Young Deep Cuts Policy Brief #4

"Hacking" Away at Risks at the Cyber-Nuclear Nexus

By Grace Kier, Lindsay Rand and Tim Thies

Summary

As Russia and the United States modernize their nuclear forces and introduce a growing number of digital components, the surface for possible cyberattacks by an adversary and, thus the risk of nuclear escalation increases. Although the United States and Russia are at odds in numerous arenas, there has historically been political will for cooperation on reducing cyber threats to nuclear forces. Therefore, Washington and Moscow should

- promote discussions on nuclear doctrines taking into account the implications of cyber operations among the P5. China, France, Russia, the United Kingdom and the United States should jointly acknowledge the risks at the cyber-nuclear nexus.
- launch bilateral consultations to gain a better understanding of specific escalation mechanisms and enable decision-makers to exercise restraint in cyber operations. They should start by outlining and jointly evaluating existing internal risk assessment procedures for cyber operations.
- move from a Launch Under Attack (LUA) to a Decide Under Attack (DUA) launch posture, given the compounded risk of accidental escalation from cyber vulnerabilities of nuclear command, control, communications and intelligence (NC3I) and kinetic vulnerability of silo-based missiles.

Major Risks and High Tensions

A formal acknowledgement of the link between the cyber and nuclear realm and unilateral and cooperative efforts to reduce the risks at the cyber-nuclear nexus are key to reducing the danger of inadvertent or accidental nuclear war and could open further opportunities for nuclear arms control. After the June 2021 Geneva Summit between U.S. President Joe Biden and Russian President Vladimir Putin, the bilateral Strategic Stability Dialogue (SSD) is slowly taking shape.[1] The two nations have a positive, fifty-year record of mutual engagement on strategic matters.[2] This may give rise to expectations of a quick fix to the current escalation risks between the two nuclear superpowers. However, simply reapplying the tools from the past century will not suffice to address the dangers emanating from emerging and disruptive technologies in the 21st century.

> *Simply reapplying the tools from the past century will not suffice to address the dangers emanating from emerging and disruptive technologies in the 21st century.*

As U.S. and Russian nuclear arsenals have shrunk after the Cold War, the potential impact of conventional or cyber capabilities on strategic stability is growing. [3] A follow-on agreement to New START based on numerical parity in strategic offensive delivery vehicles, launchers, and associated warheads alone cannot eliminate first-strike incentives or prevent a costly arms race.[4] The emergence of cyber vulnerabilities in the nuclear enterprise especially requires new and innovative steps to reduce the risk of a crisis escalating into nuclear war.

There is an increasing consensus among scholars and policymakers that cooperation on cyber issues is necessary, but the pathway to a verifiable cyber arms control agreement is not yet clear.[5] Fortunately, U.S. and Russian officials seem to be aware of the strategic importance of cybersecurity. Both sides placed the issue on the agenda of the SSD in Geneva and the two governments have already established consultations on the matter.[6] Until recently, the two sides seemed to be in disagreement on the range of topics they want to address in the SSD, with the Biden administration questioning the inclusion of cyber issues in the dialogue.[7] Especially in the United States, recent cases of ransomware attacks against hospital and electricity systems as well as intrusion into information networks critical to national security garnered attention for cybersecurity risks. Impunity for private hacking groups and even more so the delegation of offensive cyber operations to private intermediaries ("proxies") are without any doubt detrimental to peaceful bilateral relations.[8] However, the most serious risks arise at the nexus between the cyber and nuclear spheres. It is therefore an assuring signal that the latter issue was at the center of the cyber discussion as a U.S. State Department official told press reporters after the second round of SSD talks in September 2021.[9]

Exacerbating the risk at the nexus is nuclear modernization which could increase the vulnerabilities of nuclear command, control, communications and intelligence (NC3I) networks to cyberattacks.[10] Thus, in the case of recently

modernized systems, it is especially important to consider scenarios by which a cyberattack on or a misattributed technical failure in NC3I systems could lead to escalation in a crisis or limited conflict. This essay highlights escalation risks at the cyber-nuclear nexus and identifies targeted measures to reduce both the likelihood of trigger events and to mitigate the possible consequences of such incidents. These risk reduction measures consist of confidence-building measures within the P5 process, a relaunch of U.S.-Russian transparency measures and crisis communication channels, and modifications to the existing launch protocol that promote moderated responses requiring sufficient time for information processing.

Evolution of Nuclear Policies and Modernization of Infrastructure

Recent policies and statements from nuclear weapons states (NWS) have suggested that plans for incidence response may transcend the barrier between cyber and nuclear tactics. In the United States, the Trump administration's 2018 Nuclear Posture Review (NPR) declared that "[t]he United States would only consider the employment of nuclear weapons in extreme circumstances to defend the vital interests of the United States, its allies, and partners."[11] Furthermore, the NPR specifies that these circumstances could include significant non-nuclear strategic attacks "on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities."[12] This formulation suggests that the United States might use nuclear weapons in response to a cyberattack against its NC3I capabilities.[13] The Biden administration is in the process of revising the U.S. NPR and it remains to be seen whether it will entail a similarly broad concept of deterrence.

Russia has adopted a similar language to deter potential adversaries from interfering with the infrastructure supporting its nuclear forces. The Basic Principles of State Policy of the Russian Federation on Nuclear Deterrence specify the conditions under which Russia would consider the use of nuclear weapons. These include an "attack by an adversary against critical governmental or military sites of the Russian Federation, disruption of which would undermine nuclear forces response actions."[14] France, the United Kingdom, and China have each acknowledged links between the cyber and nuclear realms, too.[15]

> *At the same time as the United States and Russia adopted a policy of nuclear response to cyber or non-nuclear attacks on nuclear infrastructure, modernization efforts are increasing vulnerabilities of these very systems.*

At the same time as governments are introducing the possibility of nuclear retaliation in response to a cyberattack on NC3I, they are also continuing nuclear modernization efforts. These add further complexity to NC3I networks and provide more gateways for interference with information and communication systems by a potential adversary. As part of the ongoing U.S. modernization process, the Department of Defense plans to introduce digital technologies into many components of the United States' nuclear enterprise, which previously relied on old but secure analogue technology. Delivery

vehicles for strategic nuclear weapons like the Minuteman intercontinental ballistic missiles (ICBMs) will be affected as well as the early-warning satellites, and communication systems designed to transmit launch orders.[16] While the Strategic Automated Command and Control System (SACCS) ran on floppy discs until 2019, replacements will feature state-of-the-art technology.[17] According to a report by the Nuclear Threat Initiative (NTI), "almost 9 out of 10 planned nuclear modernization programs involve at least some new digital components or upgrades."[18] Russia's modernized NC3 assets, too, may well become more vulnerable due to increasingly complex digital components.[19]

However, more digital and more complex components increase the attack surface for cyber operations. In 2013, the U.S. Defense Science Board, an advisory body within the Department of Defense, acknowledged that a highly sophisticated state actor could plant faulty hardware into U.S. NC3I components which, then, could "change the processor output to incorrect results for specified inputs."[20] An affected early-warning system, for example, could fail to transmit its signal despite an incoming missile attack. Similarly, an affected command-and-control system could be manipulated so that launch orders do not reach their addressees. The Defense Science Board warned about the growing vulnerability of ever more complex software and hardware and the difficulty, if not impossibility "to develop components without flaws or to detect malicious insertions."[21] At the same time, risk assessments in the Pentagon's acquisition processes have not kept up with the technological change of the past decade.[22] Cyber aspects are only recently and slowly receiving more attention in risk assessments, which still focus on traditional parameters of performance, costs, and reliability.

Thus, at the same time as the United States and Russia adopted a policy of nuclear response to cyber or non-nuclear attacks on nuclear infrastructure, modernization efforts are increasing vulnerabilities of these very systems.[23]

Essence of Cyber-Nuclear Exposure

Given these projected exposures, what concrete escalation risks arise at the cyber-nuclear nexus and how do these risks differ from pre-existing ones? Nuclear forces have been vulnerable since before the introduction of the Internet and digital technologies. However, the emergence of cyber capabilities as potential means of counterforce attacks leads to different risks than those that traditional, kinetic weapons pose. These risks materialize in different dimensions: increased tendency to risk-acceptant behavior, entanglement of nuclear and conventional command-and-control structures, and most importantly, first-strike pressures due to high levels of mistrust.

The emergence of cyber capabilities as potential means of counterforce attacks leads to different risks than traditional, kinetic weapons: increased tendency to risk-acceptant behavior, entanglement of nuclear and conventional command-and-control structures, and most importantly, first-strike pressures due to high levels of mistrust.

A fundamental problem is the inherent uncertainty about the level of vulnerability of one's NC3I to an adversary's cyber interference. Improved intelligence, surveillance and reconnaissance (ISR) methods – and more recently the growing relevance of open-source intelligence (OSINT) – have improved transparency in the kinetic realm.[24] Moreover, through various arms control treaties the United States and the Soviet Union, and later Russia, agreed on mutual transparency and limitations including adequate verification about the sizes of their strategic nuclear arsenals. By contrast, there is no clear way to gauge and measure an adversary's cyber capabilities or to assess the status of intrusion and the specific areas of vulnerability in one's NC3I networks.

There is no clear way to gauge and measure an adversary's cyber capabilities or to assess the status of intrusion and the specific areas of vulnerability in one's NC3I networks.

Therefore, cyber threats are incompatible with many long-held deterrence concepts. States can "openly advertise [kinetic] weapons to signal the costs of aggression to potential adversaries, thereby reducing the danger of misperception and war."[25] Cyber capabilities, on the other hand, must remain hidden to be effective, as their revelation would give the defender a chance to fix vulnerabilities. The emergence of offensive cyber capabilities can thus blur the certainty about the balance of power, as each state is only aware of its own capabilities against adversary NC3I. In a crisis, such uncertainty can lead to dangerous misperceptions. If each side is only aware of the cyber vulnerabilities of its adversary's forces and unaware of its own vulnerabilities, they might adopt an overly optimistic assessment of the balance of power. As a result, both might take increasingly escalatory actions and mistakenly expect the opponent to back down.[26]

On the other hand, a detected cyberattack against the NC3I system would sow considerable mistrust and fear of further attacks.[27] Notably and adding further instability, actual cyberattacks and false alarms due to technical errors can be difficult to differentiate at first sight.[28] Cyberattacks on nuclear forces and their NC3I systems happen instantaneously, cannot be used for signalling, and often have unpredictable scopes of potential impact. Therefore, even the perception that such an attack against the nuclear forces and associated command, control, communications and intelligence (C3I) might be underway can be highly destabilizing in a crisis or the early stages of a conflict.

Because of the inherent escalation risks of a direct attack on nuclear C3I systems, a state may be more inclined to order limited cyber operations strictly against conventional systems. During a crisis or limited conflict, the attacking state could thereby hope to attain a tactical advantage e.g., by temporarily disabling air defense units or delaying an adversary's possible responses to a conventional attack. At the same time, the expected responses would remain acceptable in terms of scope and intensity.

The problem is that the distinction between C3I nodes for nuclear operations and those for

conventional ones may not always be clear. This increases the possibility for inadvertent escalation, even if decision makers seek to avoid compromising their adversary's nuclear C3I.[29] In fact, several NWS, including Russia and the United States, have C3I components important for both nuclear and conventional operations (dual-use).[30] A state might seek to take out its adversary's conventional command and control system to gain a tactical advantage in a regional conflict and, as a consequence, may degrade its nuclear C3I in the process - possibly triggering a nuclear response.

James Acton identifies three ways in which a perceived attack on dual-use C3I assets could spur inadvertent escalation: a closing "damage limitation window," a misinterpreted warning and crisis instability. First, the target state might anticipate further degradation of its NC3I system and conclude "that its window of opportunity for conducting effective damage-limitation operations might have closed by the time the war turned nuclear."[31] In order to retain its counterforce capability that state might take further escalatory steps, such as attacking anti-satellite weapons deep inside the adversary's territory. Second, unaware of the underlying intentions, the target state might misinterpret the cyberattack as a warning of an imminent nuclear attack as opposed to a conventional operation. It would thus face strong incentives to take escalatory action "to deter the nuclear strike it believed might be coming or to mitigate its potentially calamitous consequences."[32] Third, the commander-in-chief and his or her advisers would face strong pressures for a preemptive strike if they believe that their second-strike capability or enabling capabilities are vulnerable (crisis instability).[33]

In all of these scenarios, the attacking state would have to follow up the cyberattack against adversary C3I with a kinetic attack in order to gain any tangible advantage. Therefore, the vulnerability of NC3I systems to cyber interference and the vulnerability of nuclear forces to kinetic attacks facilitate the above-mentioned escalation mechanisms in conjunction. The danger of cyber interference escalating to nuclear war is especially acute in connection with silo-based ICBMs. By disabling command-and-control or early-warning systems, the attacking state can hope to take out a greater share of vulnerable land-based ICBMs before they can be launched in return.

The danger of cyber interference escalating to nuclear war is especially acute in connection with silo-based ICBMs. By disabling command-and-control or early-warning systems, the attacking state can hope to take out a greater share of vulnerable land-based ICBMs before they can be launched in return.

Compared to road-mobile or submarine-based missiles, silo-based ICBMs are more vulnerable to a preemptive nuclear strike. To mitigate the risk of an incoming first strike destroying their ICBM forces, the United States and Russia have procedures in place, which allow them to launch a retaliatory strike before any detected incoming warheads have detonated (*launch under attack* or LUA).[34] However, under this procedure, leaders would have almost no time to verify and understand the trigger of an early warning signal and face intense pressures to act on

the basis of imperfect information. By implementing a LUA posture, a nuclear weapon state thus accepts the risk that a false alarm might accidentally trigger nuclear war.[35] Growing cyber vulnerabilities in NC3I systems exacerbate this threat as they weaken decision-makers' confidence in the reliability of their forces, incentivize acting on worst-case assumptions and make the escalation scenarios, mentioned above – misinterpreted warning, the closing damage-limitation window and crisis instability – more likely.

Minimizing Impact through Transparency and Exposure Limitation

To rein in the dangers outlined above, the United States and Russia can take several measures unilaterally as well as in a bilateral and multilateral format. The P5 Process provides an opportunity for all five NWS recognized under the Nuclear Nonproliferation Treaty (NPT) to build mutual trust by discussing each other's nuclear doctrines and policies specifically with regard to the escalation risks at the cyber-nuclear nexus. They could explicitly acknowledge these risks in a joint statement. Moreover, Moscow and Washington are already engaged in a cyber-dialogue, which is a promising step for the two countries to find productive bilateral cooperation on this issue.[36] However, to reduce the likelihood of (potential) cyberattacks leading to escalation in the first place, the continuation of bilateral inter-agency meetings and the establishment of confidence-building measures between military staff involved in cyber operations would be necessary. In addition, a more restrained launch strategy is required to reduce the potentially catastrophic consequences of a real or imagined cyberattack on the United States or Russian NC3I systems.

Multilateral Option: Strengthening Predictability and Pledging Mutual Restraint

In preparation for the upcoming 10th NPT Review Conference, delegations of China, France, Russia, the United Kingdom, and the United States (the P5) jointly submitted a working paper on strategic risk reduction, in which they "recommit to taking appropriate measures to reduce strategic risks and promote strategic stability."[37] Among other measures, the P5 pledge to increase mutual trust and understanding through "a structured P5 process discussion on nuclear doctrines and policies" as well as unilateral, bilateral or joint statements "related to the recognition of risk and commitments to collective restraint."[38]

> *The P5 should use the structured discussion on nuclear doctrines and policies as an opportunity to identify specific scenarios in which cyber operations could spark nuclear escalation.*

Like Russia and the United States, the other P5 states have acknowledged the existence of a link between cyber threats and nuclear risk – although with different degrees of explicitness.[39] Therefore, the P5 should use the structured discussion on nuclear doctrines and policies as an opportunity to identify specific scenarios in which cyber operations could spark nuclear escalation. This would increase the predictability of responses to cyber operations against C3I systems, facilitate an improved

understanding of the escalation risks at the cyber-nuclear nexus, and help establish their consideration in planning processes for cyber operations.

It would also serve the P5 to take seriously the call by the Stockholm Initiative on Nuclear Disarmament[40] to reduce nuclear risks emanating from digital technologies and undertake good faith efforts to do so.[41] The P5 should further these discussions on a regular basis during the next NPT review cycle. The participating delegations should include a broad range of personnel involved in and with expertise on nuclear and cyber operations with a sufficient level of seniority to ensure that relevant decision-makers are either involved in the discussions themselves or, if not, participants can brief them directly.

> *A joint statement by which the P5 explicitly acknowledge the link between the cyber and nuclear realms and pledge to exercise restraint in cyber operations can serve as an important reference point for further multilateral risk reduction efforts.*

While a verifiable cyber arms control agreement seems unfeasible in the short-term,[42] China, France, Russia, the United Kingdom, and the United States can still establish norms about responsible state behavior at the cyber-nuclear nexus. Although seemingly trivial, a joint statement by which the P5 explicitly acknowledge the link between the cyber and nuclear realms and pledge to exercise restraint in cyber operations can serve as an important reference point for further multilateral risk reduction efforts. Ideally, such a joint statement could also include a provision of mutual assurance that any decision to conduct such operations against another state's nuclear or dual-use C3I systems are taken only by the head of state or head of government.[43]

Such a clause would not entirely rule out the use of cyber operations against NC3I. At first glance, this may seem more desirable. However, imagine a scenario where a state is certain that a nuclear attack on its territory is imminent and that state has the capability to prevent the attack through cyber and other operations. It would seem hardly credible to give up this option, as a last resort. By assuring each other that only the head-of-state or head-of-government would have the authority to launch such an attack, the P5 could at least signal that they would conduct a cyberattack against adversary nuclear or dual-use C3I networks only after proper consideration of its potentially catastrophic consequences.

Bilateral Option: Reviving Transparency and Confidence-building

Fortunately, Moscow and Washington do not have to start from scratch when it comes to cooperatively reducing the risks at the cyber-nuclear nexus. Already in 2013, Presidents Putin and Barack Obama had established bilateral cooperation formats on information and communications technology.[44] Most importantly, these included a working group to assess and propose joint measures to address security threats in the cyber realm. In addition, both sides established notification exchanges through the Nuclear Risk Reduction Centers to avoid misperception and escalation in the case of "cybersecurity incidents of national concern."[45] Finally, they created a direct

communication link between high-level officials in the White House and the Kremlin to manage any crises arising from security incidents involving information and communications technology.[46]

However, cooperation had come to a standstill amidst the Crimea crisis in 2014, and the Trump administration considered taboo anything that could remind the public of Moscow's interference in the 2016 elections.[47] Now, Presidents Biden and Putin have resumed consultations on cyber issues after the Geneva Summit in June 2021 and have launched expert-level meetings.[48] While the details of the meetings since June remain unknown, Moscow seems intent to relaunch the 2013 transparency and confidence-building measures.[49] The Biden Administration has been under domestic pressure to address broader issues of international cyber security like ransomware attacks. However, while undoubtedly important, Washington should not conflate these other issues with the escalation risks at the cyber-nuclear nexus. For both nations, the reduction of the latter should be an unconditional priority and pursued in the context of strategic risk reduction.

Specifically, Russia and the United States should supplement the expert-level meetings with military-to-military consultations including the personnel concerned with cyber operations and NC3I. Such an exchange would enable both sides to gain a better understanding of the nuclear-conventional entanglements and ensuing escalation risks. This would help reduce the risks of escalation through inadvertent interference in dual-use NC3I components and reduce mistrust in a crisis. Moreover, once the participating military officers fully understand the escalation risks, they will be able to provide better advice to their civilian superiors on offensive cyber operations. This mechanism thus ensures effective civilian authority over impactful decisions and bolsters the credibility of assurances by the two governments.[50] While participants may consider many aspects sensitive, they could start by outlining and jointly evaluating existing internal risk assessment procedures for cyber operations and successively tackle the more delicate issues once the levels of confidence have grown.

Recent developments have sparked optimism about the implementation of such ideas. In October 2021, Russia and the United States submitted a joint draft resolution on information security to the First Committee of the United Nations General Assembly. This marked a significant shift from previous diplomatic competition between two opposing camps.[51] It also demonstrates that, given political will, the two countries can put their differences aside and pursue a result-oriented and pragmatic approach. This gives reason to hope that Moscow and Washington can maintain the current momentum and jointly tackle the risks at the cyber-nuclear nexus.

> *The submission of a single draft resolution on information security to the First Committee of the United Nations General Assembly demonstrates that, given political will, the two countries can put their differences aside and pursue a result-oriented and pragmatic approach.*

Unilateral Option: Additional Guardrails in Launch Policy

As long as reliable technical fixes to the cyber vulnerability of nuclear forces are unavailable, other means must still be considered to address the possibility that a real or imagined cyberattack leads to nuclear annihilation. In light of the combined risks of accidental escalation from NC3I cyber vulnerabilities and kinetic vulnerability of silo-based ICBMs, a change of launch posture is overdue. This holds especially true for the United States, where fixed ICBMs account for 45 percent of deployed warheads.[52] Russia's force structure is less dependent on silo-based ICBMs.[53] But it, too, could limit the danger of accidental nuclear war by changing its nuclear launch policy. Moreover, this measure would not hinge upon agreement with third parties, such as China. This is because Russia and the United States are currently the only states that can effectively launch some of their nuclear forces on warning, although the U.S. Department of Defense expects China to follow suit, in the future.[54]

While even the former Commander of U.S. Strategic Command and Vice Chairman of the Joint Chiefs of Staff James Cartwright endorsed previous calls to de-alert nuclear forces in reducing the danger of a false alarm leading to nuclear war,[55] such a step seems highly unlikely in the current geopolitical environment.[56] However, a more viable short-term measure could be a coordinated shift to a *decide under attack* (DUA) posture.[57] Under DUA, the President would also order a response before the impact of the perceived incoming missiles. Crucially, however, under DUA, a commander-in-chief could opt to have the order implemented only after the detonation of any incoming warheads.[58] Granted, such a delay would risk 'losing' some of the retaliatory potential. However, it would effectively rein in the danger that a false alarm sets off a nuclear war by accident. It allows decision-makers to verify and assess the nature and scope of an expected strike before carrying out a potentially excessive response. The delay also significantly lowers the risk of accidental escalation, as it leaves the President sufficient time to recall a counterattack, should the nuclear attack warning turn out to be a false alarm.

Scholars have raised the risks associated with the LUA posture before.[59] With the introduction of more digital components to NC3I these have become all the more pressing. The emergence of new cyber vulnerabilities creates new sources of potential false alarms. Once decision-makers believe that a cyberattack against their NC3I structure is underway, they would be under heightened alert about an incoming attack at their ICBM force. Such an expectation could give rise to confirmation bias and reinforce the tendency to act upon worst-case assumptions and unconfirmed information.

> *The remote possibility of incurring more damage in a nuclear war is a price worth paying in order to reduce the likelihood that such a war breaks out in the first place.*

At the same time, the main rationale for LUA is eroding. When Moscow and Washington adopted LUA, their nuclear forces were much more reliant on vulnerable ICBMs and bombers. Today, Russia has a large share of its operational warheads deployed on mobile launchers that can hide in vast

deployment areas.[60] Similarly, the United States could increase its reliance on highly survivable SLBMs, which outperform land-based missiles in terms of accuracy.[61] Therefore, damage limitation strategies of both Russia and the United States are today less dependent on vulnerable forces and, by extension, on LUA. The remote possibility of incurring more damage in a nuclear war is a price worth paying in order to reduce the likelihood that such a war breaks out in the first place (see Equation). Thus, the growing risks at the cyber-nuclear nexus are not the sole justification for DUA, but rather ultimately tip the scales against a LUA policy.

Equation

$$\frac{importance\ for\ damage\ limitation\ \searrow}{danger\ of\ inadvertent\ or\ accidental\ escalation\ \nearrow} = net\ benefit\ of\ LUA\ \searrow$$

Recommendations

In order to reduce the risk of a nuclear war at the cyber-nuclear nexus, the United States and Russia should consider these recommendations:

- In the P5 format, Washington and Moscow should promote discussions on nuclear doctrines taking into account the implications of cyber operations. The P5 should jointly acknowledge the risks at the cyber-nuclear nexus.

- Washington and Moscow should launch bilateral consultations in order to gain a better understanding of the specific escalation mechanisms and enable decision-makers to effectively exercise restraint in cyber operations. They should start by outlining and jointly evaluating existing internal risk assessment procedures for cyber operations.

- Given the compounded risk of accidental escalation from cyber vulnerabilities of NC3I and kinetic vulnerability of silo-based missiles, Washington and Moscow should revise their launch postures – moving from Launch Under Attack (LUA) to Decide Under Attack (DUA).

Endnotes

1 Elena Chernenko, “Мы не играем в политические игры вокруг стратегической стабильности [We do not play political games around strategic stability],” Kommersant, September 10, 2021, https://www.kommersant.ru/doc/4977767.
2 Daryl Kimball and Kingston Reif, “U.S.-Russian Nuclear Arms Control Agreements at a Glance,” Arms Control Association, last reviewed April 2020, https://www.armscontrol.org/factsheets/USRussiaNuclearAgreements.
3 Keir A. Lieber and Daryl G. Press, “The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence,” International Security 41, no. 4 (2017): 9-49.
4 Andrey Baklitskiy, Sarah Bidgood and Oliver Meier, “Russian-U.S. Strategic Stability Talks: Where they are and where they should go,” Institute for Peace Research and Security Policy at the University of Hamburg, October 2020, https://deepcuts.org/files/pdf/Deep_Cuts_Issue_Brief_13-Russian_US_Strategic_Stability_Talks.pdf.
5 Götz Neuneck, “More Responsibility for Cyberspace – But How?,” Ethics and Armed Forces, no. 1 (2019): 8, http://www.ethikundmilitaer.de/fileadmin/ethics_and_armed_forces/Ethics-and-Armed-Forces-2019-1.pdf.
6 David Sanger, “Once, Superpower Summits Were About Nukes. Now, It’s Cyberweapons,” New York Times, July 15, 2021, https://www.nytimes.com/2021/06/15/world/europe/biden-putin-cyberweapons.html. RFE/RL, “Biden Warns That Cyberattacks Could Lead To 'A Real Shooting War’,” Radio Free Europe/Radio Liberty, July 28, 2021, https://www.rferl.org/a/biden-cyber-russia-china-/31380148.html.
7 Chernenko, “Мы не играем в политические игры вокруг стратегической стабильности” [We do not play political games around strategic stability].”; Kingston Reif and Shannon Bugos, “U.S., Russia Agree to Strategic Stability Dialogue,” Arms Control Today, July/August 2021, https://www.armscontrol.org/act/2021-07/news/us-russia-agree-strategic-stability-dialogue.
8 Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018).
9 Cited in Matthew Lee, “US-Russia set 2nd round of strategic talks under Biden admin,” Associated Press, September 27, 2021, https://apnews.com/article/joe-biden-russia-geneva-united-states-vladimir-putin-430e037f5c91cfd8d1969450dc9ade4d.
10 Andrew Futter, “War Games Redux? Cyberthreats, US-Russian Strategic Stability, and New Challenges for Nuclear Security and Arms Control,” European Security 25, no. 2 (April 2, 2016): 172, https://doi.org/10.1080/09662839.2015.1112276.
11 U.S. Department of Defense, “2018 Nuclear Posture Review,” U.S. Department of Defense, February 2018, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.
12 U.S. Department of Defense, “2018 Nuclear Posture Review.”
13 Dmitry Stefanovich, “Russia’s Basic Principles and the Cyber-Nuclear Nexus,” European Leadership Network, July 24, 2020, https://www.europeanleadershipnetwork.org/commentary/russias-basic-principles-and-the-cyber-nuclear-nexus/.
14 The Ministry of Foreign Affairs of the Russian Federation, “Basic Principles of States Policy of the Russian Federation on Nuclear Deterrence,” The Ministry of Foreign Affairs of the Russian Federation, June 8, 2020, https://www.mid.ru/en/web/guest/foreign_policy/international_safety/disarmament/-/asset_publisher/rp0fiUBmANaH/content/id/4152094.
15 Stefanovich, “Russia’s Basic Principles and the Cyber-Nuclear Nexus.”
16 Erin D. Dumbacher and Page O. Stoutland, “U.S. Nuclear Weapons Modernization: Security and Policy Implications of Integrating Digital Technology,” Nuclear Threat Initiative, 2020, 11-12, https://media.nti.org/documents/NTI_Modernization2020_FNL-web.pdf.
17 Valerie Insinna, “The US nuclear forces’ Dr. Strangelove-era messaging system finally got rid of its floppy disks,” C4ISRNet, October 17, 2019, https://www.c4isrnet.com/air/2019/10/17/the-us-nuclear-forces-dr-strangelove-era-messaging-system-finally-got-rid-of-its-floppy-disks/.
18 Dumbacher and Stoutland, “U.S. Nuclear Weapons Modernization: Security and Policy Implications of Integrating Digital Technology.”
19 Futter, “War Games Redux?."
20 Defense Science Board, „Resilient Military Systems and the Advanced Cyber Threat,” U.S. Department of Defense, January 2013, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf, 25.
21 Defense Science Board, „Resilient Military Systems and the Advanced Cyber Threat.” Unfortunately, a similarly rigorous analysis for the Russian NC3I system is not available. However, Moscow, too, began to modernize its early-warning systems and military communications satellites after some components had already exceeded their lifetimes. Therefore, the timely completion of the modernization efforts was essential to ensure the continued reliability of Russia’s NC3I system. This suggests that during the modernization process speediness may have received priority over resilience against cyber risks. See: Jason Fritz, “Hacking Nuclear Command and Control,” International Commission on Nuclear Non-proliferation and Disarmament, 2009, https://www.ifap.ru/pr/2009/n090730a.pdf.
22 Futter, “War Games Redux?.”
23 Amy Woolf, “Russia’s Nuclear Weapons: Doctrine, Forces, and Modernization,” Congressional Research Service, September 13, 2021, https://sgp.fas.org/crs/nuke/R45861.pdf.
24 On the function of transparency in the Cuban Missile Crisis, see David G. Coleman, “The Missiles of November, December,

January, February…: The Problem of Acceptable Risk in the Cuban Missile Crisis Settlement,” Journal of Cold War Studies 9, no. 3 (Summer 2007): 5-48. For an overview of accomplishments in OSINT, see The Economist, “The people’s panopticon,” The Economist, November 14, 2013, https://www.economist.com/briefing/2013/11/14/the-peoples-panopticon.

25 Erik Gartzke and Jon R. Lindsay, “Thermonuclear cyberwar,” Journal of Cybersecurity 3, no. 1 (March 2017): 37.

26 Gartzke and Lindsay, “Thermonuclear cyberwar.”

27 Gartzke and Lindsay, “Thermonuclear cyberwar.”

28 Gartzke and Lindsay, “Thermonuclear cyberwar.”

29 James M. Acton, “Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War,” International Security 43, no. 1 (Summer 2018): 56-99.

30 Acton, “Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War.”

31 Acton, “Escalation through Entanglement,” 73-76.

32 Acton, “Escalation through Entanglement,” 72-73.

33 Acton, “Escalation through Entanglement,” 76-82.

34 Steven Starr, Robin Collins, Robert Green, and Ernie Regehr, “New Terminology to Help Prevent Accidental Nuclear War,” Bulletin of the Atomic Scientists, September 25, 2015, https://thebulletin.org/2015/09/new-terminology-to-help-prevent-accidental-nuclear-war/. Cynthia Roberts, “Revelations About Russia’s Nuclear Launch Posture,” War on the Rocks, June 19, 2020, https://warontherocks.com/2020/06/revelations-about-russias-nuclear-deterrence-policy/.

35 Frank von Hippel, “Eliminate the launch-on-warning option for U.S. ballistic missiles,” Physicists Coalition for Nuclear Threat Reduction, November 15, 2020, https://www.aps.org/policy/nuclear/upload/Ending-launch-on-warning.pdf.

36 Jen Psaki, “Press Briefing by Press Secretary Jen Psaki, July 6, 2021,” The White House, July 6 , 2021, https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/07/06/press-briefing-by-press-secretary-jen-psaki-july-6-2021/.

37 2020 Review Conference of the Treaty on the Non-Proliferation of Nuclear Weapons, “Strategic risk reduction: Working paper submitted by China, France, the Russian Federation, the United Kingdom of Great Britain and Nothern Ireland and the United States of America,” December 07, 2021, https://undocs.org/NPT/CONF.2020/PC.I/WP.33, 3.

38 2020 Review Conference of the Treaty on the Non-Proliferation of Nuclear Weapons, “Strategic risk reduction,” 3.

39 Stefanovich, “Russia’s Basic Principles and the Cyber-Nuclear Nexus”.

40 Under the Stockholm Initiative on Nuclear Disarmament, 16 non-nuclear weapon states promote concrete steps towards nuclear disarmament. As of January 2022, the group consists of Argentina, Canada, Ethiopia, Finland, Germany, Indonesia, Japan, Jordan, Kazakhstan, the Netherlands, New Zealand, Norway, the Republic of South Korea, Spain, Sweden and Switzerland. Government Offices of Sweden, “Stockholm Initiative for Nuclear Disarmament,” December 23, 2021, https://www.government.se/government-policy/stockholm-initiative-for-nuclear-disarmament/.

41 2020 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, “A nuclear risk reduction package: Working paper submitted by the Stockholm Initiative , supported by Argentina, Belgium, Canada, Denmark, Ethiopia, Finland, Germany, Iceland, Indonesia, Japan, Jordan, Kazakhstan, Luxembourg, the Netherlands, New Zealand, Norway, South Korea, Spain, Sweden and Switzerland,” May 14, 2021, https://undocs.org/pdf?symbol=en/NPT/CONF.2020/WP.9.

42 Götz Neuneck, “More Responsibility for Cyberspace – But How?.”

43 James M. Acton, “Cyber Warfare & Inadvertent Escalation,” Daedalus 149, no. 2 (April 1, 2020): 145, https://doi.org/10.1162/daed_a_01794.

44 Office of the Press Secretary, “Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building,” whitehouse.gov, June 17, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/joint-statement-presidents-united-states-america-and-russian-federatio-0.

45 Office of the Press Secretary, “FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security,” whitehouse.gov, June 17, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.

46 Office of the Press Secretary, “FACT SHEET: U.S.-Russian Cooperation in Information and Communications Technology Security.

47 Oleg Shakirov, “Putin and Biden’s Cyber Summit,” Russian International Affairs Council, June 29, 2021, https://russiancouncil.ru/en/analytics-and-comments/analytics/putin-and-biden-s-cyber-summit/.

48 Psaki, “Press Briefing by Secretary Jen Psaki, July 6, 2021”. “Путин: хакерских атак с территории РФ проводится в разы меньше, чем из других стран [Putin: hacker attacks from the territory of the Russian Federation are carried out several times less than from other countries]”, TASS, November 30, 2021, https://tass.ru/politika/13067939.

49 “ Заявление Владимира Путина о Комплексной Программе Мер По Восстановлению Российско-Американского Сотрудничества в Области Международной Информационной Безопасности [Vladimir Putin's Statement on a Comprehensive Program of Measures to Restore U.S.-Russian Cooperation in the Field of International Information Security],” President of Russia, September 25, 2020, http://kremlin.ru/events/president/news/64086.

50 Acton, “Cyber Warfare & Inadvertent Escalation:” 144.

51 Oleg Shakirov, “Importance of Russian-U.S. Resolution on Information Security,” PIR Center, November 8, 2021, http://www.pircenter.org/en/blog/view/id/539.
52 Hans M. Kristensen and Matt Korda, “United States nuclear weapons, 2021,” Bulletin of the Atomic Scientists 77, no. 1 (2021): 43-63.
53 Hans M. Kristensen and Matt Korda, “Russian nuclear weapons, 2021,” Bulletin of the Atomic Scientists 77, no. 2 (2021): 90-108.
54 Hans M. Kristensen and Matt Korda, “Chinese nuclear Weapons, 2021,” Bulletin of the Atomic Scientists 77, no. 6 (2021): 322-323.
55 Global Zero Commision on Nuclear Risk Reduction, “De-Alerting and Stabilizing the World’s Nuclear Force Postures,” Global Zero, 2015, https://www.globalzero.org/wp-content/uploads/2018/09/global_zero_commission_on_nuclear_risk_reduction_report_0.pdf.
56 Futter, “War Games redux?”.
57 James a Winnefeld Jr, “A Commonsense Policy for Avoiding a Disastrous Nuclear Decision,” Carnegie Endowment for International Peace, September 10, 2019, https://carnegieendowment.org/2019/09/10/commonsense-policy-for-avoiding-disastrous-nuclear-decision-pub-79799.
58 George Perkovich and Pranay Vaddi, “Proportionate Deterrence: A Model Nuclear Posture Review,” Carnegie Endowment for International Peace, January 21, 2021, https://carnegieendowment.org/files/Perkovich_Vaddi_NPR_full.pdf.
59 See for example Jeffrey Lewis, “Is Launch Under Attack Feasible?,” Nuclear Threat Initiative, August 24, 2017, https://www.nti.org/analysis/articles/launch-under-attack-feasible/.
60 Kristensen and Korda, “Russian nuclear weapons, 2021.”
61 Hans M. Kristensen, Matthew McKinzie, and Theodore Postol, “How US nuclear force modernization is undermining strategic stability: The burst-height compensating super-fuze,” Bulletin of the Atomic Scientists, March 1, 2017, https://thebulletin.org/2017/03/how-us-nuclear-force-modernization-is-undermining-strategic-stability-the-burst-height-compensating-super-fuze/.

About the Authors

Grace Kier is an M.A. student in Russian, East European, and Eurasian Studies at Stanford University. Previously, she was a Junior Fellow in the Russia and Eurasia Program at the Carnegie Endowment. She graduated from the College of William & Mary with degrees in Russian and Government, and has studied in Saint Petersburg and Moscow.

Lindsay Rand is a PhD student at the University of Maryland. Her research focuses on emerging technologies and implications for nuclear deterrence, force structure, and arms control. Her dissertation examines quantum sensing as a specific case study of emerging technologies. She has an MS in nuclear health physics and an MPP in international security.

Tim Thies is a Researcher at the Institute for Peace Research and Security Policy at the University of Hamburg. Previously, he was a Visiting Fellow at the James Martin Center for Nonproliferation Studies. In his research, Tim focuses on arms control and the impact of emerging technologies on strategic stability.

About the Young Deep Cuts Commission

The Young Deep Cuts Commission (YDCC) is a group of twelve young arms control experts from Germany, Russia, and the United States with diverse academic and professional backgrounds. The Young Commissioners develop fresh ideas to strengthen and revitalize nuclear arms control and disarmament. YDCC is part of the Deep Cuts project, an independent, nongovernmental initiative, which provides decision-makers as well as the interested public with concrete policy options based on realistic analysis.

For further information please go to
www.deepcuts.org/young-deep-cuts
@YoungDeepCuts

Impressum

Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH)

Beim Schlump 83
20144 Hamburg, Germany

Phone: +49 (0)40 86 60 77-21
Fax: +49 (0)40 866 36 15

Project Management
Franziska Stärk
Oliver Meier

Email: ydcc@deepcuts.org