattacks on US 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. None, of these however, will be easy.

The most obvious and immediate priority for both the USA and Russia is working (potentially together) to harden and better protect nuclear systems against possible cyber-attack, intrusion, or cyber-induced accidents. In fact, in October 2013 it was announced that Russian nuclear command and control networks would be protected against cyber incursion and attacks by “special units” of the Strategic Missile Forces (*Russia Today* 2014). Other measures will include better network defences and firewalls, more sophisticated cryptographic codes, upgraded and better protected communications systems (including cables), extra redundancy, and better training and screening for the practitioners that operate these systems (see Ullman 2015). However, and while comprehensive reviews are underway to assess the vulnerabilities of current US and Russian nuclear systems to cyberattacks, it may well be that US and Russian C2 infrastructure becomes more vulnerable to cyber as it is modernised and old analogue systems are replaced with increasingly hi-tech digital platforms. As a result, and while nuclear weapons and command and control infrastructure are likely to be the best protected of all computer systems, and “air gapped”<sup>14</sup> from the wider Internet – this does not mean they are invulnerable or will continue to be secure in the future, particularly as systems are modernised or become more complex (Fritz 2009). Or as Peggy Morse, ICBM systems director at Boeing, put it, “while its old it’s very secure” (quoted in Reed 2012).

Another set of options involves examining the potential for cyber arms control agreements, both bilaterally between the USA and Russia, and perhaps multilaterally with other

nuclear-armed and non-nuclear-armed states as well. The first possibility would be the pursuit of some type of international agreement on the prohibition of cyberattack 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 (China, the Russian Federation, Tajikistan and Uzbekistan 2011). Some have suggested that this could potentially mirror the thinking, methods, and mechanisms of previous arms control treaties, notably the 1972 Biological Weapons Convention (see Geers 2010, Fidler 2015), or – perhaps more problematically – 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; clarification of definitions; and conceivably laying the basis for an international organisation to control this (Goldsmith 2011, p. 2). It might also help stave off concerns about a possible US–Russia cyber arms race (Kulikova 2015). However, at 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, verification complications, issues of attribution, and accepted definitions and demarcations (Ford 2010). That said, in 2013 the USA and Russia did agree to establish a “cyber hotline” (Nakashima 2013).

Another possibility would be to consider a more discrete agreement focused primarily on the cyberthreat to nuclear weapons and C2. This might involve a specific bilateral deal or moratoria between the USA and Russia not to target each other’s (and indeed other nuclear powers’) nuclear forces and associated command and control infrastructure (for a discussion of this, see Danzig 2014, p. 26). In fact, given that other nuclear-armed states are also suspected of drawing up plans to target the nuclear weapons infrastructure of their current or possible future adversaries (see Fritz 2009, Keck 2014), it would probably make sense to involve other nuclear-armed parties too. Such an agreement might be pursued through the auspices of the P5 dialogue, the broader framework of the Treaty on the Non-proliferation of Nuclear Weapons or an entirely new organisation or regime. Again, this would be very hard to verify and monitor, and of course would not address actions by third-party actors or terrorist groups. Moreover, as Richard Weitz notes, US–Russian dialogue regarding the possible negative effects of cyber on nuclear forces and strategic stability remains very much in its infancy (Weitz 2015, p. 5). That said this could be an area in which to build confidence between the USA and Russia, and with other nuclear-armed states.

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 US–Russian strategic stability dialogue. While this would unquestionably be the most comprehensive and difficult option, the sustainability of current bilateral arms control accords and certainly any further nuclear reductions talks between the USA and Russia will have to at least address if not formally include discussion and probably some type of agreement about the emerging challenges beyond nuclear weapons. While this would appear to be a logical and perhaps only credible way forward, there are unfortunately considerable political and strategic barriers to achieving this, particularly in the USA, where any future arms control agreement that includes limits on other US systems is unlikely to fare well not only in the Senate, but also in Russia.<sup>15</sup> Essentially, it is very difficult to see any further progress on arms control between the USA and Russia, and therefore the possibility of including other nuclear-armed states in these discussions, if the

whole gamut of technological and military dynamics effecting US–Russian relations and strategic stability are not addressed holistically.<sup>16</sup>

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 regaining a sense of US–Russian strategic stability, confidence building, and shoring up current arms control agreements (see Acton 2012, p. 50). This is likely to mean including cyber, alongside other emerging techno-military dynamics, in US–Russian strategic dialogue and as part of any future formal bilateral agreements. As the Deep Cuts Commission (2015) points out:

While continuing to implement New START, the United States and Russia should resume a comprehensive dialogue across the whole spectrum of strategic stability issues ... concentrating on how to achieve further cuts in the New START limits in strategic offensive forces and addressing the issues of how missile defense and conventional arms impact nuclear arms reductions. (p. 7)

Essentially, it appears that the threat of cyber *disablement* of US and Russian nuclear forces will need to be prioritised and addressed before measures can be taken to mitigate and minimise the possibility that hackers might facilitate a nuclear launch or explosion.<sup>17</sup> Without addressing these concerns now, it is difficult to envisage a credible and efficacious pathway back towards meaningful bilateral or multilateral arms control and disarmament measures in the medium and longer term. That said, it is important to remember that previous bilateral US–Russia arms control agreements have often been instigated during periods of high tension and unease.

### Conclusion: cyber and the future of the US–Russian nuclear relationship

The continued development of offensive cyber capabilities by different actors across the globe is creating a range of new challenges and problems for the safe, secure, and reliable management of US and Russian nuclear forces, and for the US–Russian strategic relationship more broadly. In particular, they increase the risk that hackers might somehow gain access to nuclear C2 systems and either indirectly “spoof” them into believing an attack was underway, or in a worse case scenario directly facilitate the detonation or launch of a nuclear weapon. While the most logical response to this challenge would appear to be de-alerting and reducing US and Russian nuclear forces, enhancing nuclear security measures, as well as working hard to maintain strategic stability, so as to minimise 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 geopolitical environment, neither the USA nor Russia are likely to feel inclined to take any measures to move away from the retention of a sophisticated suit of nuclear capabilities, including forces kept on high alert and able to launch on warning. This is particularly acute for Russia, especially when US cyber capabilities are combined with concerns about the deployment of BMDs, new conventional precision strike technologies, and the increasing problems within the Russian nuclear command and control infrastructure. In this way, cyber is not the main cause of current east–west instability, but rather another factor exacerbating

nuclear insecurity and strategic instability and making it more difficult to rebuild trust and confidence.

While the direct threat to the credibility of US nuclear forces might be comparably less severe than that 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, strategic stability, and further nuclear reductions are, therefore, not particularly encouraging at the time of writing. Nevertheless, it is imperative that both the new challenges presented by cyber and the way that cyber is exacerbating other dynamics undermining US–Russia relations (particularly BMD) be addressed. Indeed, while there may be a number of options to help mitigate the cyberthreat, primarily through arms control measures, moratoria, or better security and cooperation (none of which are straightforward), it is difficult to envisage any progress on any of these measures without considerable improvement in the overall US–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 unauthorised use, we must first focus on US–Russian strategic stability and, particularly, on the new gamut of techno-military challenges – including cyber – that are transforming and, in some cases, undermining this central nuclear relationship. More broadly, it is essential for experts and policy-makers on both sides to keep pace with these new technological developments as they become increasingly central to future US–Russian, and perhaps also global, nuclear stability. While finding a solution to these problems will undoubtedly not be easy, it does appear to be the only credible way to maintain a strong arms control regime and to reinvigorate any serious nuclear disarmament agenda in the medium to long term. This in turn will provide the best defence against the threat of cyberattack and the nightmare scenario of possible future nuclear use.

## Notes

1. The first *Hackers Handbook* was not published until 1986 (see Cornwall 1986), and Tim Berners Lee did not unveil his proposal for a “World Wide Web” until 1989.
2. Since 1993 these missiles have however been de-targeted (or at least aimed into the ocean), although they could probably be re-targeted within a matter of minutes (see Clinton and Yeltsin 1994).
3. The START treaty, signed in 1991, was due to expire on 5 December 2009, and with it would go the associated rigorous inspection regime to ensure compliance by both sides. On this see Sheridan (2010).
4. There is no one accepted definition of “cyber”. The one used here draws on the typology developed by Andres and Winterfeld (2011, p. 167).
5. This builds on the taxonomy provided by Libicki (2007).
6. Attacks designed to appear as though other actors are responsible for committing them.
7. At the time of writing, it is estimated that Russia possesses 7500 nuclear weapons and the US 7100, out of a global total of approximately 15,695 (Ploughshares Fund 2015).
8. Notwithstanding recent concerns about the “go codes” used to launch US nuclear weapons (see Lamothe 2014).
9. For a good overview of various safety measures, see Shultz and Drell (2012), particularly chapters one and two.
10. This is even more worrying if the authority over nuclear forces is pre-delegated to commanders in the field.



11. A logic bomb is a piece of code (malware) that can be activated when certain conditions are met, or when it receives instructions to do so. A backdoor/trapdoor is a way to circumvent security and regain access to systems quickly when required. For a good introduction to the basics of “cyber”, see Singer and Friedman (2014).
12. Russian nuclear early warning systems malfunctioned in 2014, and as of February 2015, Russia has no nuclear-warning satellites in space.
13. The same is also true for China, perhaps even more so. On this see Gompert and Libicki (2014).
14. An “air gapped” computer is physically separated from the wider Internet and from unsecured networks, and therefore cannot (theoretically) communicate with other computers on the other side of the “gap”.
15. It might also necessitate a change of approach (see Peczeli 2014).
16. In fact, as Austin (2015) points out US “cyber superiority, while legal and understandable, is now a cause of strategic instability between nuclear armed powers”.
17. This may be particularly prudent given the likelihood that the threat of cyber disablement will become even more pronounced if and when nuclear numbers are reduced closer towards “minimum deterrent” postures (Cimbala and McDermot 2015, p. 104).

## Disclosure statement

No potential conflict of interest was reported by the author.

## Notes on contributor

**Andrew Futter** is a Senior Lecturer in International Politics at the University of Leicester (UK), 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 cyberthreats and nuclear strategy is funded by the UK Economic and Social Research Council (ESRC) Future Research Leader’s scheme (grant number ES/K008838/1).

## References

- Acton, J., 2012. Bombs away? Being realistic about deep nuclear reductions. *The Washington quarterly*, 35 (2), 37–53.
- Andres, J. and Winterfield, S., 2011. *Cyber warfare: techniques, tactics and tools for security practitioners*. Waltham MA: Syngress.
- Arbatov, A., 16 June 2015. *An unnoticed crisis: the end of history for nuclear arms control?* [online]. Carnegie Moscow Center. Available from: <http://carnegie.ru/2015/06/16/unnoticed-crisis-end-of-history-for-nuclear-arms-control/ians> [Accessed 1 Aug 2015].
- Austin, G., 6 Aug 2015. Cost of American cyber-superiority. *ChinaUSFocus* [online]. Available from: <http://www.chinausfocus.com/peace-security/costs-of-american-cyber-superiority/> [Accessed 10 Aug 2015].
- Bender, B., 2015. Russia ends nuclear security alliance. *Boston Globe*, 19 Jan. Available from: <https://www.bostonglobe.com/news/nation/2015/01/19/after-two-decades-russia-nuclear-security-cooperation-becomes-casualty-deteriorating-relations/5nh8NbtjitUE8UqVWFloL/story.html> [Accessed 14 Oct 2015].
- Berls, B. and Ratz, L., 2015. *RisiNuclear dangers: assessing the risk of nuclear use in the Euro-Atlantic region* [online]. Nuclear Threat Initiative. Available from: [http://www.nti.org/media/pdfs/NTI\\_Rising\\_Nuclear\\_Dangers\\_Paper\\_FINAL.pdf?\\_id=1443443566](http://www.nti.org/media/pdfs/NTI_Rising_Nuclear_Dangers_Paper_FINAL.pdf?_id=1443443566) [Accessed 16 Oct 2015].



- Blair B., 2010. Could terrorists launch America's nuclear missiles? *TIME*, 11 Nov. Available from: <http://content.time.com/time/nation/article/0,8599,2030685,00.html> [Accessed 25 May 2015].
- Blair, B., 2014. *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, 8–9 December, Vienna, Austria. Available from: <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> [Accessed 8 May 2015].
- Blakely, R. and Coghlan, T., 2015. US considers sending missiles to Europe. *The Times*, 6 June. Available from: <http://www.thetimes.co.uk/tto/news/world/europe/article4461950.ece> [Accessed 20 June 2015].
- Burns, R., 2015. Former US commander: take nuclear missiles off high alert. *Associated Press*, 29 Apr. Available from: [http://hosted2.ap.org/APDEFAULT/89ae8247abe8493fae24405546e9a1aa/Article\\_2015-04-29-US-Nuclear-Weapons-Cyber/id-83b7c14d6f504aa2ad2f88b00f7ad5b6](http://hosted2.ap.org/APDEFAULT/89ae8247abe8493fae24405546e9a1aa/Article_2015-04-29-US-Nuclear-Weapons-Cyber/id-83b7c14d6f504aa2ad2f88b00f7ad5b6) [Accessed 2 May 2015].
- Charles, D., 2013. US homeland chief: cyber 9/11 could happen 'imminently'. *Reuters*, 24 Jan. Available from: <http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124> [Accessed 15 Oct 2015].
- China, the Russian Federation, Tajikistan and Uzbekistan, 2011. *Developments in the field of information and telecommunications in the context of international security*. Letter dated 12 September from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary General, A/66/359. Available from: [https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct\\_0.pdf](https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf) [Accessed 18 May 2015].
- Cimbala, S. and McDermott, R., 2015. A new Cold War? Missile defenses, nuclear arms reductions and cyber war. *Comparative strategy*, 34 (1), 95–111.
- Clinton, B. and Yeltsin, B., 14 Jan 1994. *Clinton, Yeltsin reaffirm importance of joint cooperation* [online]. Federation of American Scientists. Available from: <http://fas.org/nuke/control/detarget/docs/940114-321186.htm> [Accessed 15 May 2015].
- Cornwall, H., 1986. *Hackers handbook*. New York: Arthur Brown Company.
- Danzig, R., 2014. *Surviving on a diet on poisoned fruit: reducing the national security risks of America's cyber dependencies* [online]. Center for a New American Century. Available from: [http://www.cnas.org/sites/default/files/publicationspdf/CNAS\\_PoisonedFruit\\_Danzig\\_0.pdf](http://www.cnas.org/sites/default/files/publicationspdf/CNAS_PoisonedFruit_Danzig_0.pdf) [Accessed 2 May 2015].
- Deep Cuts Commission, 2015. *Strengthening stability in turbulent times* [online]. Second Report of the Deep Cuts Commission. Available from: [http://deepcuts.org/images/PDF/Second\\_Report\\_of\\_the\\_Deep\\_Cuts\\_Commission\\_English.pdf](http://deepcuts.org/images/PDF/Second_Report_of_the_Deep_Cuts_Commission_English.pdf) [Accessed 15 June 2015].
- Ewing, P., 2015a. Ash Carter warns Russia on nukes. *Politico*, 23 Feb. Available from: <http://www.politico.com/story/2015/02/ash-carter-russia-vladimir-putin-defense115421.html> [Accessed 25 May 2015].
- Ewing, P., 2015b. The Pentagon's new cyber attack plan: 'blunt force trauma'. *Politico*, 18 Apr. Available from: <http://www.politico.com/story/2015/04/dod-hopes-cyber-can-create-blunt-force-trauma-117095.html> [Accessed 10 May 2015].
- Farnsworth, T., 2013. Study sees cyber risk for US arsenal. *Arms Control Today*, Apr. Available from: [https://www.armscontrol.org/act/2013\\_04/Study-Sees-Cyber-Risk-for-US-Arsenal](https://www.armscontrol.org/act/2013_04/Study-Sees-Cyber-Risk-for-US-Arsenal) [Accessed 16 Apr 2015].
- Fidler, D., 26 Mar 2015. *The relationship between the biological weapons convention and cybersecurity* [online]. Council on Foreign Relations Net Politics Blog. Available from: <http://blogs.cfr.org/cyber/2015/03/26/the-relationship-between-the-biological-weapons-convention-and-cybersecurity/> [Accessed 2 Aug 2015].
- Ford, C.A., 2010. The trouble with cyber arms control. *The new Atlantis*, 29 (Fall), 52–67. Available from: [http://www.thenewatlantis.com/docLib/20110301\\_TNA29Ford.pdf](http://www.thenewatlantis.com/docLib/20110301_TNA29Ford.pdf) [Accessed 4 July 2015].
- Fritz, J., 2009. *Hacking nuclear command and control* [online]. International Commission on Nuclear Non-proliferation and disarmament. Available from: [www.icnnd.org/Documents/Jason\\_Fritz\\_Hacking\\_NC2.doc](http://www.icnnd.org/Documents/Jason_Fritz_Hacking_NC2.doc) [Accessed 5 Jan 2015].

- Fulghum, D., 12 Nov 2013. *Why Syria's air defenses failed to detect Israeli's* [online]. Aviation Week & Space Technology. Available from: <http://www.imra.org.il/story.php3?id=36291> [Accessed 20 May 2015].
- Futter, A.J., 2015a. *Hacking the bomb: nuclear weapons in the cyber age*. Paper presented at the International Studies Annual Conference, 23–27 February, New Orleans. Available from: [https://www2.le.ac.uk/departments/politics/people/afutter/copy\\_of\\_AFutterHackingtheBombISAPaper2015.pdf](https://www2.le.ac.uk/departments/politics/people/afutter/copy_of_AFutterHackingtheBombISAPaper2015.pdf) [Accessed 5 May 2015].
- Futter, A.J., 15 June 2015b. *Cyber threats and the challenges of de-alerting US and Russian nuclear forces* [online]. Nautilus Institute NAPSNet Policy Forum. <http://nautilus.org/napsnet/napsnet-policy-forum/cyber-threats-and-the-challenge-of-de-alerting-us-and-russian-nuclear-forces/> [Accessed 15 June 2015].
- Futter, A.J. and Williams, H.W., forthcoming. Questioning the Holy Trinity: why the US nuclear triad still makes sense. *Comparative Strategy*.
- Futter, A.J. and Zala, B.P., 2013. Advanced US conventional weapons and nuclear abolition: why the Obama plan wont work. *The nonproliferation review*, 20 (1), 107–122.
- Gady, F.-S., 2015. Could cyber attacks lead to nuclear war? *The Diplomat*, 4 May. Available from: <http://thediplomat.com/2015/05/could-cyber-attacks-lead-to-nuclear-war/> [Accessed 10 May 2015].
- Geers, K., 2010. Cyber weapons convention. *Computer law & security review*, 26 (5), 547–551.
- Global Zero Commission on Nuclear Risk Reduction, 2015. *De-alerting and stabilizing the world's nuclear force postures*. Available from: [http://www.globalzero.org/files/global\\_zero\\_commission\\_on\\_nuclear\\_risk\\_reduction\\_report\\_0.pdf](http://www.globalzero.org/files/global_zero_commission_on_nuclear_risk_reduction_report_0.pdf) [Accessed 4 May 2015].
- Goldsmith, J., 2011. *Cybersecurity treaties: a skeptical view* [online]. Koret-taube task force on national security and law, Hoover Institution, Stanford University. Available from: [http://www.hoover.org/sites/default/files/research/docs/futurechallenges\\_goldsmith.pdf](http://www.hoover.org/sites/default/files/research/docs/futurechallenges_goldsmith.pdf) [Accessed 13 June 2015].
- Gompert, D. and Libicki, M., 2014. Cyber warfare and Sino-American crisis instability. *Survival*, 56 (4), 7–22.
- Hayes, P., 17 Feb 2015. *Nuclear command-and-control in the Millenials era* [online]. Nautilus Institute NAPSNet Special Reports. Available from: <http://nautilus.org/napsnet/napsnet-special-reports/nuclear-command-and-control-in-the-millenials-era/> [Accessed 12 Apr 2015].
- Huessy, P., 2015. Want stability? Fund nuke triad modernization. *Breaking Defense*, 23 Feb. Available from: <http://breakingdefense.com/2015/02/want-stability-fund-nuke-triad-modernization/> [Accessed 8 Apr 2015].
- Keck, Z., 2014. S. Korea seeks cyber weapons to target North Korea's nukes. *The Diplomat*, 21 Feb. Available from: <http://thediplomat.com/2014/02/s-korea-seeks-cyber-weapons-to-target-north-koreas-nukes/> [Accessed 10 June 2015].
- Koebler, J., 2012. US nukes face up to 10 million cyber attacks daily. *USNews*, 20 Mar. Available at: <http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily> [Accessed 15 Oct 2015].
- Krickovic, A. and Weber, Y., 30 Sept 2015. *Why a new Cold War with Russia is inevitable* [online]. Brookings Institution. Available from: <http://www.brookings.edu/blogs/order-from-chaos/posts/2015/09/30-new-cold-war-with-russia-krickovic-weber> [Accessed 16 Oct 2015].
- Kristensen, H. and McKinzie, M., 2012. *Reducing alert rates of nuclear weapons* [online]. United Nations Institute for Disarmament Research, Geneva. Available from: <http://www.unidir.org/files/publications/pdfs/reducing-alert-rates-of-nuclear-weapons-400.pdf> [Accessed 15 July 2015].
- Kulikova, A., 2015. Is a cyber arms race between the US and Russia possible? *Russia Direct*, 28 Jan. Available from: <http://www.russia-direct.org/analysis/cyber-arms-race-between-us-and-russia-possible> [Accessed 5 July 2015].
- Lamothe, D., 2014. Air Force swears: our nuke launch code was never '00000000'. *Foreign Policy*, 21 Jan. Available from: <http://foreignpolicy.com/2014/01/21/air-force-swears-our-nuke-launch-code-was-never-00000000/> [Accessed 28 May 2015].
- Lewis, P., et al., 28 Apr 2014. *Too close for comfort: cases of near nuclear use and options for policy*. Chatham House Report. Available at: <https://www.chathamhouse.org/publications/papers/view/199200> [Accessed 14 Oct 2014].

- Libicki, M., 2007. *Conquest in cyberspace: national security and information war*. New York: Cambridge University Press.
- Libicki, M., 2012. *Crisis and escalation in cyberspace*. Santa Monica CA: The RAND Corporation.
- Mearsheimer, J., 2014. Why the Ukraine crisis is the west's fault. *Foreign affairs*, 93 (5), 77–89.
- Mecklin, J., 2015. Disarm and modernize. *Foreign Policy*, 24 Mar. Available from: <http://foreignpolicy.com/2015/03/24/disarm-and-modernize-nuclear-weapons-warheads/> [Accessed 27 Apr 2015].
- Nakashima, E., 2011. Cyber-intruder sparks response debate. *The Washington Post*, 8 Dec. Available from: [http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxlUFGO\\_story.html](http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxlUFGO_story.html) [Accessed 10 May 2015].
- Nakashima, E., 2013. US and Russia sign pact to create communication link on cyber security. *The Washington Post*, 17 June. Available from: [https://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788-11e2-9df4-895344c13c30\\_story.html](https://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788-11e2-9df4-895344c13c30_story.html) [Accessed 9 June 2015].
- Obama, B., 2008. Q and A with President-elect Barack Obama. *Arms Control Today*, Dec. Available from: <http://legacy.armscontrol.org/2008election> [Accessed 10 June 2015].
- Osborn, K., 2015. Russia's satellite nuclear warning system down until November. *Defense Tech*, 20 June. Available from: <http://defensetech.org/2015/06/30/russias-satellite-nuclear-warning-system-down-until-november/>. [Accessed 5 Aug 2015].
- Panetta, L., 11 Oct 2012. *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security*. New York City. Available at: <http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136>. [Accessed 15 Oct 2015].
- Peczel, A., 2014. Negotiated cuts: a new nuclear weapons treaty is not the only option. *Bulletin of the Atomic Scientists*, 27 Jan. Available from: <http://thebulletin.org/negotiated-cuts-new-nuclear-weapons-treaty-not-only-option>. [Accessed 3 June 2015].
- Ploughshares Fund, 23 June 2015. *World nuclear weapon stockpile*. Available from: <http://www.ploughshares.org/world-nuclear-stockpile-report> [Accessed 1 Aug 2015].
- Reed, J., 2012. Keeping our nukes safe from cyber attack. *Foreign Policy*, 25 Sept. Available from: <http://foreignpolicy.com/2012/09/25/keeping-nukes-safe-from-cyber-attack/> [Accessed 15 Apr 2015].
- Remnick, D., 2014. Watching the eclipse. *The New Yorker*, 11 Aug. Available from: <http://www.newyorker.com/magazine/2014/08/11/watching-eclipse> [Accessed 23 May 2015].
- Rodriguez, S., 2015. US tried, failed to sabotage North Korea nuclear weapons program with Stuxnet-style cyber attack. *International Business Times*, 29 May. Available from: <http://www.ibtimes.com/us-tried-failed-sabotage-north-korea-nuclear-weapons-program-stuxnet-style-cyber-1945012> [Accessed 3 July 2015].
- Rose, F., 5 Feb 2015. *Four years in, the New START Treaty still works* [online]. DipNote, the US Department of State Official Blog. Available from: <https://blogs.state.gov/stories/2015/02/05/four-years-new-start-treaty-still-works>. [Accessed 20 July 2015].
- Russia Today, 2013. US nuclear weapons researchers targeted with Internet Explorer virus. *Russia Today*, 7 May. Available from: <http://rt.com/usa/attack-department-nuclear-internet-955/> [Accessed 12 May 2015].
- Russia Today, 2014. Cyber security units to protect Russia's nuclear weapons stockpiles. *Russia Today*, 17 Oct. Available from: <http://rt.com/news/196720-russia-missile-forces-cybersecurity/> [Accessed 4 June 2015].
- Schlosser, E., 2013a. *Command and control*. London: Allen Lane.
- Schlosser, E., 2013b. Neglecting our nukes. *Politico*, 16 Sept. Available from: <http://www.politico.com/story/2013/09/neglecting-our-nukes-96854.html> [Accessed 14 May 2015].
- Shapiro, J.S., 2015. Russian bomber flights buzzing US airspace doubled last year. *The Washington Times*, 8 June. Available from: <http://www.washingtontimes.com/news/2015/jun/7/russian-bomber-flights-buzzing-us-airspace-doubled/?page=all> [Accessed 23 May 2015].
- Sheridan, M.B., 2010. START expiration ends US inspection of Russian nuclear bases. *The Washington Post*, 17 Aug. Available from: <http://www.washingtonpost.com/wp-dyn/content/article/2010/08/16/AR2010081605422.html> [Accessed 28 May 2015].

- Shultz, S. and Drell, S., eds., 2012. *The nuclear enterprise: high consequence accidents: how to enhance safety and minimize risks in nuclear weapons and reactors*. Stanford CA: Hoover Institution Press.
- Simes, D., 2007. Losing Russia: the costs of renewed confrontation. *Foreign affairs*, 86 (2), 36–52.
- Singer, P. and Friedman, A., 2014. *Cybersecurity and cyberwar: what everyone needs to know*. Oxford: Oxford University Press.
- Sokov, S. and Pomper, M., 2014. Is Russia violating the INF Treaty? *The National Interest*, 11 Feb. Available from: <http://nationalinterest.org/commentary/russia-violating-the-inf-treaty-9859> [Accessed 3 June 2015].
- Sputnik News, 19 Aug 2015. Revealed: Russia's new ambitious new ICBM early warning system. Available from: <http://sputniknews.com/russia/20150819/1025927540/russia-nuclear-early-warning-system-development.html#ixzz3jGfJCHj3> [Accessed 14 Oct 2015].
- Ullman, G., 2015. Cybersecurity a rising concern in protecting nuclear stockpile. *Fedscoop*, 10 June. Available from: <http://fedscoop.com/cybersecurity-a-mounting-concern-in-protecting-u-s-nuclear-stockpile> [Accessed 15 June 2015].
- United States Department of Defense, 2013. *Task force report: resilient military systems and the advanced cyber threat* [online]. US Defense Science Board. Available from: <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf> [Accessed 10 Jan 2015].
- Weitz, R., 2015. New technologies complicate US-Russia-China arms control. *World Politics Review*, 28 Apr. Available at: <http://www.worldpoliticsreview.com/articles/15635/new-technologies-complicate-u-s-russia-china-arms-control> [Accessed 6 June 2015].
- Withnall, A., 2015. Vladimir Putin says Russia was preparing to use nuclear weapons 'if necessary' and blames US for Ukraine crisis. *The Independent*, 15 Mar. Available from: <http://www.independent.co.uk/news/world/europe/vladimir-putin-says-russia-was-preparing-to-use-nuclear-weapons-if-necessary-and-blames-us-for-ukraine-crisis-in-crimea-documentary-10109615.html> [Accessed 5 Apr 2015].
- Wolfsthal, J.B., Lewis, J., and Quint, M., 2014. *The trillion dollar nuclear triad* [online]. James Martin Center for Nonproliferation Studies, Monterey, California. Available from: [http://cns.miis.edu/opapers/pdfs/140107\\_trillion\\_dollar\\_nuclear\\_triad.pdf](http://cns.miis.edu/opapers/pdfs/140107_trillion_dollar_nuclear_triad.pdf) [Accessed 23 Feb 2015].
- Yadron, D. and Valentino-Devries, J., 2015. This article was written with the help of a 'cyber' machine: overuse of prefix sparks backlash, but alternatives are few; 'computery'. *The Wall Street Journal*, 4 Mar. Available from: <http://www.wsj.com/articles/is-the-prefix-cyber-overused-1425427767> [Accessed 6 May 2015].
- Zetter, K., 2014. *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. New York: Crown Publishers.