Reducing Cyber Risks to Nuclear Weapons: Proposals from a U.S.-Russia Expert Dialogue

SEPTEMBER 2023

NTI
BUILDING A SAFER WORLD

About NTI

The Nuclear Threat Initiative (NTI) is a non-profit, non-partisan global security organization focused on reducing nuclear and biological threats imperiling humanity.

The views expressed in this publication do not necessarily reflect those of the NTI Board of Directors or institutions with which they are associated.

NTI
BUILDING A SAFER WORLD

About the Dialogue

NTI convened a dialogue among nongovernmental U.S. and Russian cyber/information security and nuclear weapons policy experts. Following initial conversations in Moscow in 2019 about the findings from NTI's Cyber-Nuclear Weapons Study Group, the Track II dialogue was established and proceeded virtually in plenary and small-group sessions in 2020 and 2021. The participants are listed in Appendix 1.

Expert participants built on a shared understanding that nuclear weapons systems must be protected from cyber threats, as well as other threats involving information and communications technologies (ICT), and that despite the current geopolitical environment, the unique U.S.-Russian nuclear relationship requires bilateral cooperation to maintain stability. They addressed topics including possible crisis scenarios and escalation pathways, opportunities for building confidence and predictability in the relationship, and bilateral cyber-nuclear norms that could mitigate the risks. The group generated ideas for joint and parallel actions to reduce cyber-nuclear weapons risks for both governments to consider and adopt.

The following recommendations are designed to help avoid or mitigate the risks of a cyberattack prompting a nuclear crisis. The recommendations in this paper offer policymakers in Russia and the United States—and in other countries—options for reducing the risks of a cyber or information security attack that could lead to nuclear war.

Expert participants offered feedback on the draft content and recommendations of this report. Involvement in the dialogue does not imply agreement with each aspect of the report or its recommendations, however.

Contents

Foreword

In the modern nuclear age, there is no more urgent task than understanding and mitigating the potential risks posed by the interaction of advancing cyber capabilities with nuclear weapons systems. In 2016, the Nuclear Threat Initiative convened a study group of distinguished former officials, retired military leaders, and experts in nuclear systems and policy who assessed that a successful cyberattack on U.S. nuclear weapons systems could have catastrophic consequences.[1] They validated the concern that the United States—and all states with nuclear weapons—cannot assume digital components in nuclear weapons, command and control, and warning systems are not, or will not be, compromised. Moreover, technical cybersecurity measures, while critically important, cannot, by themselves, provide sufficient confidence in the security and reliability of critical nuclear systems. Cyber threats to nuclear weapons systems increase the risk of use due to false warning or miscalculation, and could undermine confidence in the nuclear deterrent and further erode strategic stability.

The 2016 study group recommended that the United States, and all countries with nuclear weapons, should take independent steps to reduce cyber-nuclear risks to the greatest extent possible. In that vein, we have been privately and publicly calling for the U.S. government to undertake a comprehensive "nuclear fail-safe review" focused precisely on these issues.[2] The review has now been mandated by law in the Fiscal Year 2022 National Defense Authorization Act and announced by the Biden administration in the 2022 Nuclear Posture Review.

Recognizing that unilateral and technical measures are necessary but insufficient, the 2016 study group also recommended that the U.S. government pursue a global diplomatic approach, given that the implications for strategic stability are global and because other countries with and without nuclear weapons both face and pose cyber threats. Specifically, the report recommended a bilateral dialogue with Russia as a first step, given the mutual responsibility of the world's two largest nuclear powers to avoid the dangerous scenario of nuclear use. The United States and the Russian Federation must work together to develop norms, red lines, and other measures, understanding that a cyberattack could trigger a catastrophic and unintended conflict. How would either side react if the other probes nuclear warning or command-and-control systems? Where is the line between probing and attacking? Could mutual security be enhanced through better understanding of the risks, and are agreements possible to exercise restraint in the cyber-nuclear realm? The tragic Russia-Ukraine conflict makes each of these important questions more urgent and also more dangerous.

Given the obvious sensitivities, it is challenging to have these discussions in official channels with a nuclear competitor, even when relations are less strained than they are currently. Unofficial dialogue between nongovernmental experts can often lead the way by informally exploring and developing ideas and recommendations to governments. That is exactly what we intended when NTI convened American experts to meet with Russian counterparts in Moscow in 2019 to explore cooperation in this area. The effort that ensued through the end of 2021 resulted in deeply substantive discussions and the important recommendations reflected in this report.

There is no more urgent task than understanding and mitigating the potential risks posed by the interaction of advancing cyber capabilities with nuclear weapons systems.

1 The Cyber Nuclear Weapons Study Group's work is summarized in the 2018 report, *Nuclear Weapons in the New Cyber Age: Report of the Cyber-Nuclear Weapons Study Group*, by Page O. Stoutland and Samantha Pitts-Kiefer, Nuclear Threat Initiative (September 2018), https://media.nti.org/documents/Cyber_report_finalsmall.pdf.

2 Sam Nunn and Ernest J. Moniz, "Biden Should Do More to Prevent the Accidental Launch of Nuclear Weapons. Here's How," *Washington Post,* November 17, 2021, https://www.washingtonpost.com/opinions/2021/11/17/biden-should-do-more-prevent-accidental-launch-nuclear-weapons-heres-how. The 2022 National Defense Authorization Act (NDAA) requires the Secretary of Defense to conduct a "fail-safe" review of nuclear weapons, command and control, and the Integrated Tactical Warning and Attack Assessment (ITW/AA) systems.

In light of the conflict in Ukraine, we recognize that this is far from a propitious time to introduce new urgent policy ideas for a bilateral security dialogue, but the cyber-nuclear challenges pose a grave threat to U.S.-NATO and Russia. Today, the conflict tragically grinds on, tensions between the United States and Russia have worsened, and nuclear risks are growing. Even so, President Biden has said the United States is prepared to work on new arms control arrangements with Russia and implementation of New Start continues. Despite the serious differences and frictions in the bilateral relationship, the mutual obligation to prevent nuclear disaster remains paramount. Strategic stability dialogue and arms control negotiations between our countries must resume, and as they do, the topic of reducing cyber-nuclear risks should be high on the agenda. In addition, and particularly when trust between the United States and Russia is very low, both countries should prioritize unilateral actions to reduce nuclear risks. We hope the ideas in this report offer some grist for essential actions and dialogue between the United States and Russia.

Former U.S. Senator Sam Nunn is co-founder and co-chair of NTI. During his 24 years in the U.S. Senate, Nunn served as chairman of the Senate Armed Services Committee and pioneered the Cooperate Threat Reduction Program, which secured and disposed of weapons of mass destruction across the former Soviet republics.

Former U.S. Secretary of Energy Ernest J. Moniz is co-chair and CEO of NTI. Dr. Moniz served as U.S. Secretary of Energy from 2013–2017, during which he was a key negotiator of the historic Joint Comprehensive Plan of Action nuclear agreement between the United States and Iran.

Page Stoutland is a consultant to NTI and former vice president for NTI's Scientific and Technical Affairs Program. Stoutland has held senior positions at Lawrence Livermore National Laboratory, the U.S. Department of Energy, and Los Alamos National Laboratory.

Strategic stability dialogue and arms control negotiations between our countries must resume, and as they do, the topic of reducing cyber-nuclear risks should be high on the agenda.

Principles for Cooperation

In their Joint Statement of June 16, 2021, President Biden and President Putin reaffirmed that a nuclear war cannot be won and must never be fought, echoing the historic 1985 statement by President Reagan and Chairman Gorbachev.[3] But vigilance, creativity, and restraint are required by both countries to ensure that nuclear war never happens, including one inadvertently precipitated by a cyber or information incident or attack.

Bilateral cooperation in this area requires a foundation of shared principles by the United States and Russia, recognizing that:

- The cyber threat to nuclear weapons and related systems, now and into the future, poses a serious risk to strategic stability and security.
- Nuclear weapons systems must be protected from cyber threats, which will require a combination of unilateral and cooperative technical and policy measures. The global cyber threat is likely to grow and worsen in coming years, necessitating an urgency to act now.
- In addition to unilateral actions, and despite the currently low levels of trust, the unique nature of the U.S.-Russian nuclear relationship and the existential nature of the cyber threat to nuclear weapons systems require that parties prioritize finding mutual areas of agreement and cooperation to reduce nuclear risks.
- Monitoring and high-confidence verification of any agreed measures may be very difficult, or even impossible, to achieve. Parties should consider confidence-building, transparency, information-sharing measures, and guidelines for responsible state behavior based on U.S.-Russian best practices, even when technical measures for strict verification are unavailable or impractical.

The cyber threat to nuclear weapons and related systems, now and into the future, poses a serious risk to strategic stability and security.

3 On January 3, 2022, leaders of the five nuclear weapons states recognized in the Treaty on the Non-Proliferation of Nuclear Weapons (NPT)—the People's Republic of China, the French Republic, the Russian Federation, the United Kingdom of Great Britain and Northern Ireland, and the United States of America—affirmed the same: "that a nuclear war cannot be won and must never be fought." Joint Statement of the Leaders of the Five Nuclear-Weapon States on Preventing Nuclear War and Avoiding Arms Races, The White House (January 3, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/03/p5-statement-on-preventing-nuclear-war-and-avoiding-arms-races.

Proposals in Brief

The following six proposals for the United States and Russia are intended to reduce cyber risks to improve strategic stability and avoid a catastrophic use of nuclear weapons.

The United States and Russia should:

1. Refrain from interfering with nuclear weapons and related systems, including nuclear command, control, communications, delivery, and warning systems;
2. Evaluate options to minimize entanglement and/or integration of conventional and nuclear assets;
3. Continue to improve the cybersecurity of their respective nuclear systems;
4. Increase transparency and expand communications during periods of increased tension;
5. Adopt procedures to ensure that any cyber, information, or other operation involving information and communications technologies emanating from the United States or Russia with the potential to disrupt another nation's nuclear deterrence mission be approved at the same level as required for nuclear use;
6. Eliminate policies that threaten a nuclear weapons response to cyberattack.

Various mechanisms to implement these recommendations are available to U.S. and Russian leaders. Some do not require mutual agreement and can be achieved unilaterally. Others should be pursued mutually. The United States and Russia should simultaneously pursue multiple approaches to fully address the range of necessary risk-reduction measures that will minimize the potential for cyber or information operations that prompt a nuclear crisis.

Escalation Risk: From Cyber Operations to Nuclear War[4]

For decades during the Cold War, American and Soviet strategists worried about a "bolt from the blue"—a surprise, large-scale nuclear attack that would cause devastating damage and precipitate an equally devastating nuclear response. But in this century, the primary concern is a miscalculation, misunderstanding, accident, or escalation that triggers the United States or the Russian Federation to use one or more nuclear weapons.

Today, the United States and Russia still possess roughly 90 percent of the world's nuclear weapons and are also among the most proficient and active developers and users of ICT. Nuclear weapons policies, however, have not kept up with these technological advancements. Meanwhile, the ubiquity of advanced digital ICT tools, as well as their fulsome functional benefits, have led both countries' nuclear weapons enterprises to incorporate digital technologies into their nuclear weapons, warning, command, control, and communications systems.[5] With that modernization come vulnerabilities and openness to cyberattacks that could prompt dangerous miscalculations or accidents, leading to nuclear use.

Cyber or ICT attacks heighten the risk of a nuclear weapons launch as a result of misunderstanding, misattribution of actors, or even unauthorized use of a weapon by compromising physical security.[6] In the worst case, leaders could misattribute the source of a cyberattack, lose confidence in their ability to control their nation's nuclear weapons, incorrectly perceive an initiation of a large-scale conflict, or lose confidence in the credibility of their deterrent forces. Any of these situations could prompt a nuclear crisis. These risks are compounded by the broader strained relations between Russia and the United States.

What kind of cyberattacks would be so destructive as to undermine nuclear deterrence? Digital vulnerabilities and offensive cyber activities pose new risks associated with nuclear weapons, including:

Today, the United States and Russia still possess roughly 90 percent of the world's nuclear weapons and are also among the most proficient and active developers and users of ICT. Nuclear weapons policies, however, have not kept up with these technological advancements.

4 Within this paper, "cyber" roughly equals "information and communications technology" (ICT).

5 Erin D. Dumbacher and Page O. Stoutland, *U.S. Nuclear Weapons Modernization: Security and Policy Implications of Integrating Digital Technology*, Nuclear Threat Initiative (November 2020), https://media.nti.org/documents/NTI_Modernization2020_FNL-web.pdf; and Hans M. Kristensen and Matt Korda, "Russian Nuclear Weapons, 2021," *Bulletin of the Atomic Scientists* 77, no. 2, 90–108.

6 Stoutland and Pitts-Kiefer, *Nuclear Weapons in the New Cyber Age*.

- Compromising nuclear weapons, command and control, or conventional military or intelligence, surveillance, and reconnaissance systems;
- Cutting off access to military assets in peacetime and periods of increased tension; and
- Corrupting, spoofing, or poisoning decisionmaker information, or altering automation or machine-learning applications that may be integrated into nuclear weapons systems or operations and used in decision-making support systems.

Any of these intrusions or attacks that disrupt the normal (planned) functioning of the various systems and subsystems for controlling nuclear weapons and their delivery vehicles,[7] whether for espionage or more malicious purposes, could prompt decisions with potential nuclear consequences. Each could lead to incorrect judgments among leaders. The following illustrative scenarios were considered in our bilateral dialogue:

- **Direct cyberattack against nuclear weapons or related systems.** Points of vulnerability in nuclear weapons systems include, but are not limited to:
  - Early warning systems, including radar and satellites, the signals from which could be spoofed or otherwise provide false indications of an attack that could lead to the launch of a nuclear weapon;[8]
  - Communication systems, including means by which presidents and commanders communicate with one another during times of increased tension, and means by which the use of nuclear weapons is authorized;[9]
  - Components used in nuclear weapons delivery vehicles (on bombers, submarines, and ballistic missiles) upon which deterrence policies depend; and
  - Security systems of stockpiles and military bases housing nuclear weapons, compromise of which could result in theft or sabotage of nuclear materials or weapons.

Cyber or ICT attacks heighten the risk of a nuclear weapons launch as a result of misunderstanding, misattribution of actors, or even unauthorized use of a weapon by compromising physical security.

- **Supply chain intervention, espionage, data collection, malware, or malicious code that compromises a nuclear weapon or other elements of the nuclear enterprise, which may result in a loss of confidence in nuclear weapons and related systems operating properly.** Both the United States and Russia rely on varied and diverse suppliers of parts and services to support and modernize their nuclear weapons and other elements of the nuclear enterprise. Modernization efforts underway in both countries will incorporate off-the-shelf or widely available technology of the 2020s, which is likely to consist of largely digital tools. The risks are particularly tangible in efforts to modernize the command, control, and communications systems of nuclear weapons in both countries.[10]

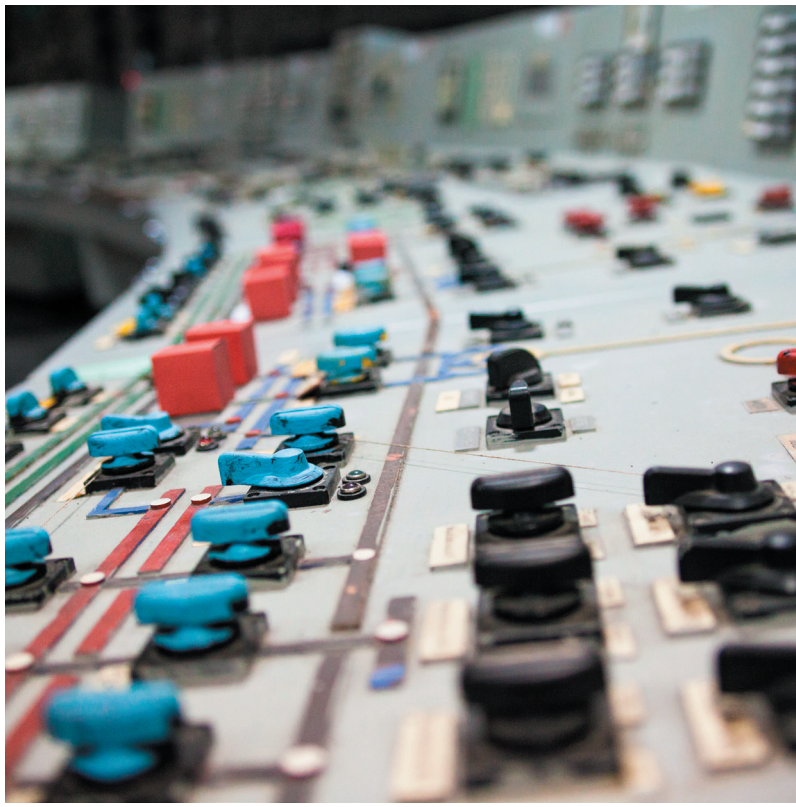
7 N. P. Romashkina, A. S. Markov, D. V. Stefanovich, *International Security, Strategic Stability and Information Technologies* (Moscow: IMEMO, 2020), 98, https://www.imemo.ru/en/publications/info/romashkina-np-markov-as-stefanovich-dv-mezhdunarodnaya-bezopasnosty-strategicheskaya-stabilynosty-i-informatsionnie-tehnologii-otv-red-av-zagorskiy-np-romashkina-m-imemo-ran-2020-98-s.

8 Stoutland and Pitts-Kiefer, *Nuclear Weapons in the New Cyber Age*, 13.

9 P. S. Zo Iotarev, *Approaches to Ensuring Cybersecurity of the Nuclear Weapons Control Systems*, https://www.elibrary.ru/item.asp?id=44185598.

10 V. V. Putin, "Meeting with Heads of Defence Ministry, Federal Agencies and Defence Companies," http://en.kremlin.ru/events/president/news/64396; U.S. Cyberspace Solarium Commission Report, 118, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxlXJGT4yv/view.

- **Communications systems attacks that disrupt or disable communication channels could result in an accidental or ill-advised nuclear launch.** Misinterpretation of information, inability to de-escalate in times of increased tension, or loss of confidence in the ability to issue launch orders to respond to a nuclear attack could prompt authorities in each country to act quickly and decisively but perhaps not wisely.[11] Such an event could be brought on by a remote intrusion or hack, which, for example, could occur when using a control system designed to control both conventional and strategic weapons, sending inaccurate information or false signals via sensors and radars through military chains of command and to leaders. Similarly, an espionage action could be uncovered but misunderstood: for example, what could have been intended as a data-collection action could be perceived as an insertion of malware or some sort of time bomb intended to cause damage. The perpetrator could be a third party (outside of NATO countries or Russia), yet assumed to be either the United States, Russia, or another nuclear-weapons state. Such a discovery could prompt retaliation, potentially escalating to a nuclear response.



Deterrence policies rely on accurate information to be effective and to guard against the precipitation of unintended nuclear war. At the same time, deterrence policies are ineffective against cyber threats.[12] Contemporary history, however, is full of cases where potentially dangerous accidents may have happened but passed without consequence. Some of these were the result of miscalculations, misinterpretations, or misinformation and could have led to a nuclear crisis between the United States and Russia. Greater vulnerability to digital attack and the increased pace of cyber and information attacks threaten the nuclear weapons of both countries (and other countries with nuclear weapons, as well). The United States, Russia, and other nuclear and non-nuclear weapons states are fielding new capabilities in space and missile development, which, combined with growing digital vulnerabilities and a climate of distrust among nuclear-weapon-states, increases risks. Together these pose a heightened need for restraint, transparency, communication, and policy commitments between states with nuclear weapons.

11 Stoutland and Pitts-Kiefer, Nuclear Weapons in the New Cyber Age, 16.

12 Lauren Zabierek, Christie Lawrence, Miles Neumann, and Pavel Sharikov, U.S.-Russian Contention in Cyberspace: Are Rules of the Road Necessary or Possible? Belfer Center Working Paper (June 10, 2021), https://www.russiamatters.org/sites/default/files/media/files/PDF-CyberRulesoftheRoad-061021-RMPaper.pdf.

Proposals for U.S. and Russian Actions

The following describes proposals for U.S. and Russian actions to help avoid a catastrophic use of a nuclear weapon amid cyber threats.

Refrain from Interference in Nuclear Weapons and Related Systems, including Nuclear Command, Control, Communications, and Warning Systems

The United States and Russia should refrain from interfering *with each other's nuclear weapons and related systems, including nuclear command, control, communications (NC3), delivery and warning systems* in peacetime and during periods of increased tension. This would necessitate restraint from attacks, exploitations, and network intrusions—including those for intelligence, reconnaissance, and surveillance purposes—within NC3 and warning systems, thereby avoiding potentially incorrect and catastrophic assessments upon discovery of a perpetrator, malware, or other suspicious indicator.[13]

Attacks, exploitations, or intrusions into the digital elements of nuclear weapons systems—including delivery vehicles and supporting infrastructure, and supply chains—could lead to catastrophic escalation. Periods of increased tension, such as we are facing today, present greater dangers, necessitating additional measures to ensure attacks, exploitations, and intrusions are not misunderstood. Uncertainties about cyber and information security risks to NC3 may grow over time, eroding confidence and raising the risks of misinterpretation and miscalculation should one nation suspect intrusion and risk of attack on NC3 and warning systems.[14] This restraint is also not intended to signal that interference in non-nuclear command, control, communications, and warning assets is permissible, but that interference in nuclear systems is unique in potentially prompting catastrophic escalation.

Attacks, exploitations, or intrusions into the digital elements of nuclear weapons systems—including delivery vehicles and supporting infrastructure, and supply chains—could lead to catastrophic escalation.

To implement this recommendation, we propose the following steps:

- **Clarify relevant systems.** Creating concrete definitions of which assets support nuclear, conventional, or dual missions could reduce the risk that an action intended to disrupt or damage conventional military command, control, and communications systems could spur a nuclear response.
- **Refrain from digital intelligence gathering within one another's NC3 systems during peacetime.** If agreements could be reached and monitored to assure that certain systems would be off-limits for espionage purposes, it could reduce the risk of intelligence gathering being mistakenly interpreted as a damaging attack. Such a commitment or even the loss of intelligence would not pose real threats to the strategic calculations of either U.S. or Russian decisionmakers.[15] However, such an approach does not solve the problem of third parties that could attack these networks. Nevertheless, it would be a significant starting point and would require additional investment and R&D on possible monitoring and verification methods. Such commitments can also be initiated in a unilateral manner as a "non-targeting pledge," or perhaps as a *"voluntary commitment."*

13 Inclusive of computer network attacks (CNAs), computer network exploitations (CNEs), and other espionage within and across sensitive systems.

14 Richard J. Danzig, *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*, Center for a New American Security (July 2014), 24–25, https://www.cnas.org/publications/reports/surviving-on-a-diet-of-poisoned-fruit-reducing-the-national-security-risks-of-americas-cyber-dependencies.

15 If information were to be gained through espionage of these assets, it would not likely be determinative and therefore of limited utility.

- **Refrain from interference in nuclear weapons.** Infiltration or intrusion into the digital systems of a nuclear weapons delivery vehicle, a known supplier of nuclear deterrence capabilities, or a nuclear bomb or warhead—when discovered or even suspected—could trigger miscalculation. A real or perceived attack on any infrastructure underpinning nuclear deterrence, including the industrial base or infrastructure, such as warhead production and safety processes, could be perceived as the beginning of the use of a nuclear weapon.

- **Do not aid, sponsor, or provide support for another state or non-state actor to interfere in the nuclear weapons or supporting systems of a party in compliance with the Treaty on the Non-Proliferation of Nuclear Weapons (NPT).** Interference in any country's dual-use or NC3 and warning systems, even if unintentional, could lead to catastrophic escalation as a result of miscalculation. To avoid miscalculations, the United States and Russia should commit not to interfere in the nuclear weapons enterprises—including the nuclear fuel cycle—of any country in compliance with its obligations under the NPT.

- **Commit publicly.** The United States and Russia should make formal assurances and political commitments, through declaratory policy, to refrain from digital intelligence gathering and interference in nuclear weapons and related systems, including dual-use systems. In addition, the United States and Russia should commit not to aid or support such interference by another state or non-state actor. Such public commitments would send important signals of policy and intent to domestic and global audiences.

Evaluate Options to Minimize Entanglement and/or Integrate Conventional and Nuclear Assets

Both the United States and Russia are modernizing their nuclear forces, potentially integrating new digital vulnerabilities into existing nuclear delivery vehicles and warning, command, control, and communications systems. Some have suggested that technical parity may now be more important than a numerical balance.[16] These investments present an opportunity to isolate or shield nuclear systems from both civilian infrastructure and non-nuclear command and control systems. Integrating conventional military and nuclear systems, including those in orbit, risks escalation in periods of increased tension, although defining the dividing line between conventional and nuclear systems can be difficult.[17] To reduce the risk of escalation, the United States and Russia should:

- **Evaluate, to the extent possible, the potential for separation and isolation of conventional and nuclear command and control systems.** Recognizing that completely separating systems from NC3 systems would be expensive, modernization efforts should proceed with the recognition that integrating nuclear and conventional military systems might raise escalatory risks. Where separation is not possible, other arms control, confidence-building, and transparency measures should be devised to compensate.[18]

- **Reduce nuclear system links to critical national assets.** The United States and Russia should also consider separating and isolating nuclear weapons, including NC3 systems from critical national assets, to the extent possible. These separations could include isolation from satellite networks with significant civilian and commercial impact (e.g., the U.S. Global Positioning System (GPS) and the Russian Global Navigation Satellite System (GLONASS)).

- **Reduce nuclear system links to civilian critical infrastructure.** Although the United States and Russia have agreed[19] to not attack critical civilian infrastructure, links between nuclear systems and civilian infrastructure should be reduced to avoid the potential for unintended consequences in the event that cyberattacks do occur.

16 S. M. Rogov, "Global and Regional Stability in a Nuclear World," *Bulletin of the Russian Academy of Sciences* 91, no. 6 (2021): 571–584.

17 See Alexey Arbatov, Vladimir Dvorkin, and Petr Topychkanov, *Entanglement as a New Security Threat: A Russian Perspective*, Carnegie Endowment for International Peace (November 8, 2017), https://carnegieendowment.org/2017/11/08/entanglement-as-new-security-threat-russian-perspective-pub-73163; 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): 56–9, https://doi.org/10.1162/isec_a_00320.

18 P. S. Zolotarev, *Approaches to Ensuring Cybersecurity of the Nuclear Weapons Control Systems*, https://www.elibrary.ru/item.asp?id=44185598.

19 Such as the United Nations Groups of Government Experts reports, including "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," United Nations General Assembly, A/70/174 (July 22, 2015), 8, item (f), https://digitallibrary.un.org/record/799853?ln=en. The recent events in Ukraine, unfortunately, call this commitment into question.

Continue to Improve Cybersecurity of Nuclear Systems

Modern nuclear weapons in the United States and Russia include some digital and automated systems. Adding digital tools carries potential benefits but also significant risks, including some that are not fully understood. To reduce these risks, the United States and Russia should:

- **Conduct unilateral fail-safe reviews to understand and identify steps to reduce vulnerabilities in warning, command, control, and communications systems for nuclear weapons, as well as in nuclear weapons and delivery vehicles that may be introduced or exacerbated by cyber threats.** An internal review to affirm that any nuclear system problems would be "fail-safe" would strengthen internal safeguards against cyber threats. Such reviews should be done at a classified level as needed.
- **Prioritize digital security and reliability alongside cost, schedule, and performance for all operating systems, as well as in acquiring and procuring nuclear weapons and related systems in the context of nuclear modernization and increasing reliance on digitization.** Such prioritization may necessitate compromises to functional technology advantages in service of security and reliability. In both the United States and Russia, digital systems should meet clearly established security and reliability thresholds before being adopted into the service. Resources should be allocated to test and establish that leaders and militaries can retain confidence that their nuclear forces will always be ready if needed, but never used without proper authorization due to cyber/information attacks.[20]

20 Dumbacher and Stoutland, *U.S. Nuclear Weapons Modernization*, 30–2.

Increase Transparency and Communication

Improved transparency and communication would improve stability and reduce risks of miscalculation, particularly during periods of increased tension. Regular, ongoing, high-level strategic stability dialogues and other exchanges (e.g., military-to-military exchanges) help to build a broader environment of understanding and trust. The approaches described below, if adopted, could help guard against potentially dangerous miscalculations or blunders.

- **Deploy the "cyber hotline" communications channel more readily, ideally within hours of an incident, suspected disruption, destruction, or otherwise destabilizing cyber activity related to nuclear weapons or related systems.** Quicker, collaborative, and more thorough use of emergency communications channels is necessary to avert both nuclear miscalculation and cyber confrontation. Engagement via diplomatic channels can help ascertain and verify the source of an attack or technical failure and avoid mistaken attribution. The existing risk-reduction center communications channels are not survivable links to connect leaders in times of nuclear crises, however. Secure communication channels to connect U.S. and Russian leaders should be established.

- **Terms of use of the communications channels should be better established between the United States and Russia, including the type of content expected to be shared (e.g., the degree to which tactics, techniques, and procedures can and should be shared), to avoid unhelpful or ineffective collaboration.** Leaders and their teams should make better use of the official communications channels by clarifying the purpose of their use. Existing practices for using "hotlines" or risk-reduction centers—originally devised to reduce escalatory and nuclear risks between Russia and the United States—are valuable, but insufficient.

- **To avert miscalculations, enhance communications between military leaders at different levels and establish practices of providing notice of cyber trainings and exercises, or military exercises with cyber components, modeled on the 1972 Incidents at Sea agreement between the United States and U.S.S.R., which enables information sharing to help clarify military activities at sea.** The approach could reduce the possibility of conflict by accident or miscalculation in the same way the Incidents at Sea agreement provides clarity about the movement of ships and aircraft. Both Russia and the United States have previously proposed such an agreement to alleviate cyber-nuclear risks.[21]

- **Increase transparency by sharing data on ballistic missile launches, to include launches from nation states and commercial entities.** Given the proliferation of global space and missile launches, gathering a list of all anticipated launches by drawing on public and private channels is an extensive task. A shared data source collating only already-public and official, unclassified information could improve the scope and timeliness of launch data, against which the military officers could verify warning signatures. Although physical locations for such data-exchange centers could be considered, virtual centers may be viable and more feasible. China could also be invited to join in such a virtual center.

- **Engage in consultations with other countries.** Dialogue on cyber-nuclear risks is critical for U.S.-Russian relations, but cybersecurity is also a global challenge. The United States and Russia should seek ways to discuss cyber-nuclear risks with other countries including China, France, India, Pakistan, and the United Kingdom. Most urgent tracks for cooperation should include exchanging information about cyber threats and challenges and best practices on addressing them.

21 American diplomats have proposed such an approach dating to at least 2017; President Putin of Russia recommended the approach in "Statement by President of Russia Vladimir Putin on a Comprehensive Program of Measures for Restoring the Russia–U.S. Cooperation in the Field of International Information Security," September 25, 2020, http://en.kremlin.ru/events/president/news/64086.

Joint Data Exchange Center

On June 4, 2000, the U.S. and Russian presidents signed a Memorandum of Agreement establishing a Joint Center for the Exchange of Data from Early Warning Systems and Notifications of Missile Launches (JDEC) in Moscow, for the exchange of information derived from each side's warning systems on the launches of ballistic missiles and space-launch vehicles. The stated purpose of the agreement was to strengthen strategic stability by further reducing the danger that ballistic missiles might be launched on the basis of false warning of attack, and to promote increased mutual confidence in the capabilities of the ballistic missile early warning systems of both sides. The agreement was the first time the United States and Russia agreed to a permanent joint operation involving U.S. and Russian military personnel.

The JDEC was to be staffed 24 hours a day, seven days a week, with American and Russian personnel. It would also serve as the repository for the notifications to be provided as part of an agreed system for exchanging pre-launch notifications of the launches of ballistic missiles and space-launch vehicles, negotiated separately.

Although the parties expended considerable effort for more than a decade, the JDEC failed to produce a tangible result. Failure to resolve issues associated with taxes and liabilities—and increasing Russian concerns over U.S. policies on missile defense—effectively stalled progress. In 2009, the U.S. and Russian presidents agreed to pursue the long-stalled activation of the JDEC, for the stated purpose of becoming "the basis for a multilateral missile-launch notification regime," but that effort also failed to produce the intended result.

Since JDEC was first discussed, significant global proliferation of advanced missile systems, and advances in missile technology and launch-detection sensors, have dramatically altered the strategic landscape. The original rationale for the JDEC—to reduce the danger that ballistic missiles might be launched on the basis of false warning of an attack and increase mutual confidence—persists. Moreover, the depth of these concerns has been amplified by the threat of cyberattacks on NC3 structures and early warning systems.

These significant changes suggest that the JDEC concept should be revisited and that a broadened scope may be beneficial.

Consistent with the general intent of the original JDEC agreement, nations could share information from their respective satellite and radar sensors on the launch of missiles and space-launch vehicles. In contrast to the original concept, however, advances in communication technology enable consideration of a virtual center, potentially avoiding some of the pitfalls of the original agreement. In addition, the cyber and space domains, not envisioned in the original agreement, could be considered for inclusion.

Finally, including other countries could be considered. NATO and/or China could be brought into the initiative and agreement, either at the outset or later. Other countries could be added, as agreed by the parties to the agreement, making it a truly "global" center.

Elevate Approval Authority for Cyber, Information, or Any Other Operation Involving ICTs

A cyber or information operation with the potential to disrupt a nation's nuclear deterrence mission should be approved at the same level as required for nuclear use. This policy would ensure that cyber operations with the potential to impact nuclear systems of another country would have the explicit knowledge and approval of the same officials who would authorize use of a nuclear weapon. Toward this end, the United States and Russia should:

- **Ensure cyber, information, or any other operation involving ICTs with the potential to disrupt another nation's nuclear deterrence mission are approved by the same officials with authority for ordering use of a nuclear weapon.** This commitment would ensure that the most sensitive and potentially escalatory cyber and information operations have the explicit approval of the same leader responsible for the most significant of military decisions, use of a nuclear weapon. This change would not necessarily alter existing policy for cyber or information operations that do not have the potential to impact nuclear deterrence missions.
- **In addition, the United States and Russia should commit to enhance oversight of and take legal action to minimize or halt any non-state cyber or information operations emanating from their territory that have the potential to influence or harm nuclear deterrence and stability.** Government situational awareness should extend to non-military and non-state actors' cyber or information activities that could lead to catastrophic nuclear risks. This concept builds on the existing agreement between the United States and Russia that "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs."[22]

Eliminate Policies That Threaten Nuclear Response to Cyberattack

The United States and Russia should narrow the circumstances under which they would consider a nuclear response and should not threaten a nuclear response to a cyberattack. Cyberattacks can be deterred and/or followed by more proportionate responses, thereby increasing the credibility of cyber as well as nuclear deterrence. Previously established American and Russian nuclear policies have not yet fully addressed the risks of cyber insecurity and may, in their current form, increase the potential for use of a nuclear weapon.

The United States and Russia should:

- **Revise policies, posture, and force-planning documents to reduce the potential for nuclear response to cyberattacks.** Political commitments are a way of communicating intent and can help avert misinterpretation and actions that could lead to inadvertent nuclear war. Policy, force posture, and doctrine should not signal an intention to wage a nuclear attack against the perpetrator of a cyber or information attack, even if those responses are considered to be non-nuclear strategic attacks. A potentially important exception could be to maintain the option for nuclear retaliation against a cyberattack that severely impacts nuclear weapons command, control, communications, or warning systems.[23]

22 Report of the UN GGE 2015 (later adopted by the U.N. General Assembly Resolution A/RES/70/237), https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F70%2F237&Language=E&DeviceType=Desktop&LangRequested=False.

23 This recommendation would work in tandem with the recommendations regarding the need for clarification of which systems are critical to the nuclear deterrence mission and for restraint in conducting cyber or information intrusions, or intelligence probing in them.

Implementation

Various mechanisms to implement these proposals are available to U.S. and Russian leaders, ranging from declaratory policy changes, to mutual political commitments, to changes in internal acquisitions and management procedures. To fully address the range of risk-reduction measures that will minimize the potential for cyber operations to prompt a nuclear crisis, the United States and Russia should pursue multiple approaches.

New or revised political commitments, strategic stability dialogues, and unilateral actions can be leveraged to address cyber issues and reduce risks. Changes in formal declaratory policy commitments could reduce the risk that miscalculation could prompt a nuclear crisis. In strategic stability talks, refraining from interference in nuclear weapons and NC3 systems could be discussed. The United States and Russia could also opt to share information that would build understanding and set expectations in a crisis situation. In addition, each state should undertake unilateral actions, such as conducting extensive fail-safe reviews of their respective nuclear systems. In the near term, the two governments should also consider participating in track 1.5 dialogues to develop ideas and work through challenges of some of the more practical considerations in this report, such as the joint exchange of missile launch data.

In the mid- to long-term, cybersecurity can be improved in the context of ongoing nuclear weapons systems modernization. Mutual commitments can be codified through various political or legal formats. Nuclear force modernization in each country presents an opportunity to clarify, isolate, and distinguish which systems are involved in nuclear deterrence missions from civilian infrastructure, critical national assets, and conventional warfighting systems. Modernization also provides opportunities to improve system resiliency and upgrade cybersecurity measures and practices. Both the United States and Russia should prioritize cyber-nuclear weapons risk-reduction as they pursue future bilateral and multilateral arms control, confidence-building, and transparency initiatives.

Appendix 1: Track II Participants

U.S./U.K. Participants

Steve Andreasen | National Security Consultant, NTI

Madelyn Creedon | Former Principal Deputy Administrator, National Nuclear Security Administration and former Assistant Secretary of Defense for Global Strategic Affairs

Erin Dumbacher | Senior Program Officer, Scientific and Technical Affairs, NTI

Michael Elliot | Former Deputy Director for Strategic Stability, Department of Defense, Joint Staff

Andrew Futter | Professor of International Politics, Leicester University

Herb Lin | Senior Research Scholar, Center for International Security and Cooperation, Stanford University

Chris Painter | President, The Global Forum on Cyber Expertise, Stanford University, Commissioner, Global Commission on the Stability of Cyberspace

Lynn Rusten | Vice President, Global Nuclear Policy Program, NTI

Page Stoutland | Consultant and Former Vice President, Scientific and Technical Affairs, NTI

Russian Participants

Viktor Esin | Leading Research Fellow, Department for Military-Political Research, ISKRAN, former Head of Staff of Strategic Rocket Force, Col. General (ret.)

Vadim Kozyulin | Project Director, Emerging Technologies and Global Security Project, PIR Center

Oleg Krivolapov | Research Fellow, Department of Military-Political Studies, ISKRAN

Sergei Rogov | Academic Director, ISKRAN, Russian Academy of Sciences Full Member

Yuri Ryzhikh | Specialist at the Russian Space Systems Company, Colonel (ret.)

Pavel (Pasha) Sharikov | Leading Research Fellow, Institute of Europe, Russian Academy of Sciences

Dmitry Stefanovich | Research Fellow, Department of Military and Economic Security Research, IMEMO

Nataliya Stepanova | Research Fellow, Department of Military-Political Studies, ISKRAN

Elena Zinovieva | Associate Professor, Department of World Politics, Deputy Director, Centre for International Information Security, Science and Technology Policy MGIMO-University

Pavel Zolotarev | Leading Research Fellow, Head of the Department of Military-Political Studies, ISKRAN, Major General (ret.)

Acknowledgments

Discussing cyber threats to nuclear weapons and related systems, a sensitive topic, is challenging even outside of government. We are thankful to everyone involved, as well as their host organizations, for taking on such an important, but difficult topic.

This project spanned several years and included meetings in Moscow and over Zoom, as necessitated by the pandemic. We owe a debt of gratitude to the individuals who participated in this effort. These are some of the most highly respected experts from around the world, and they were extremely generous with their time.

At NTI, we thank former Senator Sam Nunn, former Secretary of Energy Ernest J. Moniz, and NTI President Joan Rohlfing for their vision and leadership on reducing nuclear threats globally. We are also grateful for the work of NTI staff, past and present, including Erin Dumbacher, Lynn Rusten, Steve Andreasen, and NTI's communications team. We are particularly in debt to our executive assistant Catherine Crary for her excellent work.

We send our sincerest thanks to all who remain personally committed to reducing global cyber-nuclear risks, despite the challenges of the current geopolitical situation.

Page Stoutland

Снижение кибер-рисков для ядерного оружия: предложения по итогам российско-американского экспертного диалога

СЕНТЯБРЬ 2023

NTI
BUILDING A SAFER WORLD

О NTI

Инициатива по сокращению ядерной угрозы (Nuclear Threat Initiative – NTI) – это некоммерческая, непартийная организация, занимающаяся вопросами глобальной безопасности и направленная на снижение ядерных и биологических угроз, угрожающих человечеству.

Мнения, выраженные в данной публикации, не обязательно отражают точку зрения Совета директоров NTI или учреждений, связанных с ним.

NTI
BUILDING A SAFER WORLD

О диалоге

NTI организовала диалог между неправительственными американскими и российскими экспертами по кибер/информационной безопасности и политике в области ядерного оружия. После первых бесед в Москве в 2019 году о выводах Исследовательской группы NTI по киберядерному оружию был установлен диалог по Треку II, который продолжался виртуально на пленарных заседаниях и заседаниях малых групп в 2020 и 2021 годах. Список участников приведен в Приложении 1.

Эксперты основывались на общем понимании того, что системы ядерного оружия должны быть защищены от киберугроз, а также других угроз, связанных с информационно-коммуникационными технологиями (ИКТ), и что поддержание стабильности уникальных американо-российских ядерных отношений требует двустороннего сотрудничества, даже несмотря на текущую геополитическую обстановку. Были рассмотрены такие темы, как возможные сценарии кризиса и пути эскалации, возможности для укрепления доверия и предсказуемости в отношениях, а также двусторонние киберядерные нормы, которые могут снизить риски. Группа выработала идеи совместных и параллельных действий по снижению рисков, связанных с киберядерным оружием, для рассмотрения и принятия правительствами обеих стран.

Приведенные ниже рекомендации призваны помочь избежать или снизить риски кибератаки, которая может привести к ядерному кризису. Рекомендации, приведенные в данной статье, предлагают политикам в России и США, а также в других странах варианты снижения риска кибератаки или атаки на информационную безопасность, которые могут привести к ядерной войне.

Участники-эксперты высказали замечания по проекту содержания и рекомендаций данного отчета. Однако участие в диалоге не означает согласия с каждым аспектом отчета или его рекомендациями.

Оглавление

Предисловие

В современный ядерный век нет более актуальной задачи, чем понимание и смягчение потенциальных рисков, возникающих при использовании кибернетических систем для управления ядерным оружием. В 2016 году Инициатива по сокращению ядерной угрозы созвала исследовательскую группу, в которую вошли видные бывшие государственные служащие, отставные военачальники и эксперты по ядерным системам и политике, которые пришли к выводу, что успешная кибератака на системы ядерного оружия США может иметь катастрофические последствия.[1] Они подтвердили обеспокоенность тем, что Соединенные Штаты и все государства, обладающие ядерным оружием, не могут рассчитывать на то, что цифровые компоненты ядерного оружия, систем управления и предупреждения не скомпрометированы или не будут скомпрометированы. Более того, технические меры кибербезопасности, несмотря на их исключительную важность, сами по себе не могут обеспечить достаточную уверенность в безопасности и надежности критически важных ядерных систем. Киберугрозы системам ядерного оружия повышают риск применения из-за ложного предупреждения или просчета, могут подорвать доверие к силам ядерного сдерживания и еще больше подорвать стратегическую стабильность.

Исследовательская группа 2016 года рекомендовала Соединенным Штатам и всем ядерным державам предпринять самостоятельные шаги по максимально возможному снижению киберядерных рисков. В связи с этим мы частным образом и публично призываем правительство США провести всеобъемлющий «обеспечивающий высокую надежность обзор ядерной безопасности», сфокусированный именно на этих вопросах.[2] В настоящее время проведение обзора предписано на законодательном уровне в Законе о полномочиях в области национальной обороны от 2022 года и объявлено администрацией Байдена в Обзоре ядерной политики за 2022 год.

Признавая, что односторонние и технические меры необходимы, но недостаточны, исследовательская группа 2016 года также рекомендовала правительству США применять глобальный дипломатический подход, учитывая, что последствия для стратегической стабильности носят глобальный характер и что другие страны — как с ядерным оружием, так и без него — сталкиваются с киберугрозами и сами представляют их. В частности, в качестве первого шага в докладе рекомендуется провести двусторонний диалог с Россией, учитывая взаимную ответственность двух крупнейших ядерных держав мира за то, чтобы избежать опасного сценария применения ядерного оружия. Соединенные Штаты и Российская Федерация должны совместно разработать нормы, «красные линии» и другие меры, понимая, что кибератака может вызвать катастрофический и непреднамеренный конфликт. Как отреагирует любая из сторон, если другая сторона решит проверить в деле свои ядерные системы предупреждения или управления? Где грань между проверкой и нападением? Можно ли повысить взаимную безопасность за счет лучшего понимания рисков, и возможно ли достижение соглашений о проявлении сдержанности в киберядерной сфере? Трагический конфликт между Россией и Украиной делает каждый из этих важных вопросов более актуальным, а также более опасным.

Учитывая очевидную деликатность, сложно вести такие обсуждения по официальным каналам с ядерным конкурентом, даже когда отношения менее напряженные, чем сейчас. Неофициальный диалог между неправительственными экспертами часто может быть основным путем неофициального изучения и разработки идей и рекомендаций для правительств. Именно это мы и предполагали, когда NTI созвала американских экспертов для встречи с российскими коллегами в Москве в 2019 году, чтобы изучить возможности сотрудничества в этой области. Последующие усилия, продолжавшиеся до конца 2021 года, привели к глубоким содержательным дискуссиям и разработке важных рекомендаций, отраженных в данном отчете.

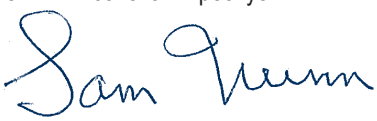
Учитывая конфликт на Украине, мы признаем, что сейчас далеко не самое подходящее время для выдвижения новых неотложных политических идей для двустороннего диалога

1 Работа Исследовательской группы по киберядерному оружию обобщена в отчете 2018 года «Ядерное оружие в новую киберэпоху: отчет исследовательской группы по киберядерному оружию», авторы Пейдж О. Стаутленд и Саманта Питтс-Кифер, Инициатива по сокращению ядерной угрозы (сентябрь 2018 г.), https://media.nti.org/documents/Cyber_report_finalsmall.pdf.

2 Сэм Нанн и Эрнест Дж. Мониз, «Байден должен сделать больше, чтобы предотвратить случайный запуск ядерного оружия. Вот как» (Biden Should Do More to Prevent the Accidental Launch of Nuclear Weapons. Here's How), *Washington Post,* 17 ноября 2021 года, https://www.washingtonpost.com/opinions/2021/11/17/biden-should-do-more-prevent-accidental-launch-nuclear-weapons-heres-how. Закон о полномочиях в области национальной обороны (NDAA) от 2022 года требует от министра обороны провести «обеспечивающий высокую надежность» обзор ядерного оружия, командования и управления, а также систем интегрированного оповещения о возможной угрозе и оценки угрозы (ITW/AA).

по безопасности, но киберядерные вызовы представляют серьезную угрозу для США, НАТО и России. Сегодня конфликт трагически продолжается, ситуация с напряженностью между США и Россией ухудшилась, а ядерные риски растут. Несмотря на это, президент Байден заявил, что Соединенные Штаты готовы работать с Россией над новыми договоренностями по контролю над вооружениями, и реализация программы «Новый старт» продолжается. Несмотря на серьезные разногласия и трения в двусторонних отношениях, взаимные обязательства по предотвращению ядерной катастрофы сохраняют первостепенную важность. Диалог о стратегической стабильности и переговоры по контролю над вооружениями между нашими странами должны возобновиться, и по мере их проведения тема снижения киберядерных рисков должна занять важное место в повестке дня. Кроме того, и особенно в условиях очень слабого доверия между США и Россией, обе страны должны уделять первоочередное внимание односторонним действиям по снижению ядерных рисков. Мы надеемся, что идеи, изложенные в этом отчете, могут стать основой для важных действий и диалога между Соединенными Штатами и Россией.

Бывший сенатор США Сэм Нанн является соучредителем и сопредседателем NTI. За 24 года работы в Сенате США Нанн был председателем сенатского комитета по вооруженным силам и стал инициатором программы «Совместное уменьшение угрозы», которая обеспечивала сохранность и утилизацию оружия массового поражения на территории бывших советских республик.



Бывший министр энергетики США Эрнест Дж. Мониз является сопредседателем и генеральным директором NTI. Д-р Мониз занимал пост министра энергетики США с 2013 по 2017 год, и в этот период он был одним из ключевых участников переговоров по историческому ядерному соглашению между США и Ираном о Совместном всеобъемлющем плане действий.

Пейдж Стаутленд – консультант NTI и бывший вице-президент программы NTI по научно-техническим вопросам. Стаутленд занимал руководящие должности в Ливерморской национальной лаборатории имени Лоуренса, Министерстве энергетики США и Лос-Аламосской национальной лаборатории.

Диалог о стратегической стабильности и переговоры по контролю над вооружениями между нашими странами должны возобновиться, и по мере их проведения тема снижения киберядерных рисков должна занять важное место в повестке дня.

Принципы сотрудничества

В совместном заявлении от 16 июня 2021 года президент Байден и президент Путин подтвердили, что в ядерной войне нельзя победить и нельзя ее начинать, повторив историческое заявление 1985 года президента Рейгана и председателя Горбачева.[3] Однако чтобы ядерная война никогда не произошла, в том числе и война, случайно спровоцированная кибернетическим или информационным инцидентом или атакой, обеим странам необходимы бдительность, творческий подход и сдержанность.

Для двустороннего сотрудничества в этой области США и России необходимо разработать общие принципы, признавая, что:

- киберугроза ядерному оружию и связанным с ним системам — сейчас и в будущем — представляет серьезный риск для стратегической стабильности и безопасности;
- системы ядерного оружия должны быть защищены от киберугроз, что потребует сочетания односторонних и совместных технических и политических мер. В ближайшие годы риск глобальной киберугрозы с большой вероятностью будет расти и усугубляться, что требует принятия срочных мер уже сейчас;
- в дополнение к односторонним действиям и несмотря на низкий уровень доверия, уникальный характер американо-российских ядерных отношений и экзистенциальный характер киберугрозы для систем ядерного оружия требуют от сторон приоритетного внимания к поиску взаимных областей согласия и сотрудничества для снижения ядерных рисков;
- мониторинг и высокодостоверная проверка любых согласованных мер может быть очень сложной или даже невозможной задачей. Стороны должны рассмотреть меры по укреплению доверия, прозрачности, обмену информацией и руководящие принципы ответственного поведения государств, основанные на передовой практике США и России, даже если технические меры для строгой проверки недоступны или непрактичны.

Киберугроза ядерному оружию и связанным с ним системам — сейчас и в будущем — представляет серьезный риск для стратегической стабильности и безопасности.

3 3 января 2022 года лидеры пяти государств, обладающих ядерным оружием и признанных в Договоре о нераспространении ядерного оружия (ДНЯО) — Китайская Народная Республика, Французская Республика, Российская Федерация, Соединенное Королевство Великобритании и Северной Ирландии и Соединенные Штаты Америки, — одновременно заявили, «что в ядерной войне нельзя победить и нельзя ее начинать». Совместное заявление лидеров пяти государств, обладающих ядерным оружием, о предотвращении ядерной войны и недопущении гонки вооружений. Белый дом (3 января 2022 года), https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/03/p5-statement-on-preventing-nuclear-war-and-avoiding-arms-races.

Предложения (краткое описание)

Следующие шесть предложений для США и России направлены на снижение киберрисков с целью повысить стратегическую стабильность и избежать катастрофического применения ядерного оружия.

Соединенные Штаты и Россия должны:

1. Воздерживаться от вмешательства в ядерное оружие и связанные с ним системы, включая системы предупреждения, связи, управления ядерным оружием и средствами его доставки;
2. Оценить варианты минимизации совмещения в рамках одной системы управление ядерным и обычным оружием;
3. Продолжать повышать кибербезопасность своих соответствующих ядерных систем;
4. Повышать прозрачность и расширять коммуникации в периоды повышенной напряженности;
5. Принять процедуры, гарантирующие, что любая кибер-, информационная или любая другая операция с использованием информационно-коммуникационных технологий, исходящая из США или России и способная нарушить миссию ядерного сдерживания другой страны, будет одобрена на том же уровне, который требуется для применения ядерного оружия.
6. Отказаться от политики, угрожающей применением ядерного оружия в ответ на кибератаку.

В распоряжении американских и российских лидеров имеются разнообразные механизмы для реализации этих рекомендаций. Некоторые из них не требуют взаимного согласия и могут быть достигнуты в одностороннем порядке. Других целей следует добиваться взаимно. Соединенные Штаты и Россия должны одновременно использовать несколько подходов для основательного рассмотрения ряда необходимых мер по снижению рисков, которые позволят свести к минимуму возможность кибер- или информационных операций, провоцирующих ядерный кризис.

Риск эскалации: от кибероперaций до ядерной войны[4]

На протяжении десятилетий холодной войны американские и советские стратеги опасались «неожиданной» крупномасштабной ядерной атаки, которая нанесет разрушительный ущерб и вызовет столь же разрушительный ядерный ответ. Но в этом столетии основную озабоченность вызывает просчет, недопонимание, случайность или эскалация, которая побудит Соединенные Штаты или Российскую Федерацию осуществить один или несколько ядерных ударов.

Сегодня США и Россия по-прежнему обладают примерно 90 процентами ядерного оружия в мире, а также являются одними из самых опытных и активных разработчиков и пользователей ИКТ. Однако политика в области ядерного оружия не успевает за этим технологическим прогрессом. Между тем повсеместное распространение передовых цифровых средств ИКТ, а также их всесторонние функциональные преимущества заставили предприятия ядерного оружейного комплекса обеих стран внедрить цифровые технологии в свои системы ядерного оружия, предупреждения, командования, управления и связи.[5] С модернизацией приходят уязвимости и открытость для кибератак, которые могут привести к опасным просчетам или авариям, ведущим к применению ядерного оружия.

Кибер- или ИКТ-атаки повышают риск запуска ядерного оружия в результате недопонимания, неправильной атрибуции вовлеченных лиц или даже несанкционированного использования оружия посредством нарушения физической безопасности.[6] В худшем случае лидеры могут неверно определить источник кибератаки, потерять уверенность в своей способности контролировать ядерное оружие своей страны, неверно воспринять начало крупномасштабного конфликта или потерять уверенность в надежности своих сил сдерживания. Любая из этих ситуаций может привести к ядерному кризису. Эти риски усугубляются еще более напряженными отношениями между Россией и США.

Сегодня США и Россия по-прежнему обладают примерно 90 процентами ядерного оружия в мире, а также являются одними из самых опытных и активных разработчиков и пользователей ИКТ. Однако политика в области ядерного оружия не успевает за этим технологическим прогрессом.

4 В данном документе термин «кибер» приблизительно равнозначен термину «информационно-коммуникационные технологии» или ИКТ.

5 Эрин Д. Думбахер и Пейдж О. Стаутленд, «Модернизация ядерного оружия США: последствия интеграции цифровых технологий для безопасности и политики» (U.S. Nuclear Weapons Modernization: Security and Policy Implications of Integrating Digital Technology), Инициатива по сокращению ядерной угрозы, ноябрь 2020, https://media.nti.org/documents/NTI_Modernization2020_FNL-web.pdf; и Ханс М. Кристенсен и Мэтт Корда, «Российское ядерное оружие в 2021 году» (Russian Nuclear Weapons, 2021), *Bulletin of the Atomic Scientists* 77, № 2, стр. 90–108.

6 Стаутленд и Питтс-Кифер, «Ядерное оружие в новую киберэпоху» (Nuclear Weapons in the New Cyber Age).

Какие кибератаки могут быть настолько разрушительными, чтобы подорвать ядерное сдерживание? Цифровые уязвимости и наступательные кибердействия создают новые риски возникновения ядерной опасности, включая:

- нарушения, связанные с состоянием либо непосредственно ядерного оружия, либо систем боевого управления ядерным оружием, либо обычных систем военного управления или систем разведки, наблюдения и целеуказания;
- перекрытие доступа к военным активам в мирное время и в периоды повышенной напряженности; а также
- искажение, подмена или отравление информации для лиц, принимающих решения, или алгоритмические изменения в автоматизированных системах или алгоритмах машинного обучения, которые могут быть интегрированы в системы управления ядерным оружием и использоваться в системах санкционирования применения ядерного оружия.

Любое из этих вторжений или атак, нарушающих нормальное (запланированное) функционирование различных систем и подсистем управления ядерным оружием и его носителями[7], будь то в целях шпионажа или в более злонамеренных целях, может привести к принятию решений с потенциальными ядерными последствиями. Каждое из них может привести к неверным суждениям со стороны руководства. В ходе нашего двустороннего диалога были рассмотрены следующие наглядные сценарии:

- **Прямая кибератака на ядерное оружие или связанные с ним системы.** Точки уязвимости в системах ядерного оружия включают, среди прочего:
  - системы раннего предупреждения, включая радары и спутники, сигналы от которых могут быть подделаны или иным образом сформировать ложные указания на атаку, которая может привести к пуску ядерного оружия;[8]
  - системы связи, включая средства, с помощью которых президенты и командующие общаются друг с другом в периоды повышенной напряженности, и средства, с помощью которых выдается санкция на применение ядерного оружия[9];
  - кибернетические устройства, используемые в средствах доставки ядерного оружия (на бомбардировщиках, подводных лодках и баллистических ракетах), от которых зависит политика сдерживания; а также
  - системы безопасности складов и военных баз, где хранится ядерное оружие, компрометация которых может привести к краже или диверсиям, направленным на ядерные материалы или оружие.

> Кибер- или ИКТ-атаки повышают риск запуска ядерного оружия в результате недопонимания, неправильной атрибуции вовлеченных лиц или даже несанкционированного использования оружия посредством нарушения физической безопасности.

- **Вмешательство в цепочку поставок, шпионаж, сбор данных, вредоносные программы или вредоносный код, подвергающие опасности ядерное оружие или другие элементы ядерного арсенала, которые могут привести к потере уверенности в том, что ядерное оружие и связанные с ним системы работают правильно.** И Соединенные Штаты, и Россия полагаются на разнообразных и разноплановых поставщиков деталей и услуг для поддержки и модернизации своего ядерного оружия и других элементов ядерного арсенала. Усилия по модернизации, предпринимаемые в обеих странах, будут включать готовые или широкодоступные технологии 2020-х годов, которые, вероятно, будут состоять в основном

7 Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии / отв. ред. А.В. Загорский, Н.П. Ромашкина. – М.: ИМЭМО РАН, 2020. – 98 с., https://www.imemo.ru/en/publications/info/romashkina-np-markov-as-stefanovich-dv-mezhdunarodna-ya-bezopasnosty-strategicheskaya-stabilynosty-i-informatsionnie-tehnologii-otv-red-av-zagorskiy-np-romashkina-m-imemo-ran-2020-98-s.

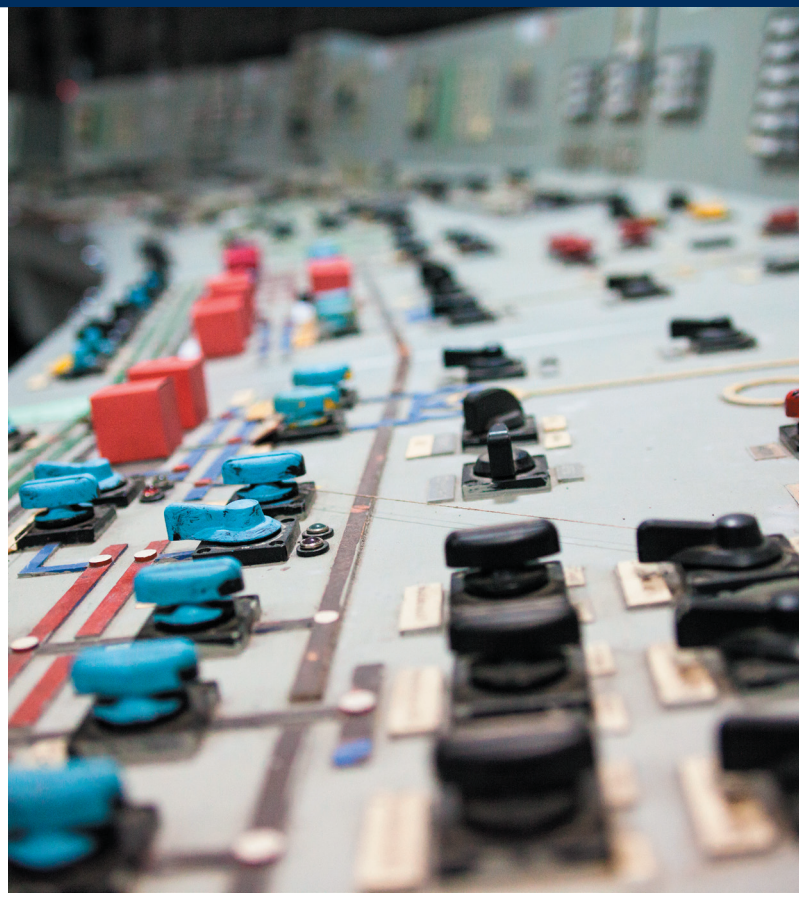
8 Стаутленд и Питтс-Кифер, «Ядерное оружие в новую киберэпоху» (Nuclear Weapons in the New Cyber Age), 13.

9 П.С. Золотарев О подходах к обеспечению кибербезопасности систем управления ядерным оружием. https://www.elibrary.ru/item.asp?id=44185598.

из цифровых инструментов. Риски особенно ощутимы в усилиях по модернизации систем связи и боевого управления ядерным оружием в обеих державах.[10]

- **Атаки на системы связи, нарушающие или выводящие из строя каналы связи, могут привести к случайному или опрометчивому запуску ядерного оружия.** Неверная интерпретация информации, неспособность к деэскалации в период повышенной напряженности или потеря уверенности в способности отдать приказ о запуске в ответ на ядерную атаку могут побудить власти каждой страны действовать быстро и решительно, но, возможно, неразумно.[11] Такое событие может быть вызвано удаленным вторжением или взломом, который, например, может произойти при использовании системы управления, одновременно предназначенной для управления обычными и стратегическими вооружениями, посылая неверную информацию или ложные сигналы через датчики и радары по военной сети управления и в адрес руководства. Аналогичным образом могут быть раскрыты, но неверно истолкованы действия по шпионажу: например, изначальный сбор данных может быть воспринят как внедрение вредоносного ПО или своего рода бомбы замедленного действия, предназначенной для нанесения ущерба. Виновником может быть третья сторона (вне стран НАТО или России), но предполагается, что это либо США, либо Россия, либо другое ядерное государство. Такое обнаружение может вызвать ответные действия, потенциально перерастающие в ядерный ответ.

Чтобы быть эффективной и защитить от непреднамеренной ядерной войны, политика сдерживания должна опираться на точную информацию. Вместе с тем, политика сдерживания неэффективна против киберугроз[12]. Однако современная история полна случаев, когда потенциально опасные происшествия могли случиться, но прошли без последствий. Некоторые из них были результатом просчетов, неправильной интерпретации или неверной информации и могли привести к ядерному кризису между Соединенными Штатами и Россией.



Повышение уязвимости к цифровым атакам и увеличение темпов кибер- и информационных атак угрожают ядерному оружию обеих стран (а также других ядерных стран). США, Россия и другие ядерные или неядерные государства наращивают новые возможности в космической сфере и разработке ракет, что в сочетании с растущей цифровой уязвимостью и атмосферой недоверия между ядерными государствами повышает риски. Все это в совокупности создает повышенную потребность в сдержанности, прозрачности, коммуникации и политических обязательствах со стороны государств, обладающих ядерным оружием.

10 В.В. Путин: http://en.kremlin.ru/events/president/news/64396; Отчет Комиссии США по киберпространству «Солярий» (U.S. Cyberspace Solarium Commission), стр. 118, https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

11 Стаутленд и Питтс-Кифер, «Ядерное оружие в новую киберэпоху» (Nuclear Weapons in the New Cyber Age), 16.

12 Лорен Забьерек, Кристи Лоренс, Майлз Ньюманн и Павел Шариков, «Соперничество между США и Россией в киберпространстве: нужны ли и возможны ли правила дорожного движения?» (US-Russian Contention in Cyberspace: Are Rules of the Road Necessary or Possible?), 10 июня 2021 г. Belfer Center Working Paper https://www.russiamatters.org/sites/default/files/media/files/PDF-CyberRulesoftheRoad-061021-RMPaper.pdf.

Предложения по действиям США и России

Ниже описаны предложения по действиям США и России, которые помогут избежать катастрофического применения ядерного оружия в условиях киберугроз.

Воздерживаться от вмешательства в ядерное оружие и связанные с ним системы, включая ядерные системы командования, управления, связи, доставки и предупреждения

Соединенные Штаты и Россия должны воздерживаться от вмешательства *в ядерное оружие и связанные с ним системы друг друга, включая системы связи и боевого управления (NC3), системы доставки и предупреждения,* в мирное время и в периоды повышенной напряженности. Это потребует сдерживания атак, действий с использованием компьютерных сетей и вторжений в сеть, в том числе в целях разведки, целеуказания и наблюдения, в рамках NC3 и систем предупреждения, что позволит избежать потенциально неверных и катастрофических оценок при обнаружении злоумышленника, вредоносного ПО или других подозрительных признаков.[13]

Атаки, действия с применением компьютерных сетей или вторжения в цифровые элементы систем управления ядерным оружием, включая средства доставки, вспомогательную инфраструктуру и цепочки поставок, могут привести к катастрофической эскалации. Периоды повышенной напряженности, с которыми мы сталкиваемся сегодня, представляют большую опасность, требуя дополнительных мер для обеспечения того, чтобы атаки, действия с применением компьютерных сетей и вторжения не были неверно истолкованы. Неопределенность в отношении рисков кибер- и информационной безопасности для NC3 может со временем возрастать, подрывая доверие и повышая риск неверной интерпретации и просчетов, если одна из стран заподозрит вторжение и риск атаки на системы NC3 и предупреждения.[14] Это ограничение также не призвано показать, что вмешательство в неядерные средства командования, управления, связи и оповещения допустимо, а что вмешательство в ядерные системы уникально тем, что может привести к катастрофической эскалации.

Для выполнения этой рекомендации предлагается предпринять следующие шаги.

- **Конкретизировать соответствующие системы.** Создание конкретных определений того, какие активы поддерживают ядерные, обычные или двойные миссии, может снизить риск того, что действия, направленные на нарушение или повреждение обычных систем военного, управления и связи, могут вызвать ядерный ответ.

- **Воздерживаться от сбора цифровой разведывательной информации в системах NC3 друг друга в мирное время.** Если бы можно было заключить соглашения и обеспечить контроль за тем, чтобы определенные системы были недоступны для целей шпионажа, это могло бы снизить риск того, что сбор разведданных будет ошибочно интерпретирован как вредоносная атака. Такие обязательства или даже потеря разведывательных данных не несут реальных угроз стратегическим расчетам американских или российских лиц, принимающих решения.[15] Но такой подход не решает проблему третьих сторон, которые могут атаковать эти сети. Тем не менее, он станет важным начальным шагом, а также потребует дополнительных инвестиций и исследований возможных методов мониторинга и проверки. Такие обязательства также могут быть инициированы в одностороннем порядке как «нецелевые обязательства» или, возможно, «добровольные обязательства».

- **Воздерживаться от вмешательства в ядерное оружие.** Проникновение или вторжение в цифровые системы носителей ядерного оружия, как главной составляющей ядерного сдерживания , или ядерных бомб или боеголовок, может привести к просчету при обнаружении или

13 Включает атаки на компьютерные сети (CNA), использование компьютерных сетей (CNE) и другие виды шпионажа в рамках чувствительных систем и между ними.

14 Ричард Дж. Данциг, «Выживание на диете из отравленных фруктов: снижение рисков национальной безопасности киберзависимых стран Америки» (Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies), Центр новой американской безопасности (июль 2014 г.), стр. 24–25, https://www.cnas.org/publications/reports/surviving-on-a-diet-of-poisoned-fruit-reducing-the-national-security-risks-of-americas-cyber-dependencies.

15 *Если бы информация была получена в результате шпионажа за этими активами, она, скорее всего, не была бы определяющей и, следовательно, имела бы ограниченную полезность.*

Атаки, действия с применением компьютерных сетей или вторжения в цифровые элементы систем управления ядерным оружием, включая средства доставки, вспомогательную инфраструктуру и цепочки поставок, могут привести к катастрофической эскалации.

даже подозрении на такое вторжение. Реальная или предполагаемая атака на любую инфраструктуру, лежащую в основе ядерного сдерживания, включая промышленную базу или инфраструктуру, такую как производство боеголовок и процессы обеспечения безопасности, может быть воспринята как начало применения ядерного оружия.

- **Не помогать, не спонсировать и не оказывать поддержку другому государству или негосударственному субъекту с целью вмешательства в ядерное оружие или системы поддержки стороны, соблюдающей Договор о нераспространении ядерного оружия (ДНЯО).** Вмешательство в системы двойного назначения, системы NC3 и системы предупреждения любой страны, даже непреднамеренное, может привести к катастрофической эскалации в результате просчета. Чтобы избежать просчетов, США и Россия должны взять на себя обязательство не вмешиваться в работу предприятий ядерного оружейного комплекса, включая ядерный топливный цикл, любой страны, соблюдающей свои обязательства по ДНЯО.

- **Принять публичные обязательства.** Соединенные Штаты и Россия должны дать официальные гарантии и взять на себя, посредством декларативной политики, политические обязательства воздерживаться от сбора цифровых разведданных и вмешательства в ядерное оружие и связанные с ним системы, включая системы двойного назначения. Кроме того, Соединенные Штаты и Россия должны взять на себя обязательство не помогать и не поддерживать такое вмешательство со стороны другого государства или негосударственного субъекта. Такие публичные обязательства станут важным сигналом о политике и намерениях для внутренней и глобальной аудитории.

Оценить варианты минимизации переплетения и/или интеграции систем управления одновременно обычными и ядерными силами и средствами.

И США, и Россия модернизируют свои ядерные силы, потенциально интегрируя новые цифровые уязвимости в существующие носители ядерного оружия, системы предупреждения, боевого управления и связи. Есть мнение, что сегодня научно-технический паритет важнее, чем количественное равновесие[16]. Эти инвестиции дают возможность изолировать или оградить ядерные системы как от гражданской инфраструктуры, так и от систем управления неядерными средствами. Интеграция обычных военных и ядерных систем, включая орбитальные системы, чревата риском эскалации в периоды повышенной напряженности, хотя определить разделительную линию между обычными и ядерными системами может быть непросто.[17] Чтобы снизить риск эскалации, Соединенные Штаты и Россия должны:

- **насколько возможно, оценить потенциал разделения и изоляции систем управления одновременно обычными и ядерными силами средствами.** Признавая, что полное разделение систем от систем NC3 будет дорогостоящим, усилия по модернизации должны проводиться с учетом того, что интеграция ядерных и обычных военных систем может повысить эскалационные риски. В случае невозможности такого разделения следует разработать другие меры по контролю над вооружениями, укреплению доверия и прозрачности, чтобы компенсировать такую невозможность[18];

16 Рогов С.М. Глобальная и региональная стабильность в ядерном мире. Вестник Российской академии наук. 2021. Т. 91. № 6. С. 571-584.

17 См. Алексей Арбатов, Владимир Дворкин и Петр Топычканов, «Переплетение обычных и ядерных вооружений как новая угроза безопасности: российская точка зрения», Фонд Карнеги за международный мир (19 апреля 2018 г.), https://carnegieendowment.org/2018/04/19/ru-pub-76126; и Джеймс М. Актон, «Эскалация через запутывание: как уязвимость систем командования и управления повышает риски непреднамеренной ядерной войны» (Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War), International Security 43, №1 (лето 2018 г.): 56–9, https://doi.org/10.1162/isec_a_00320.

18 П.С. Золотарев О подходах к обеспечению кибербезопасности систем управления ядерным оружием. https://www.elibrary.ru/item.asp?id=44185598.

- **сократить связи ядерных систем с критически важными национальными активами.** США и Россия также должны рассмотреть вопрос об отделении и изоляции ядерного оружия, включая системы NC3, от критически важных национальных активов, насколько это возможно. Эти разделения могут включать изоляцию от спутниковых сетей со значительным гражданским и коммерческим влиянием, например, американской Глобальной системы позиционирования (GPS) и российской Глобальной навигационной спутниковой системы (ГЛОНАСС);

- **сократить связи ядерных систем с критически важной гражданской инфраструктурой.** Хотя США и Россия договорились не атаковать [19]критически важную гражданскую инфраструктуру, связи между ядерными системами и гражданской инфраструктурой необходимо сократить, чтобы избежать возможных непредвиденных последствий в случае кибератак.

Продолжить работу по повышению кибербезопасности ядерных систем

Современное ядерное оружие в США и России включает некоторые цифровые и автоматизированные системы. Добавление цифровых инструментов несет в себе потенциальные преимущества, но также и значительные риски, в том числе такие, которые не до конца изучены. Для снижения этих рисков Соединенные Штаты и Россия должны:

- **проводить односторонние обзоры отказоустойчивости, чтобы понять и определить шаги по уменьшению уязвимостей в системах предупреждения, боевого управления ядерным оружием и связи, а также в ядерном оружии и носителях, которые могут быть созданы или усугублены киберугрозами.** Внутренняя проверка, подтверждающая, что любые проблемы в ядерной системе будут «отказоустойчивыми», укрепит внутренние гарантии предотвращения киберугроз. При необходимости такие проверки должны проводиться на секретном уровне;

19 Например, доклады групп правительственных экспертов ООН, в том числе «Группа правительственных экспертов по достижениям в области информации и телекоммуникаций в контексте международной безопасности», Генеральная Ассамблея ООН, A/70/174 (22 июля 2015 года), 8, пункт (f), https://digitallibrary.un.org/record/799853?ln=en. Недавние события в Украине, к сожалению, ставят под сомнение это обязательство.

Добавление цифровых инструментов несет в себе потенциальные преимущества, но также и значительные риски, в том числе такие, которые не до конца изучены.

- **обеспечить приоритет цифровой безопасности и надежности наряду со стоимостью, графиком и эффективностью для всех операционных систем, а также при приобретении и закупке ядерного оружия и связанных с ним систем в контексте ядерной модернизации и растущей зависимости от цифровизации.** Такая расстановка приоритетов может потребовать ущемления функциональных технологических преимуществ в угоду безопасности и надежности. Как в США, так и в России, цифровые системы должны соответствовать четко установленным порогам безопасности и надежности до их принятия на вооружение. Необходимо выделить ресурсы для проверки и установления того, что лидеры и военные смогут сохранить уверенность в постоянной готовности их ядерных сил в случае необходимости, но никогда не используют их без надлежащего разрешения в результате кибер- или информационных атак.[20]

Повышение прозрачности и коммуникации

Улучшение прозрачности и коммуникации повысит стабильность и снизит риски просчетов, особенно в периоды повышенной напряженности. Регулярные, постоянные диалоги на высоком уровне по вопросам стратегической стабильности и другие взаимодействия (например, взаимодействие между военными) помогают создать более широкую среду взаимопонимания и доверия. Описанные ниже подходы, если они будут приняты, помогут уберечься от потенциально опасных просчетов или ошибок.

- **Более оперативно развернуть канал связи «горячая киберлиния», в идеале в течение нескольких часов после инцидента, предполагаемого нарушения, уничтожения или иной дестабилизирующей кибердеятельности, связанной с ядерным оружием или сопутствующими системами.** Необходимо более быстрое, совместное, тщательное использование каналов экстренной связи для предотвращения как ядерного просчета, так и киберконфронтации. Взаимодействие по дипломатическим каналам может помочь установить и проверить источник атаки или технического сбоя и избежать ошибочной атрибуции. Тем не менее, существующие каналы связи центров снижения риска нельзя назвать неуязвимыми каналами для связи лидеров во время ядерных кризисов. Необходимо обеспечить защищенные каналы связи между лидерами США и России.

- **Во избежание бесполезного или неэффективного сотрудничества между США и Россией следует лучше определить условия использования каналов связи, включая тип контента, которым предполагается обмениваться (например, степень, в которой можно и нужно обмениваться тактикой, техникой и процедурами).** Руководители и их команды должны более эффективно использовать официальные каналы связи, уточнив цели их использования. Существующая практика использования «горячих линий» или Центров снижения рисков, изначально созданных для снижения эскалационных и ядерных рисков между Россией и США, ценна, но недостаточна.

- **Предотвращать просчеты, усиливать связь между военным руководством на различных уровнях и устанавливать практики уведомления о кибер-тренировках и учениях или военных учениях с кибер-компонентами, по образцу Соглашения 1972 года о предотвращении инцидентов в открытом море между США и СССР, которое позволяет обмениваться информацией для уточнения военных действий на море.** Этот подход может снизить вероятность конфликта из-за случайности или просчета, подобно тому, как соглашение о предотвращении инцидентов в открытом море обеспечивает ясность в отношении передвижения судов и самолетов. И Россия, и Соединенные Штаты ранее предлагали заключить такое соглашение для снижения киберядерных рисков.[21]

20 Думбахер и Стаутленд, «Модернизация ядерного оружия США» (U.S. Nuclear Weapons Modernization), 30-2.

21 Американские дипломаты предлагали такой подход как минимум с 2017 года; президент России Путин рекомендовал такой подход в «Заявлении президента России Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности», 25 сентября 2020 года, http://en.kremlin.ru/events/president/news/64086.

- **Повысить прозрачность путем обмена данными о запусках баллистических ракет, включая запуски, осуществляемые национальными государствами и коммерческими организациями.** Учитывая распространение глобальных космических и ракетных запусков, собрать список всех ожидаемых запусков, используя государственные и частные каналы – задача не из легких. Общий источник данных, объединяющий исключительно уже опубликованную и официальную, несекретную информацию, мог поспособствовать улучшению объема и своевременности данных о запуске, по которым военные офицеры могли бы прогнозировать формирование сигналов предупреждения. Хотя можно рассмотреть возможность физического размещения таких центров обмена данными, виртуальные центры могут оказаться жизнеспособными и более целесообразными. Также к участию в таком виртуальном центре может быть привлечен Китай.
- **Проводить консультации с другими странами.** Диалог по киберядерным рискам крайне важен для российско-американских отношений, но кибербезопасность также является глобальной проблемой. США и Россия должны искать пути обсуждения киберядерных рисков с другими странами, включая Китай, Францию, Индию, Пакистан и Великобританию. Наиболее актуальные направления сотрудничества должны включать обмен информацией о киберугрозах и вызовах, а также передовым опытом по противодействию им.

Улучшение прозрачности и коммуникации повысит стабильность и снизит риски просчетов, особенно в периоды повышенной напряженности.

Совместный центр обмена данными

4 июня 2000 года президенты США и России подписали Меморандум о достижении соглашения о создании в Москве Центра обмена данными от систем раннего предупреждения и уведомления о пусках ракет, ЦОД (Joint Center for the Exchange of Data from Early Warning Systems and Notifications of Missile Launches, JDEC) для обмена информацией, получаемой от систем предупреждения о пусках баллистических ракет и космических носителей каждой из сторон. Заявленной целью соглашения было укрепление стратегической стабильности путем дальнейшего снижения опасности запуска баллистических ракет на основе ложного предупреждения об атаке, а также содействие повышению взаимной уверенности в возможностях систем раннего предупреждения о ракетном нападении обеих сторон. Это соглашение стало первым случаем, когда США и Россия договорились о постоянной совместной операции с участием американских и российских военнослужащих.

ЦОД должен был быть укомплектован американским и российским персоналом, работающим 24 часа в сутки, семь дней в неделю. Он также должен был служить хранилищем для уведомлений, которые будут предоставляться в рамках согласованной системы обмена предстартовыми уведомлениями о пусках баллистических ракет и космических ракет-носителей, переговоры по которой ведутся отдельно.

Несмотря на то, что стороны прилагали значительные усилия в течение более десяти лет, ЦОД не принес ощутимых результатов. Неспособность решить вопросы, связанные с налогами и обязательствами, а также растущая озабоченность России политикой США в области противоракетной обороны, фактически остановили прогресс. В 2009 году президенты США и России договорились продолжить затянувшийся ввод в действие ЦОД с заявленной целью стать «основой для многостороннего режима уведомления о пусках ракет», но эти усилия также не привели к желаемому результату.

Со времени первого обсуждения ЦОД значительное глобальное распространение передовых ракетных систем, а также прогресс в ракетных технологиях и датчиках обнаружения пуска резко изменили стратегический ландшафт. Сохраняется первоначальное обоснование создания ЦОД – уменьшение опасности запуска баллистических ракет на основе ложного предупреждения о нападении, а также повышение взаимного доверия. Более того, глубина этих опасений усилилась из-за угрозы кибератак на структуры NC3 и системы раннего предупреждения.

Эти значительные изменения говорят о том, что концепцию ЦОД необходимо пересмотреть и что расширение сферы применения может принести пользу.

В соответствии с общим замыслом первоначального соглашения ЦОД, страны могли бы обмениваться информацией со своих соответствующих спутниковых и радиолокационных датчиков о запуске ракет и космических ракет-носителей. Однако, в отличие от первоначальной концепции, достижения в области коммуникационных технологий позволяют рассмотреть вопрос о виртуальном центре, потенциально избегая некоторых подводных камней первоначального соглашения. Кроме того, можно рассмотреть возможность включения кибернетической и космической областей, не предусмотренных в первоначальном соглашении.

Наконец, можно рассмотреть возможность включения других стран. НАТО и/или Китай могут быть привлечены к инициативе и соглашению либо в самом начале, либо позже. К нему могут быть добавлены другие страны по согласованию сторон соглашения, что сделает его поистине «глобальным» центром.

Повышение уровня полномочий по утверждению кибер-, информационных или любых других операций с использованием ИКТ

Кибер- или информационная операция, способная нарушить миссию ядерного сдерживания страны, должна проходить процесс одобрения на том же уровне, который требуется для применения ядерного оружия. Такая политика гарантирует, что кибер-операции, способные оказать воздействие на ядерные системы другой страны, будут проводиться с явного ведома и одобрения тех же должностных лиц, которые санкционируют применение ядерного оружия. Для этого Соединенные Штаты и Россия должны:

- **обеспечить, чтобы кибер-, информационные или любые другие операции с использованием ИКТ, способные нарушить миссию ядерного сдерживания другой страны, проходили процесс одобрения теми же должностными лицами, которые уполномочены отдавать приказ о применении ядерного оружия.** Это обязательство обеспечит, чтобы наиболее чувствительные и потенциально эскалационные кибер- и информационные операции получали явное одобрение того же лидера, который отвечает за самое серьезное из военных решений – применение ядерного оружия. Это изменение не обязательно повлияет на существующую политику в отношении кибер- или информационных операций, которые не имеют потенциала воздействия на миссии ядерного сдерживания;

- **кроме того, Соединенные Штаты и Россия должны взять на себя обязательство усилить надзор и принять правовые меры для минимизации или прекращения любых негосударственных кибер- или информационных операций, исходящих с их территории, которые могут повлиять на ядерное сдерживание и стабильность или нанести им ущерб.** Правительственная ситуационная осведомленность должна распространяться на кибер- или информационную деятельность невоенных и негосударственных субъектов, которая может привести к катастрофическим ядерным рискам. Эта концепция основана на существующем соглашении между США и Россией относительно того, что «государства не должны сознательно допускать, чтобы их территория использовалась для международно-противоправных действий с применением ИКТ».[22]

Отказ от политики, угрожающей ядерным ответом на кибератаку

США и Россия должны сузить круг обстоятельств, при которых они будут рассматривать возможность ядерного ответа, и не должны угрожать ядерным ответом на кибератаку. Кибератаки можно сдерживать и/или сопровождать более пропорциональными ответными мерами, тем самым повышая доверие к кибер-, а также ядерному сдерживанию. Ранее сформировавшаяся американская и российская ядерная политика еще не в полной мере учитывает риски кибербезопасности и в своем нынешнем виде может увеличить потенциал применения ядерного оружия.

США и Россия должны:

- **пересмотреть политику, позицию и документы по планированию сил, чтобы снизить вероятность ядерного ответа на кибератаки.** Политические обязательства являются способом передачи информации о намерениях и могут помочь избежать неправильного толкования и действий, которые могут привести к непреднамеренной ядерной войне. Политика, позиция сил и доктрина не должны сигнализировать о намерении нанести ядерный удар по виновнику кибер- или информационной атаки, даже если эти ответные действия считаются неядерными стратегическими атаками. Потенциально важным исключением может быть сохранение возможности ядерного ответа в случае кибератаки, которая серьезно повлияет на ядерное оружие, системы командования, управления, связи или предупреждения. [23]

22 Доклад ГПЭ ООН 2015 года (позднее принят резолюцией Генеральной Ассамблеи ООН A/RES/70/237), https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F70%2F237&Language=E&DeviceType=Desktop&LangRequested=False.

23 Данная рекомендация будет работать совместно с рекомендациями, касающимися необходимости уточнения того, какие системы являются критическими для миссии ядерного сдерживания, и сдержанности в проведении кибер- или информационных вторжений или разведывательного зондирования их рамках.

Реализация

В распоряжении американских и российских лидеров имеются различные механизмы реализации этих предложений, начиная от декларативных изменений в политике, взаимных политических обязательств и заканчивая изменениями во внутренних закупках и процедурах управления. США и Россия должны использовать несколько подходов, чтобы в полной мере охватить весь спектр мер по снижению рисков, которые позволят свести к минимуму возможность наступления ядерного кризиса в результате кибероперации.

Для решения киберпроблем и снижения рисков можно использовать новые или пересмотренные политические обязательства, диалоги по стратегической стабильности и односторонние действия. Изменения в официальных декларативных политических обязательствах могут снизить риск того, что просчет приведет к ядерному кризису. На переговорах по стратегической стабильности можно было бы обсудить отказ от вмешательства в системы ядерного оружия и NC3. Соединенные Штаты и Россия также могли бы обмениваться информацией, которая способствовала бы взаимопониманию и формированию ожиданий в кризисной ситуации. Кроме того, каждое государство должно предпринять односторонние действия, например, провести обширные проверки своих ядерных систем на отказоустойчивость. В ближайшей перспективе правительства двух стран также должны рассмотреть возможность участия в диалогах по Треку 1.5 для разработки идей и решения проблем, связанных с некоторыми более практическими соображениями, изложенными в этом докладе, такими как совместный обмен данными о ракетных запусках.

В средней и долгосрочной перспективе кибербезопасность можно улучшить в контексте продолжающейся модернизации систем ядерного оружия. Взаимные обязательства могут быть кодифицированы через различные политические или юридические форматы. Модернизация ядерных сил в каждой стране дает возможность уточнить, изолировать и отделить системы, участвующие в миссиях ядерного сдерживания, от гражданской инфраструктуры, критически важных национальных активов и обычных боевых систем. Модернизация также предоставляет возможности для повышения отказоустойчивости системы и совершенствования мер и методов обеспечения кибербезопасности. И США, и Россия должны уделять первоочередное внимание снижению риска применения киберядерного оружия при реализации будущих двусторонних и многосторонних инициатив в области контроля над вооружениями, укрепления доверия и прозрачности.

Приложение 1. Участники Трека II

Участники из США и Великобритании

Стив Андреасен | Консультант по национальной безопасности NTI

Мэделин Кридон | Бывший главный заместитель администратора Управления национальной ядерной безопасности и бывший помощник министра обороны по глобальным стратегическим вопросам

Эрин Думбахер | Старший сотрудник программы по научным и техническим вопросам NTI

Майкл Эллиот | Бывший заместитель директора по стратегической стабильности Министерство обороны, Объединенный штаб

Эндрю Фаттер | Профессор международной политики Лестерского университета

Хёрб Лин | Старший научный сотрудник Центра международной безопасности и сотрудничества Стэнфордского университета

Крис Пейнтер | Президент Глобального форума по киберэкспертизе Стэнфордского университета, комиссар Глобальной комиссии по стабильности киберпространства

Линн Растен | Вице-президент программы по глобальной ядерной политике NTI

Пейдж Стаутленд | Консультант и бывший вице-президент по научным и техническим вопросам, NTI

Российские участники

Виктор Есин | Ведущий научный сотрудник отдела военно-политических исследований ИСКРАН, бывший начальник штаба Ракетных войск стратегического назначения, генерал-полковник (в отставке)

Вадим Козюлин | Директор проекта «Новые технологии и глобальная безопасность» ПИР-Центра

Олег Криволапов | Научный сотрудник Департамента военно-политических исследований ИСКРАН

Сергей Рогов | Академический директор ИСКРАН, действительный член Российской Академии Наук

Юрий Рыжих | Специалист компании «Российские космические системы», полковник (в отставке)

Павел (Паша) Шариков | Ведущий научный сотрудник Института Европы Российской Академии Наук

Дмитрий Стефанович | Научный сотрудник отдела исследований военной и экономической безопасности, ИМЭМО

Наталия Степанова | Научный сотрудник Департамента военно-политических исследований ИСКРАН

Елена Зиновьева | Доцент кафедры мировой политики, заместитель директора Центра международной информационной безопасности, науки и технологической политики Университета МГИМО

Павел Золотарев | Ведущий научный сотрудник, заведующий отделом военно-политических исследований ИСКРАН, генерал-майор (в отставке)

Благодарности

Обсуждение такой деликатной темы, как киберугрозы для ядерного оружия и связанных с ним систем, – это сложная задача даже за рамками правительства. Мы благодарны всем участникам, а также их принимающим организациям за то, что они взялись за такую важную, но сложную тему.

Данный проект длился несколько лет и включал в себя встречи в Москве и через Zoom, что было необходимо в связи с пандемией. Мы благодарны всем, кто принял участие в этой работе. Это — одни из самых уважаемых экспертов со всего мира, и они не жалели своего времени.

NTI благодарит бывшего сенатора Сэма Нанна, бывшего министра энергетики Эрнеста Дж. Мониза и президента NTI Джоан Ролфинг за их видение и лидерство в вопросах снижения ядерных угроз в глобальном масштабе. Мы также благодарны сотрудникам NTI за их прошлую и текущую работу, включая Эрин Думбахер, Линн Растен, Стива Андреасена и команду NTI по коммуникациям. Мы в особом долгу перед нашим исполнительным помощником Кэтрин Крэри за ее отличную работу.

Мы выражаем искреннюю благодарность всем, кто сохраняет личную приверженность делу снижения глобальных киберядерных рисков, несмотря на трудности текущей геополитической ситуации.

Пейдж Стаутленд