NUCLEAR RISK REDUCTION: FRICTION POINTS SERIES PAPER 2

THE CYBER-NUCLEAR NEXUS:
Interactions and Risks

WILFRED WAN
ANDRAZ KASTELIC
ELEANOR KRABILL

UNIDIR

ACKNOWLEDGEMENTS

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. This research area of the Weapons of Mass Destruction and Other Strategic Weapons Programme is supported by the Governments of Australia, Finland, Italy, Sweden, and Switzerland.

UNIDIR's Samuele Dominioni, María Garzón Maceda, Robin Geiss, Renata Hessmann Dalaqua, Pavel Podvig, James Revill, and Yuanhu Yuin all provided invaluable advice, support, and assistance on this paper. The authors would also like to acknowledge Andrew Futter and Beyza Unal for their inputs.

ABOUT UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

NOTE

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in this publication are the individual authors' sole responsibility. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

CITATION

Wan Wilfred, Andraz Kastelic and Eleanor Krabill. 2021. *The Cyber–Nuclear Nexus: Interactions and Risks. Nuclear Risk Reduction*, Friction Points Series No. 2. Geneva, Switzerland: UNIDIR. https://doi.org/10.37559/WMD/21/NRR/03.

www.unidir.org | © UNIDIR 2021

Cover © www.shuttterstock.com/Skorzewiak

TABLE OF CONTENTS

ABOUT THE AUTHORS

Wilfred Wan is the Lead Researcher in the WMD and Other Strategic Weapons Programme at UNIDIR. He is the editor of *Nuclear Risk Reduction: Closing Pathways to Use (UNIDIR, 2020), and the author of Regional Pathways to Nuclear Nonproliferation* (University of Georgia Press, 2018). Wilfred was previously a JSPS–UNU Postdoctoral Fellow with the UNU Centre for Policy Research, and a Stanton Nuclear Security Fellow at the Belfer Center at Harvard Kennedy School. He holds a PhD in political science from the University of California, Irvine.

Andraz Kastelic is the Lead Cyber Stability Researcher of the Security and Technology Programme. Prior to joining UNIDIR, Andraz held various research positions in different international organizations and research institutions around the world. Andraz holds a PhD in international law, and an MA in diplomacy.

Eleanor Krabill has been with UNIDIR's Graduate Professional Programme since June 2021. She has completed a MA in non-proliferation and terrorism studies at the Middlebury Institute of International Studies at Monterey. Her research interests include nuclear non-proliferation, security, and disarmament. She previously served as an international safeguards intern at Lawrence Livermore National Laboratory and as a graduate research assistant at the James Martin Center for Nonproliferation Studies.

ABBREVIATIONS AND ACRONYMS

GGE	Group of Governmental Experts
ICT	Information and communications technology
NATO	North Atlantic Treaty Organization
NC3	Nuclear command, control, and communications
NPT	Treaty on the Non-Proliferation of Nuclear Weapons
OEWG	Open-ended Working Group

SUMMARY

- Interactions between cyber capabilities and nuclear forces are likely to increase as the cyber domain continues to be incorporated into military operations and nuclear weapons systems rely further on digital technologies.

- There remains much ambiguity, some intentional, surrounding the types of cyber operations that could elicit nuclear response; the lack of clarity around these 'red lines' feeds into the kind of misperception, miscalculation, or misunderstanding that can drive escalation.

- The primary deterrent role of nuclear weapons suggests that cyber 'red lines' begin with threats to the retaliatory capability of nuclear-armed States, including support systems that provide assurance of that capability. Examining the manner in which this capability can be threatened by cyber operations provides key insight into potential trigger events, a prerequisite for effective risk reduction.

- Considering State doctrines, postures, and capabilities—in the cyber and nuclear spheres—can help to identify other pathways to potential nuclear use stemming from cyber–nuclear interactions.[1]

- The nuclear doctrines of some States provide room for manoeuvrability that opens the door for consideration of nuclear weapon use in response to cyber operations. An area in which subjectivity about circumstance of use is acute concerns critical national infrastructure, a concept highly dependent on national context.

- Cyber–nuclear interactions can take direct and indirect forms; indeed, recent history underscores that cyber operations that do not directly interact with nuclear forces (or infringe on 'red lines' outlined in nuclear doctrines) can still impact on potential escalation scenarios by affecting communications and decision-making in and around nuclear weapons.

- Addressing escalatory risks at the cyber–nuclear nexus will require States to engage at all levels with all stakeholders, including industry actors, in a multifaceted manner, building upon the foundation of existing nuclear risk reduction activities, and recent efforts towards broader norms of behaviour in cyberspace.

- A normative framework around cyber behaviours in the context of nuclear weapons systems requires some common understandings around risks, threats, and vulnerabilities; direct engagement on these topics in turn can help both to minimize cyber–nuclear interactions and to mitigate the consequences of those that might take place.

1 A note on methodology: The information upon which assessments of State doctrines, postures, and capabilities in the cyber and nuclear spheres are based is drawn from publicly accessible information. Lack of official documentation in some instances has made necessary data triangulation methods that include reliance on secondary sources, such as peer-reviewed journal articles. This is further complicated by differences in terminology used by States themselves: e.g. 'cyber operations' versus 'information warfare'. Such issues underline the complexities of perception and interpretation as depicted in this paper.

1. CONTEXT

Pathways to the potential use of nuclear weapons are intertwined with the characteristics of a given context. These characteristics include the doctrines and force postures of involved nuclear-armed States, the nature of their alliances, and underlying sources of tension, emanating from the surrounding regional and subregional security environments.[2] Naturally, risk-of-use pathways—and the underlying drivers that can manifest them—can originate beyond the nuclear sphere. Experts often express concern about the consideration of nuclear use in times of crisis, when decision makers may feel pressure to act quickly and decisively and the possibility of error, both human and technical, is acute. They also raise the possibility of nuclear weapons being introduced into existing conflict as a means of escalation. The notion of use emerging from 'lesser conflicts' over isolated, regional, and non-nuclear issues, dates back to the earliest thinking about nuclear strategy, to the very beginnings of the Cold War.[3]

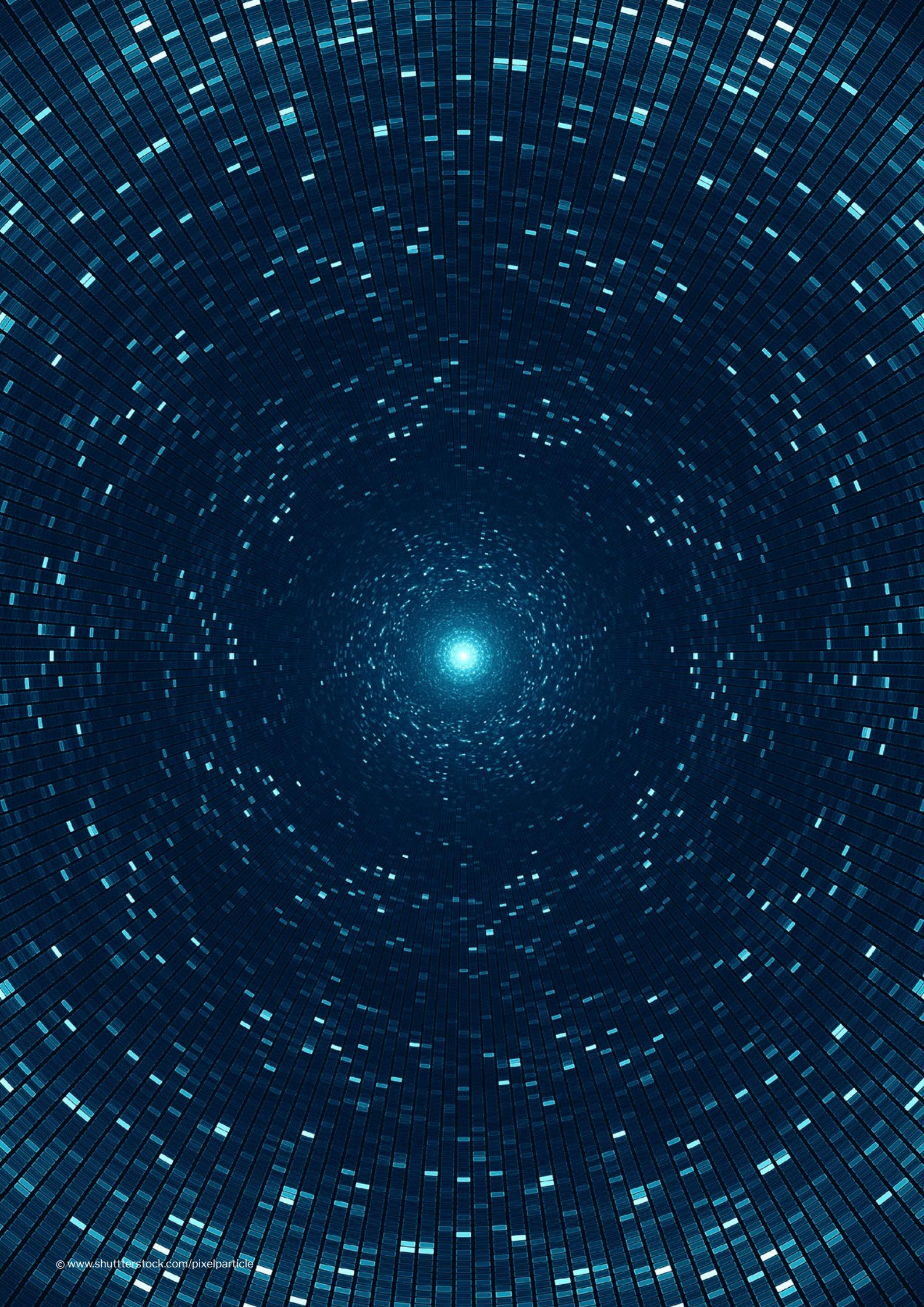
In recent years, discourse on escalatory risk has taken on new dimensions, considering scenarios of intensification across sectors and domains. This is partly due to the multipolar geopolitical landscape, in which capabilities across nuclear-armed and nuclear-allied States are often asymmetric and the practice of deterrence appears increasingly complex. It is also a function of the widened scope of strategic competition, with developments that at times foster technology-and arms-racing dynamics. Accordingly, there is increased attention on potential escalation linked to entangled interaction between nuclear and non-nuclear capabilities.[4] The cyber–nuclear nexus in particular has been a focal point of policymaking and expert communities. Ahead of the June 2021 Geneva summit between US President Joe Biden and Russian President Vladimir Putin, for instance, top US national security aides reportedly sought an agreement to declare nuclear command and control off-limits from cyber offensive operations in peacetime.[5] Yet even nuclear command and control is just one part of the picture.

This paper is the second in a series of profiles of different 'friction points' among nuclear-armed and nuclear-allied States—looking at the issues of contention in their relations that could spark potential conflict and nuclear escalation. There is a burgeoning literature that considers the implications of cyberspace being perceived as an operational domain. Experts have examined the spectrum of threat posed by cyber capabilities to strategic stability, mapping out in the abstract scenarios of inadvertent nuclear war.[6] This paper focuses on filtering these possible scenarios through State policies and perspectives. What constitute to States the critical 'entry points' in their nuclear forces that, if penetrated by cyber operations, might elicit consideration of nuclear response?[7] And following from that, given existing State doctrines, postures, and capabilities both in the cyber and nuclear spheres, what are the likely pathways to potential nuclear use stemming from the interaction of the cyber and nuclear spheres?

This report seeks to weigh these 'cyber–nuclear interactions' that could drive escalatory scenarios by considering relevant developments in the two spheres. Section 2 establishes a foundation for these potential interactions. It first considers the evolving role of computers in nuclear weapons systems; it also looks at the place of cyber capabilities in the security calculus of nuclear-armed States and their alliances. Section 3 examines the possibility of escalation linked to the direct interaction of cyber and nuclear forces, considering existing doctrines then centring on cyber operations that can interfere with the practice of deterrence. Section 4 examines the possibility of indirect interactions, considering for instance operations that could bolster conventional attacks and render nuclear assets physically vulnerable. Section 5 concludes by identifying policy options to reduce the risk of cyber-induced nuclear weapon use.

---

2 See W. Wan, "Nuclear Risk Reduction: A Framework for Analysis", UNIDIR, 2019, https://doi.org/10.37559/WMD/19/NRR01.
3 B. Brodie, Escalation and the Nuclear Option, RAND, 1965, https://www.rand.org/pubs/research_memoranda/RM4544.html.
4 For more, see J.M. Acton, "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War", *International Security*, vol. 41, no. 1, 2018, https://doi.org/10.1162/isec_a_00320.
5 D.E. Sanger, "Once, Superpower Summits Were About Nukes. Now, It's Cyberweapons", *New York Times*, 15 June 2021, https://www.nytimes.com/2021/06/15/world/europe/biden-putin-cyberweapons.html.
6 For instance, A. Futter, *Hacking the Bomb: Cyber Threats and Nuclear Weapons*, 2018; J.R. Lindsay, "Cyber Operations and Nuclear Weapons", Nautilus Institute, 2019, https://nautilus.org/napsnet/napsnet-special-reports/cyber-operations-and-nuclear-weapons.
7 On entry points, see P. Lewis and B. Unal, "Cyber Threats and Nuclear Weapons Systems", in J. Borrie, T. Caughley, and W. Wan (eds), *Understanding Nuclear Weapon Risks*, UNIDIR, 2017.


© www.shuttterstock.com/pixelparticle

2. THE STATE OF AFFAIRS

Increased attention on the cyber–nuclear nexus as a pathway to escalation arguably has emerged because of specific developments in cyberspace over the last 15 years. This includes a 'concerted' distributed denial-of-service (DDoS) attack on the Estonian infrastructure in 2007, which, while unrelated to the nuclear space, showcased an operational scope and targeting method that led officials to suggest State involvement.[8] In 2010, an antivirus software company alerted the world to Stuxnet, a piece of computer malware that could directly affect physical equipment; it was used against nuclear facilities of the Islamic Republic of Iran.[9] Several incidents reflecting State-level "strategic thinking and operational planning" have taken place since, including operations during the confrontation between the Russian Federation and Ukraine that resulted in the shutdown of three Ukrainian energy distribution companies in 2015.[10] These incidents—potential signs of the integration of the cyber domain into State military operations—take on significance in the context of escalation because of the long-standing and increasing reliance on digital technologies in military operations, and in particular the ubiquity of computers in the nuclear space.[11]

2.1. COMPUTERS AND NUCLEAR WEAPONS SYSTEMS

Computer systems have long played a critical role in early warning infrastructure, and the historical narrative of the computer is intertwined with that of missile defence systems. In the 1950s, the United States moved to establish a series of warning and defence systems built on automation, utilizing "sophisticated communications, data processing, and display techniques";[12] this included trials of the computer-controlled Semi-Automatic Ground Environment air defence system against bombers.[13] The Soviet Union too modernized command and control of its strategic rocket forces by using innovative technologies such as computers and communications systems.[14] Such technological development efforts included support systems as well as capabilities: the United States gradually incorporated on-board digital computers over generations of intercontinental ballistic missiles; a similar process took place in the Soviet Union albeit at a slower pace.[15]

There exists an intrinsic risk of error linked to computer operations in nuclear weapons and related systems. Potential sources of problems are numerous, and include "incorrect or incomplete system specifications, hardware failure, hardware design errors, software coding errors, software design errors, and human error (such as incorrect equipment operation or maintenance)"—with a combination of these driving potential failure even in the most reliable of systems.[16] Whatever the manner or degree of computer system integration, the possibility of error cannot be discounted. This can be attributed in part to the fundamental nature of complex and tightly coupled systems that in the eyes of some makes accidents likely or even inevitable. Notably, one expert has characterized nuclear early warning systems as "moderately" if not "disastrously" complex, and observed that their "failure to deliver may be high".[17]

---

8 S. Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", *Journal of Strategic Security*, vol. 4, no. 2, 2011, https://www.jstor.org/stable/26463926.

9 See appendix.

10 S. Blank, "Cyber War and Information War à la Russe", in G. Perkovich and A.E. Levite (eds), *Understanding Cyber Conflict: Fourteen Analogies*, 2017, p. 92.

11 A. Greenberg, "The WIRED Guide to Cyberwar", 2019, https://www.wired.com/story/cyberwar-guide.

12 L. Wainstein et al., "The Evolution of U.S. Strategic Command and Control and Warning, 1945–1972", Study S-467, Institute for Defense Analyses, 1975, pp. xv–xvi, https://apps.dtic.mil/sti/citations/ADA331702.

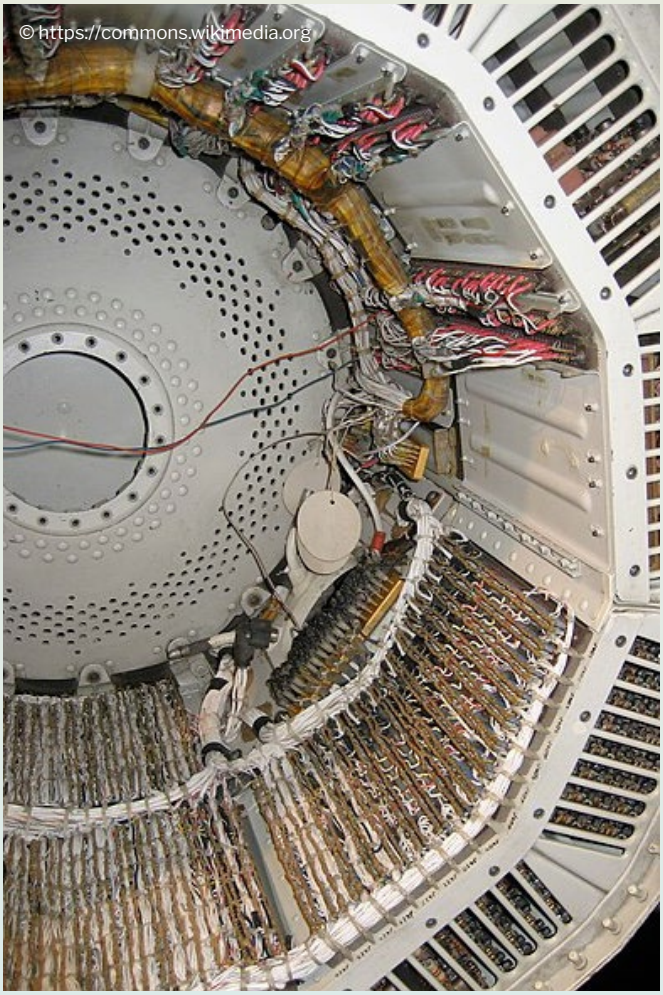
13 J. Borrie, "Cold War Lessons for Automation in Nuclear Weapon Systems", in V. Boulanin (ed.), *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*, Volume I: Euro-Atlantic Perspectives, SIPRI, 2019, https://www.sipri.org/publications/2019/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-i-euro-atlantic.

14 L. Ryabikhin, "Russia's NC3 and Early Warning Systems", *Technology for Global Security Special Report*, 2019, https://nautilus.org/napsnet/napsnet-special-reports/russias-nc3-and-early-warning-systems.

15 D. MacKenzie, "The Soviet Union and Strategic Missile Guidance", *International Security*, no. 13, no. 2, 1988, https://www.jstor.org/stable/2538970.

16 A. Borning, "Computer System Reliability and Nuclear War", Communications of the ACM, vol. 30, no. 2, 1987, p. 120, https://doi.org/10.1145/12527.12528.

17 C. Perrow, *Normal Accidents: Living with High-Risk Technologies*, 1999, p. 291. See also S.D. Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*, 1993.



In fact, several nuclear 'close calls' took place during the Cold War precisely because of computerized system malfunctions. Some observed that "erroneous or ambiguous warnings from U.S. or Russian early warning sensors of an incoming nuclear attack are relatively common".[18] Such false alarms—examples of which come primarily from the United States due to the availability of declassified information—have taken a variety of forms, reflecting the aforementioned range of potential causes. Computers have misinterpreted natural phenomena as missile launches, sensors have assigned trajectories to missiles in training exercises in a manner that falsely suggested homeland attack, and technical issues with computer chips and circuit cards have caused spurious missile warnings or communications breakdowns.[19] Human error linked to the operation of computer systems have caused other incidents that raised alert statuses as well.[20] No nuclear response came as a result of any of these occurrences, but at times it was not beyond the realm of consideration for decision makers.

History confirms the non-zero probability of computer malfunction in nuclear weapons and related systems; it also highlights the possibility of intentionally induced problems. Some historians allege that the United States explored electronic warfare capabilities and the development of hardware and software to conduct an "across-the-board assault on Soviet and Warsaw Pact command centers and military installations" aimed at undermining Soviet retaliatory capabilities.[21] The official Soviet Naval digest, meanwhile, published articles that highlighted the value of electronic countermeasures on command posts, communications systems, and intelligence systems; a piece in a magazine published by the Soviet Ministry of Defence explored the electromagnetic impact of a high-altitude nuclear detonation on those systems.[22] Such explorations aside, the known instances of system interference fall broadly in efforts to interfere with strategic communications, and to electronically generate and inject false targets into radar systems (a practice known as 'spoofing').[23]

Advances in processing power allowed computers to play a greater role in systems linked to the operations of nuclear weapons and related capabilities. This centred primarily on their ability to handle more information in missile defence and early warning systems—at the sensor level, in processing data from radar systems, and at the decision-making level.[24] Investments in research and development also drove the introduction of automated and semi-automated systems. With an eye to protecting their retaliatory strike capabilities, the Soviet Union designed a nuclear command and control system that, in some circumstances, would transmit launch orders automatically if it determined that a nuclear attack had occurred.[25]

---

18 Union of Concerned Scientists, "Close Calls with Nuclear Weapons", 2015, https://www.ucsusa.org/resources/close-calls-nuclear-weapons.
19 E. Schlosser, *Command and Control: Nuclear Weapons, the Damascus Incident, and the Illusion of Safety*, 2013; P. Lewis et al., "Too Close for Comfort: Cases of Near Nuclear Use and Options for Policy", Chatham House, 2014.
20 Ibid.
21 B.B. Fischer, "CANOPY WING: The U.S. War Plan That Gave the East Germans Goose Bumps", *International Journal of Intelligence and CounterIntelligence*, vol. 27, no. 3, 2014, p. 439, https://doi.org/10.1080/08850607.2014.900290.
22 The titles of the magazines are *Morskoy Sbornik and Technika I Vooruzheniye*. See F.D. Kennedy, Jr., "The Evolution of Soviet Thought on 'Warfare in the Fourth Dimension'", *Naval War College Review*, vol. 37, no. 2, 1984, https://www.jstor.org/stable/44642306.
23 B. Unal and P. Lewis, "Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences", Chatham House, 2018, https://www.chathamhouse.org/2018/01/cybersecurity-nuclear-weapons-systems.
24 I.I. Anureyev, "Antimissile and Space Defense Weapons", Joint Publication Research Service, 1972.
25 See P. Podvig (ed.), *Russian Strategic Nuclear Forces*, 2001.

For instance, the communication system known as 'Perimeter' would use command rockets to deliver these orders to missile silos that could then launch without human intervention. The system also appears to be capable of functioning in a fully automated mode, known as 'Dead Hand', although by all indications this mode was never activated. There have been some indications that the system may still be functioning.[26]

Extensive nuclear modernization plans undertaken by nuclear-armed States will drive further reliance on computers, and in some cases, machine learning and automation. The Russian Federation and the United States in particular are looking to retire legacy systems and to adopt state-of-the-art technologies in their nuclear command, control, and communications (NC3).[27] Some argue that it may not be possible to isolate computer systems from the Internet given technological advances, and that even such 'air-gapped' systems could still be compromised.[28] Protection from external interference would also not address the possibility of accidents linked to the tightly coupled and complex nature of these systems. Moreover, increased reliance on complex systems will challenge the transparency around them, creating scenarios in which even "engineers do not have a full understanding of [their] inner working", and undermining efforts to identify or attribute errors.[29] Ultimately, the ubiquity of computers in all aspects of the nuclear enterprise—in early warning and intelligence, surveillance and reconnaissance, command and control, payload delivery, and air and missile defence—suggests the emergence of new vulnerabilities, new system malfunction scenarios, and new risks.

2.2. CYBERSPACE, SECURITY, AND MILITARY OPERATIONS

The integration of computers into nuclear weapons systems has long been fact, as has the potential for system error (including induced malfunction). The potential for escalation linked to cyber–nuclear interactions thus rests partly on the frequency of those interactions, which in turn requires first considering the current state of cyber capabilities. In recent years, the majority of States have developed national doctrines outlining their approach to cyber defence or deterrence, underscoring the elevation of cyberspace in strategic planning.[30] In many instances, the connection between cyberspace, national security, and military operations has become explicit. Most of the nuclear-armed States have published cybersecurity positions; this section examines these positions, in the process outlining the manner in which cyberspace has been securitized and militarized.

2.2.1. NPT Nuclear-Weapon States

China's Military Strategy of 2015 recognized that cyberspace had reached "new commanding heights in strategic competition", with war taking on an informational component.[31] In the Strategy, China observed that countering cyber threats was necessary to preserve international security, aiming to do so by developing a cyber force and by enhancing its "capabilities of cyberspace situation awareness and cyber defence".[32] The same document recognized the need for the armed forces to innovate, with the intent to prevail in operations "featuring information dominance, precision strikes and joint operations".[33]

---

26 M. Peck, "Russia's 'Dead Hand' Nuclear Doomsday Weapon is Back", *The National Interest*, 2018, https://nationalinterest.org/blog/buzz/russias-dead-hand-nuclear-doomsday-weapon-back-38492.

27 V. Boulanin, "The Future of Machine Learning and Autonomy in Nuclear Weapon Systems", in V. Boulanin (ed.), *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, Vol. I: Euro-Atlantic Perspectives*, SIPRI, 2019, p. 53, https://www.sipri.org/publications/2019/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-i-euro-atlantic.

28 S.S.H. Shah, "Offensive Cyber Operations and Nuclear Weapons", Center for Strategic and International Studies, 2019, https://csis-website-prod.s3.amazonaws.com/s3fs-public/190313_Shah_OffensiveCyber_pageproofs2.pdf.

29 V. Boulanin, "Artificial Intelligence: A Primer", in V. Boulanin (ed.), *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, Vol. I: Euro-Atlantic Perspectives*, SIPRI, 2019, p. 20, https://www.sipri.org/publications/2019/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-i-euro-atlantic.

30 These doctrines may be elaborated in various strategies, policies, legislation, military manuals as well as statements of officials and in State practice to date. The documents outlining a particular cybersecurity doctrine are not always devoted to national position on activities by means of ICT; cybersecurity doctrine sometimes forms an integral part of adjacent or overarching policy related to, for instance, national military strategy, efforts of digitalization, etc.

31 The State Council Information Office of the People's Republic of China, "China's Military Strategy", 2015, Section I, http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm.

32 Ibid, Section IV.

33 Ibid, Section III.


© https://commons.wikimedia.org

Still, China has steadfastly refused to discuss offensive capabilities.[34] A 2019 white paper on national defence notes that the armed forces will "accelerate the building of their cyberspace capabilities", again for defensive purposes.[35] Other relevant documents, including the National Cybersecurity Strategy, underline protection of national cyberspace sovereignty and national security.[36]

France has outlined both offensive and defensive doctrines guiding the conduct of cyber operations.[37] Additional sources complement these doctrinal provisions; Law No. 2018-607, for example, establishes the reserve cyber defence forces, while the Strategic Review of Cyber Defence outlines the French doctrine related to the management of cyber crises.[38]

The main sources of the Russian Federation's doctrine on cybersecurity include the 2014 Concept of the State System for Detection, Prevention and Elimination of Consequences of Computer Attacks on Information Resources and the 2016 Doctrine of Information Security. The former formalizes a system for detecting, preventing and eliminating the consequences of computer attacks on information resources.[39] The latter outlines relevant national cybersecurity objectives, including a commitment to the protection of critical infrastructure.[40] Notably, the Russian Federation has issued information security doctrines since 2000 but the 2016 version for the first time linked information security to ensuring strategic deterrence; the following year it established 'information-operation troops' in its armed forces.[41]

The United Kingdom outlines its approach to cyber defence in Joint Doctrine Note 1/18 and Cyber Primer (2nd edition).[42] The latter is of particular importance, observing that methods of war apply equally to cyber activity as in other operational domains.[43] The National Cyber Security Strategy 2016–2021 notes specifically that "principles of deterrence are as applicable in cyberspace as they are in the physical sphere".[44] Notably, that document highlights the importance of offensive capabilities in deterrence. The United Kingdom under its National Offensive Cyber Programme conducted operations against the Islamic State in Iraq and the Levant and offered its capabilities to the North Atlantic Treaty Organization (NATO); it announced in 2020 its intention to continue developing those capabilities under its new National Cyber Force.[45]

---

34 A.E. Levite et al., "China–US Cyber-Nuclear C3 Stability", Carnegie Endowment for International Peace, 2021, http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm.

35 State Council Information Office of the People's Republic of China, "China's National Defense in the New Era", 2019, chp. 1, http://www.xinhuanet.com/english/2019-07/24/c_138253389.htm.

36 *Global Times*, "China Announces Cybersecurity Strategy", 27 December 2016, https://www.globaltimes.cn/content/1026015.shtml.

37 French Ministry of the Armed Forces, "Éléments publics de doctrine militaire de lutte informatique offensive", January 2019, https://www.defense.gouv.fr/content/download/551555/9394645/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf; French Ministry of the Armed Forces, "Politique ministérielle de lutte informatique defensive", 2019, www.aaan-lca.fr/files/p3/Politique%20ministerielle%20de%20lutte%20informatique%20DEFENSIVE.pdf.

38 French Secretariat-General for National Defence and Security, "Revue stratégique de cyberdéfense", 2018, www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

39 Security Council of the Russian Federation, "Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации", 2014, http://www.scrf.gov.ru/security/information/document131.

40 Ministry of Foreign Affairs of the Russian Federation, "Doctrine of Information Security of the Russian Federation", 2016, https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163 [unofficial translation].

41 International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment", 2021, p. 104, https://www.iiss.org/-/media/files/research-papers/cyber-capabilities-and-national-power---a-net-assessment.pdf.

42 United Kingdom Ministry of Defence, "Joint Doctrine Note 1/18 Cyber and Electromagnetic Activities", 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf.

43 United Kingdom Ministry of Defence, "Cyber Primer", 2nd ed., 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf.

44 HM Government, "National Cyber Security Strategy 2016–2021", 2016, p. 47, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

45 GCHQ, "National Cyber Force Transforms Country's Cyber Capabilities to Protect the UK", 19 November 2020, https://www.gchq.gov.uk/news/national-cyber-force.

The United States in 2011 declared cyberspace to be an "operational domain", with the Department of Defense establishing the Cyber Command to unify operations and to coordinate military service components.[46] The central element of its current cyber costing is the National Cyber Strategy (issued in 2018 under the Trump administration), which aims to strengthen the ability "to deter and, if necessary, punish those who use cyber tools for malicious purposes"; the document goes on to highlight the potential use of military (both kinetic and cyber) force "to prevent, respond to, and deter malicious cyber activity".[47] Indeed, cyber attacks are mentioned in the 2018 Nuclear Posture Review as warranting potential consideration of nuclear response (discussed further in section 3). Notably, the Department of Defense Cyber Strategy 2018 elaborated a "defend forward" strategy to address "malicious cyber activity at its source"; the then-National Security Agency head suggested an interrelated aggressive approach of "persistent engagement".[48] The 2017 National Security Strategy further highlights the evolving cyber threat, referring to "low-cost and deniable opportunities" for adversaries.[49]

2.2.2. Non-NPT Nuclear-Armed States

The Democratic People's Republic of Korea has not produced any official documents regarding its cyber doctrine or strategy. In 2013, Kim Jong-Un reportedly stated that cyberwarfare is "an all-purpose sword that guarantees ... ruthless striking capability, along with nuclear weapons and missiles".[50] Some experts suggest that the cyber operations conducted by the Democratic People's Republic of Korea largely resemble "outlaw raids", with little evidence to date of a "capability for sustained military cyber operations beyond classic electronic warfare".[51] Yet the emphasis on cyber crime in the financial sector may be a conscious choice; for instance the May 2017 WannaCry malware attack that affected hundreds of thousands of computers was attributed to the Democratic People's Republic of Korea by the United States and the United Kingdom.[52]


© https://www.idf.il/en/minisites/technology-and-innovation

For India, section 10 of the 2004 Indian Army Doctrine outlines impacts of information and communications technology (ICT) to the future of warfare and recognizes the utility of cyber operations for so-called deception operations; however, it provides few specifics regarding modalities of the conduct of offensive and defensive cyber operations.[53] Notably, in 2016 a former national security adviser highlighted the already considerable capacity India had in cyberwarfare.[54] The Joint Doctrine of the Indian Armed Forces 2017 refers to cyberspace as an operational domain, part of a triad (alongside space and special

---

46 Cyberspace is introduced as a fifth domain, alongside air, land, maritime, and space. See US Department of Defense, "Department of Defense Strategy for Operating in Cyberspace", 2011, p. 5, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

47 The White House, "National Cyber Strategy of the United States of America", 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

48 US Department of Defense, "Department of Defense Cyber Strategy 2018", 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF; G. Myre, "'Persistent Engagement': The Phrase Driving a More Assertive U.S. Spy Agency", *NPR*, 26 August 2019, https://www.npr.org/2019/08/26/747248636/persistent-engagement-the-phrase-driving-a-more-assertive-u-s-spy-agency.

49 The White House, "National Security Strategy of the United States of America", 2017, p. 12, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf; US Department of Defense, "Nuclear Posture Review 2018", 2018, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEWFINAL-REPORT.PDF. More recently, the 2021 Executive Order 14028 came in response to a series of cyber incidents affecting a significant number of ICT systems; Executive Office of the President, "Improving the Nation's Cybersecurity", Executive Order no. 14028, 12 May 2021, https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

50 See J.Y. Kong, J.I. Lim and K.G. Kim, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies", in T. Minárik et al. (eds), *11th International Conference on Cyber Conflict: Silent Battle*, 2019, p. 1, https://ccdcoe.org/uploads/2019/06/Art_08_The-All-Purpose-Sword.pdf.

51 The International Institute for Strategic Studies, p. 126, "Cyber Capabilities and National Power: A Net Assessment", 2021, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

52 D.E. Sanger, "U.S. Accuses North Korea of Mounting WannaCry Cyberattack", *New York Times*, 18 December 2017, https://www.nytimes.com/2017/12/18/us/politics/us-north-korea-wannacry-cyberattack.html.

53 Headquarters Army Training Command, "Indian Army Doctrine", 2004, https://www.files.ethz.ch/isn/157030/India%202004.pdf.

54 M.K. Narayanan, "The Best Among Limited Options", *The Hindu*, 21 September 2016, https://www.thehindu.com/opinion/lead/The-best-among-limited-options/article14990381.ece.

operations) in which "future wars are likely to be fought".[55] The National Cyber Security Strategy, currently being developed, promises to provide additional insight.[56]

The 2015 Israel Defense Forces Strategy Document identifies cyberspace as an area of combat for Israel. An unofficial translated version suggests that the document notes the role of cyber efforts in supporting both defensive and offensive combat efforts, and also in strengthening strategic and tactical deterrence.[57] The document recognizes cyber operations as an integral part of the offensive and defensive activities of the Israel Defense Forces. In 2012, Israeli Defense Minister Ehud Barak had already confirmed development of offensive cyber capabilities.[58] The National Cyber Security Strategy of 2017 confirms the offensive and defensive nature of the State's cybersecurity efforts.[59]

Little is publicly known of the cyber doctrine of Pakistan. The National Cyber Security Policy 2021 stipulates the main principles pertaining to defence from cyber threats. It considers "a cyber-attack on [critical infrastructure] as an act of aggression against national sovereignty and [Pakistan] will defend itself with appropriate response measures".[60] Several regional experts have noted the particular challenges of securitizing cyberspace in the State, citing the rapid growth in the use of information and communication technologies and constraints placed upon the State by traditional security culture.[61]

2.2.3. Nuclear Alliances

NATO in its 2016 Warsaw Summit Communiqué recognized cyberspace as an "operational domain", and noted the integration of cyber defence into its "operational planning and Alliance operations and missions" as means of supporting its deterrence and defence.[62] It has since developed a joint cyber doctrine and is currently working on developing a comprehensive cyber defence policy. The 2020 Allied Joint Doctrine for Cyberspace Operations outlines the role of cyber offence (conducted by States contributing to the Alliance) and defence in the military context, and provides an operational manual on planning and conducting cyber operations.[63] Elements of doctrine can also be found in the 2016 Cyber Defense Pledge—committing to "develop the full range of capabilities to defend our national infrastructures and networks".[64] The 2021 Brussels Summit Declaration suggests that "the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack", with responses that "need not be restricted to the cyber domain", with the potential for invoking the Alliance's collective defence clause.[65]

The role of cyberspace has been elevated in other nuclear alliances as well, albeit with less formal elaboration on the nature of cooperation and operations. Recent joint statements from the United States and Japan and the United States and the Republic of Korea referred to cyber security in the context of

---

55 Headquarters Integrated Defence Staff Ministry of Defence, "Joint Doctrine Indian Armed Forces", 2nd ed., 2017, https://www.ids.nic.in/IDSAdmin/upload_images/doctrine/JointDoctrineIndianArmedForces2017.pdf.

56 New Delhi Times Bureau, "India Takes Measures to Boost Cybersecurity Architecture", *New Delhi Times*, 16 November 2020, https://newdelhitimes.com/india-takes-measures-to-boost-cybersecurity-architecture.

57 Belfer Center for Science and International Affairs, "Deterring Terror: How Israel Confronts the Next Generation of Threats. English Translation of the Official Strategy of the Israel Defence Forces", trans. S. Rosenberg, 2016, https://www.belfercenter.org/sites/default/files/legacy/files/IDFDoctrineTranslation.pdf.

58 G. Cohen and O. Yaron, "Barak Acknowledges Israel's Cyber Offensive for First Time", *Haaretz*, 6 June 2012, https://www.haaretz.com/barack-acknowledges-israel-s-cyber-offensive-for-first-time-1.5170714.

59 State of Israel Prime Minister's Office National Cyber Directorate, "Israel National Cyber Security Strategy in Brief", 2017 https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf.

60 Government of Pakistan Ministry of Information Technology and Telecommunication, "National Cyber Security Policy 2021", 2021, https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf.

61 A. Rafiq, "Challenges of Securitising Cyberspace in Pakistan" , *Strategic Studies*, vol. 39, no. 1, 2019, pp. 90–101, https://www.jstor.org/stable/48544290; M. Yasin, "Cyber Security Imperatives and Pakistan's Readiness: A Brief Overview", *Journal of Development Policy, Research & Practice*, vol. 2, no. 1, 2018, pp. 59–77, https://www.sdpi.org/journal/controlpanel/assets/lib/uploads/158995320639145.pdf. On this point, Pakistani government officials and military personnel have reportedly been the target of major cyber-attacks in recent years. See Inter-Services Public Relations, "Pakistan's Intelligence Agencies have Identified a Major Cyber-attack by Indian Intelligence Agencies", 12 August 2020, https://www.ispr.gov.pk/press-release-detail.php?id=5806.

62 North Atlantic Treaty Organization, "Warsaw Summit Communiqué", 9 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

63 North Atlantic Treaty Organization, "Allied Joint Doctrine for Cyberspace Operations", 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.

64 North Atlantic Treaty Organization, "Cyber Defence Pledge", 2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

65 North Atlantic Treaty Organization, "Brussels Summit Declaration", 2018, para. 32, https://www.nato.int/cps/en/natohq/official_texts_156624.htm#20. This was reiterated in the June 2021 Brussels Summit Communiqué.


© Cameron Smith

deepened defence cooperation.[66] Bilateral collaboration on cyber security has also featured in numerous United States and Australia joint statements; the recent AUKUS pact between Australia, the United Kingdom, and the United States has cyber security dimensions.[67] Meanwhile, the Collective Security Treaty Organization, generally considered a nuclear alliance, highlights the challenge of information security in its 2016 Strategy Document, and a 2017 Agreement on Cooperation in Provision of Information Security refers to measures to jointly secure the Organization's space.[68] There remain questions as to whether article 4 of the Charter of the Organization, which considers aggression on one member as aggression on all, could encompass cyber operations.[69]

---

66 The White House, "U.S.–Japan Joint Leaders' Statement", 16 April 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/16/u-s-japan-joint-leaders-statement-u-s-japan-global-partnership-for-a-new-era;
The White House, "U.S.–ROK Leaders' Joint Statement", 21 May 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/21/u-s-rok-leaders-joint-statement.

67 Prime Minister; Minister for Defence; Minister for Foreign Affairs; Minister for Women (16 September 2021). "Australia to pursue Nuclear-powered Submarines through new Trilateral Enhanced Security Partnership". Prime Minister of Australia, https://www.pm.gov.au/media/australia-pursue-nuclear-powered-submarines-through-new-trilateral-enhanced-security.

68 Collective Security Treaty Organization, "СТРАТЕГИЯ коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года", 18 October 2016, https://odkb-csto.org/documents/documents/strategiya_kollektivnoy_bezopasnosti_organizatsii_dogovora_o_kollektivnoy_bezopasnosti_na_period_do; Collective Security Treaty Organization, "О ратификации Соглашения о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности", 30 November 2017, https://adilet.zan.kz/rus/docs/Z1900000234.

69 See R. Elamiryan and R. Bolgov, "Cybersecurity in NATO and CSTO: Comparative Analysis of Legal and Political Frameworks", in A. Josang (ed.), *Proceedings of the 17th European Conference on Cyber Warfare and Security*, 2018.

3. DIRECT NUCLEAR ESCALATION RISK

Extensive modernization plans will further incorporate digital technologies into the nuclear enterprise; the militarization of cyberspace and growth of cyber capabilities among nuclear-armed and nuclear-allied States also will likely continue. This paper has explored the presence of known accidents and errors (including malfunctions) in cyber–nuclear interactions to date, but the spectrum of escalatory risk possibilities at the cyber–nuclear nexus is vast. Experts have considered the 'attack surface' of nuclear weapons and related systems and presented lists of potentially vulnerable areas; they have disaggregated types of cyber threats and operations and speculated as to the consequences of operations across different nuclear segments.[70] Many of these identify specific use scenarios—warning, for instance, that the use of cyber operations as a force multiplier ahead of a conventional confrontation could lead to inadvertent nuclear escalation.[71]

The next sections of this report discuss potential pathways to nuclear escalation emanating from the cyber domain. This section focuses on direct interactions between cyber capabilities and nuclear forces that could drive nuclear use; the following section considers indirect interactions (that is, situations in which escalation can be triggered by cyber operations even if they do not target or engage nuclear forces). Rather than revisit the universe of system vulnerabilities, this discussion seeks to identify—from the perspective of nuclear-armed and nuclear-allied States—what constitute the critical cyber 'entry points' in their existing systems that could elicit a nuclear response. Doing so requires an understanding of the different ways in which cyber operations can impact on global nuclear order (and in particular nuclear deterrence), and of the 'red lines' underlying State perceptions of when, in fact, deterrence failure has taken place.

Before proceeding further, it is worth noting that the attribution of cyber operations is a complex if not impossible undertaking.[72] Accordingly, the challenges associated with attribution may inhibit the ability of States to retaliate; some even argue that this may lessen the likelihood of crisis and escalation.[73] At the same time, the scale of operations discussed in this paper can allow "opportunities for tracing and analysis that are not possible with common criminal cyberattacks".[74] Some level of attribution seems likely given the attribution capabilities claimed by States, and the circumstances in which operations would take place. Moreover, given the sensitivity of targets discussed in these next two sections, it seems likely that attribution supported by circumstantial evidence would not necessarily inhibit a forceful response.

3.1. THROUGH THE LENS OF NUCLEAR DOCTRINE

Public statements of nuclear policy, whether expressed in doctrine or directly by political or military leaders, should not be taken at face value. Their formation reflects a host of considerations domestic and foreign; their formulation does not ensure uptake in a manner that effectuates operations.[75] Still, as in the cyber domain, expressed doctrines and strategies have analytical utility because of their purposeful signalling effects. Most of the nine States that possess nuclear weapons to some degree have outlined the circumstances in which they would be prepared to use nuclear weapons. In some cases, they specifically

---

70 See S. Avin and S.M. Amadae, "Autonomy and Machine Learning at the Interface of Nuclear Weapons, Computers and People", in V. Boulanin (ed.), *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, Volume I: Euro-Atlantic Perspectives*, SIPRI, 2019, https://www.sipri.org/publications/2019/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-i-euro-atlantic; B. Unal and P. Lewis, "Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences", Chatham House, 2018, https://www.chathamhouse.org/2018/01/cybersecurity-nuclear-weapons-systems.

71 G. Perkovich et al., "China–US Cyber-Nuclear C3 Stability", Carnegie Endowment for International Peace, 2021, https://carnegieendowment.org/2021/04/08/china-u.s.-cyber-nuclear-c3-stability-pub-84182.

72 General Assembly, "Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", UN document A/76/135, 14 July 2021, para. 22, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf; Swiss Confederation, "National Strategy for the Protection of Switzerland against Cyber Risks", 19 June 2021 (rev.), p. 10, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf.

73 S. Kreps and J. Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics", *Journal of Cybersecurity*, vol. 5, no. 1, 2019, https://doi.org/10.1093/cybsec/tyz007.

74 N.C. Rowe, "The Attribution of Cyber Warfare", in J.A. Green (ed.), *Cyber Warfare: A Multidisciplinary Analysis*, 2016, p. 71.

75 See W. Wan, "Nuclear Escalation Strategies and Perceptions: The United States, the Russian Federation, and China", UNIDIR, 2021, p. 11, https://doi.org/10.37559/WMD/21/NRR/02.

acknowledge potential for escalation linked to the cyber domain; in most cases, there is the possibility to consider use in response to cyber operations.

The United States under President Biden is undertaking a nuclear posture review; the 2018 version the administration inherits makes explicit reference to the cyber domain. The "extreme circumstances" that drive consideration of nuclear weapon use include "significant non-nuclear strategic attacks", which comprise "attacks on the U.S., allied, or partner civilian population or infrastructure, and attacks on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities".[76] While 'attack' is left undefined, elsewhere the document paints non-nuclear strategic threats as including chemical, biological, cyber and "large-scale conventional aggression".[77] Cyberspace concerns are expressed throughout the document, which pledges to strengthen NC3 protection and makes note of Russian and Chinese "offensive cyberspace capabilities to deter, disrupt, or defeat U.S. forces dependent on computer networks".[78] According to some analysts, an earlier draft had suggested limited nuclear-use options as a means to deter Russian attacks in outer space and cyberspace;[79] as it stands, the text suggests that US nuclear deterrence encompasses the cyber domain. [80]

For the Russian Federation and China, the other participants in what the United States frames as a 'great power competition', explicit references to cyberspace in their nuclear doctrines are absent. China's firm declaration of no-first-use of nuclear weapons "at any time and under any circumstances" effectively removes cyber operations as a potential trigger event.[81] While Beijing's commitment to no-first-use has been questioned by officials in other States, some experts have cited unofficial translated versions of Chinese military documents as affirmation of that policy.[82] Concepts of multi- or cross-domain deterrence seem incompatible with a 2013 claim that Chinese nuclear weapons will not be used to deter non-nuclear enemy military activity.[83] Meanwhile, the Russian Federation has underlined its right to retaliate with nuclear weapons "when the very existence of the state is in jeopardy".[84] It does define as a condition for nuclear-use consideration an "attack by [an] adversary against critical governmental or military sites … disruption of which would undermine nuclear forces response actions".[85] The precise nature of such attacks is not elaborated upon, allowing for the possibility of a cyber 'red line'.

The nuclear policies of France and the United Kingdom contain similar ambiguity into which cyber operations could slot. Consideration of nuclear weapon use would take place "only in extreme circumstances of legitimate self-defence" (France) or "in extreme circumstances of self-defence, including the defence of our NATO allies" (United Kingdom). These are long-held positions. At the same time, France's 2017 Defence and National Security Review underlines the value of deterrence from any aggression against its vital interests—"whatever form it may take"; the document also points to cyberspace as a domain in which escalation risks "potentially crossing the nuclear threshold" are acute.[86] The United Kingdom's 2021 Integrated Review similarly acknowledges potential "multi-domain crisis" that reflects a "more complex range of routes for escalation, including to nuclear coercion".[87] It also allows for revisiting the negative security assurances the United Kingdom grants given "the future threat of … emerging technologies".[88]

---

76 US Department of Defense, "Nuclear Posture Review 2018", 2018, p. 21, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEWFINAL-REPORT.PDF.
77 Ibid, p. 38.
78 Ibid, p. 7.
79 M. Klare, "Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation", *Arms Control Today*, vol. 49, no. 9, 2019, https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation.
80 See C.A. Ford, "Strategic Stability and the Global Race for Technology Leadership", *Arms Control and International Security Papers*, vol. 1, no. 21, 2020, https://2017-2021.state.gov/wp-content/uploads/2020/11/T-paper-series-Strategic-Stability-and-Tech-508.pdf.
81 State Council Information Office of the People's Republic of China, "China's National Defense in the New Era", 2019, chp. 2, http://www.xinhuanet.com/english/2019-07/24/c_138253389.htm.
82 G. Kulacki, "The Chinese Military Updates China's Nuclear Strategy", Union of Concerned Scientists, 2015, https://www.ucsusa.org/resources/chinas-nuclear-weapons-strategy.
83 Ibid.
84 President of the Russian Federation, "Basic Principles of State Policy of the Russian Federation on Nuclear Deterrence", 2020, para. 17, https://www.mid.ru/en/foreign_policy/international_safety/disarmament/-/asset_publisher/rp0fiUBmANaH/content/id/4152094.
85 Ibid, para. 19.
86 Government of France, "Defence and National Security Strategic Review", 2017, pp. 49 and 69, https://cd-geneve.delegfrance.org/Defence-and-National-Security-Strategic-Review-1890.
87 Government of the United Kingdom, "Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy", 2021, p. 72, https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.

While the document keeps its discussion of cyberspace largely separate from that of nuclear deterrence, a multi-domain concept of deterrence is implicit. In pledging its "full spectrum of forces" to NATO, the United Kingdom cites both its nuclear deterrent and its offensive cyber capabilities.[89]

For nuclear-armed States outside of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), doctrinal space for nuclear use in response to cyber operations takes varied form. Like China, India elaborates a no-first-use policy—while additionally retaining the nuclear option in case of a major attack using biological or chemical weapons on its forces.[90] Some experts have argued that India is shifting from this point of doctrine;[91] such concerns have been exacerbated as Indian officials have referred to an "evolving" doctrine and observed that its future commitment to no-first-use "depends on the circumstances".[92] In comparison, Pakistan has not publicly stated a nuclear doctrine, but its National Command Authority outlined and reaffirmed a pursuit of full-spectrum deterrence against "all forms of aggression".[93] Such a framing contains inherent flexibility for cyber operations.[94] Room for consideration of nuclear use in response to cyber operations is abundant for the Democratic People's Republic of Korea and Israel, a function of the opacity of their respective nuclear weapons programmes. The Democratic People's Republic of Korea observed that its stockpile can be used "to repel invasion or attack from a hostile nuclear weapons state and make retaliatory strikes", and cited their purpose as "deterring and repelling the aggression and attack of the enemy".[95] Israel has not publicly acknowledged its nuclear weapons possession, leaving the possible conditions of their use largely unknown.[96]

3.2. ROOM FOR MANOEUVRABILITY

The subjectivity of terms found in nuclear doctrines like 'extreme circumstances', 'vital interests', 'critical sites', even 'attack' and 'aggression', reflects deliberate ambiguity employed by States, underlining the limited nature of self-restraint against nuclear use.[97] That many States have reserved in their policies a right to nuclear use highlights the need for further exploration of when they may exercise that right, and specifically when they could determine that the threshold for use is reached due to adversarial activity in the cyber domain. A recurrent theme in strategic doctrines is the central role of extended nuclear deterrence. Broadly speaking, the practice of nuclear deterrence entails employing a credible, reliable, and effective threat of nuclear weapon use (in kind or in an escalatory fashion) in order to dissuade attack by an adversary on a State's nuclear forces or territory, or the territory of an ally.[98] Critical to effective nuclear deterrence is a secure second-strike or retaliatory capability.[99] Accordingly, any cyber operations that undermine this capability represent the most direct path to deterrence failure, and potential nuclear use.

---

88 Ibid, p. 77.
89 Ibid, p. 72.
90 Ministry of External Affairs, "The Cabinet Committee on Security Reviews Operationalization of India's Nuclear Doctrine", 4 January 2003, https://mea.gov.in/press-releases.htm?dtl/20131/The_Cabinet_Committee_on_Security_Reviews_perationalization_of_Indias_Nuclear_Doctrine+Report+of+National+Security+Advisory+Board+on+Indian+Nuclear+Doctrine.
91 C. Clary and V. Narang, "India's Counterforce Temptations: Strategic Dilemmas, Doctrine, and Capabilities", *International Security*, vol. 43 no. 3, 2018/19, https://doi.org/10.1162/isec_a_00340.
92 Ministry of External Affairs, "Speech by NSA Shri Shivshankar Menon at NDC on 'The Role of Force in Strategic Affairs'", 21 October 2010, https://www.mea.gov.in/Speeches-Statements.htm?dtl/798/Speech+by+NSA+Shri+Shivshankar+Menon+at+NDC+on+The+Role+of+Force+in+Strategic+Affairs; S. Miglani, "India Says Committed to 'No First Use' of Nuclear Weapons for Now", *Reuters*, 16 August 2019, https://www.reuters.com/article/us-india-nuclear-idUSKCN1V613F
93 Inter-Services Public Relations, Press Release no. PR-133/2013-ISPR, 5 September 2013, https://www.ispr.gov.pk/press-release-detail.php?id=2361.
94 Former Pakistani Director General of the Strategic Plans Division Khalid Kidwai in 2002 outlined four red lines that could trigger a nuclear response, including 'political destabilization'; see B. Chakma, "Pakistan's Nuclear Doctrine and Command and Control System: Dilemmas of Nuclear Forces in the Second Atomic Age", *Security Challenges*, vol. 2, no. 2, 2006, https://www.jstor.org/stable/26459035.
95 Korean Central News Agency, "Law on Consolidating Position of Nuclear Weapons States Adopted", 1 April 2013, http://www.kcna.co.jp/item/2013/201304/news01/20130401-25ee.html.
96 See H. Elbahtimy, "Risks of Nuclear Use in the Middle East", in W. Wan (ed.), *Nuclear Risk Reduction: Closing Pathways to Use*, UNIDIR, 2020, https://doi.org/10.37559/WMD/20/NRR/01.
97 Besides no-first-use policies, another form of self-restraint includes limited negative security assurances. For an overview of these, see "Mapping Negative Security Assurances: Background Paper for Subsidiary Group 4 of the Conference on Disarmament", UNIDIR, 12 June 2018, https://www.unidir.org/files/medias/pdfs/background-paper-to-inform-cd-subsidiary-body-4-discussion-eng-0-780.pdf.
98 B. Tertrais, "Principles of Nuclear Deterrence and Strategy", NDC Research Paper no. 19, 2021, p. 39, https://www.ndc.nato.int/news/news.php?icode=1570.
99 More offensive deterrence variations are oriented towards first-strike advantage, involving the development of capabilities that aim to "disarm an adversary's nuclear launch platforms, early warning systems, or command and control" and other counterforce targets; see N. Teeple, "Offensive Weapons and the Future of Nuclear Arms Control", *Canadian Journal of European and Russian Studies*, vol. 14, no. 1, 2020, p. 82, https://doi.org/10.22215/cjers.v14i1.2695.

3.2.1. Towards Deterrence Failure

For the NPT nuclear-weapon States and India, nuclear-powered ballistic missile submarines constitute a key pillar of nuclear deterrence. This is because their mobility and stealth ensure their survivability and render them "invulnerable to a surprise first strike".[100] Some experts have argued that submarine network architectures are essentially 'air gapped'; even if this were the case, they would not be insulated from threat.[101] Cyber operations against either submarines themselves—for example, infiltration during their procurement, operation, or maintenance—or their NC3 systems could directly challenge deterrence capability and credibility; this is exacerbated by the number of commercial entities involved as suppliers of components and software in many nuclear-armed States.[102] The scenario is not far-fetched. A Russian defence contractor linked to the development of naval submarines was targeted in May 2021 with malware capable of identifying files of interest and creating longer-term vulnerabilities (there was no indication the malware succeeded in this instance).[103] Similarly, cyber operations in January 2021 against the software manufacturing company Solarwinds breached the Los Alamos National Laboratory, involved in the production of US nuclear weapons (US officials reported no known impact).[104] Meanwhile, some speculate that the launch order broadcasting systems used in the submarines of some nuclear-armed States could be vulnerable; US internal tests in the 1990s had gained back-door access to that of Trident submarines.[105] The uncovering of such operations targeting ballistic missile submarines and related systems could undermine the assured retaliatory capability of nuclear-armed States, and in times of crisis prompt a forceful military response that could drive potential nuclear escalation.

There exist other means through which nuclear-armed States have sought to secure or strengthen their second-strike capability. With an eye towards improving the "reliability, survivability, and penetrability" of their arsenals, and in response to the development of conventional precision-strike capabilities, many States have turned to the deployment of land-based mobile ballistic missiles.[106] For the Russian Federation and China, the importance of such missiles lies in their

---

100 N. Ritchie and P. Ingram, "A Progressive Nuclear Policy: Rethinking Continuous-at-Sea Deterrence", *The RUSI Journal*, vol. 155, no. 2, 2010, p. 41, https://doi.org/10.1080/03071847.2010.486550.

101 S. Abaimov and P. Ingram, "Hacking UK Trident: A Growing Threat", BASIC, June 2017, https://basicint.org/publications/stanislav-abaimov-paul-ingram-executive-director/2017/hacking-uk-trident-growing-threat; J. Johnson, "'Catalytic Nuclear War' in the Age of Artificial Intelligence & Autonomy: Emerging Military Technology and Escalation Risk Between Nuclear-Armed States", *Journal of Strategic Studies*, 2021, https://doi.org/10.1080/01402390.2020.1867541.

102 H. Lin, "Cyber Risk Across the US Nuclear Enterprise", *Texas National Security Review*, vol. 4, no. 3, 2021, http://dx.doi.org/10.26153/tsw/13986; B. Zala, "Strategic Non-Nuclear Weapons, SSBNs, and the New Search for Strategic Stability", in R. Metcalf et al. (eds), *The Future of the Undersea Deterrent: A Global Survey*, 2020, https://nsc.crawford.anu.edu.au/publication/16145/future-undersea-deterrent-global-survey.

103 J. Trevithick, "Top Russian Submarine Design Bureau Hit by Cyber Attack with Chinese Characteristics", The Drive, 10 May 2021, https://www.thedrive.com/the-war-zone/40531/top-russian-submarine-design-bureau-hit-by-cyber-attack-with-chinese-characteristics.

104 N. Bertrand, "Nuclear Weapons Agency Updates Congress on Hacking Attempt", Politico, 22 December 2020, https://www.politico.com/news/2020/12/22/nuclear-weapons-agency-congress-hacking-450184.

105 S. Peterson, "Old Weapons, New Terror Worries", The Christian Science Monitor, 15 April 2004, https://www.csmonitor.com/2004/0415/p06s02-woeu.html.

106 M. Taylor Fravel and E.S. Medeiors, "China's Search for Assured Retaliation: The Evolution of Chinese Nuclear Strategy and Force Structure", *International Security*, vol. 35, no. 2, 2010, p. 81, https://doi.org/10.1162/ISEC_a_00016.

enhanced survivability in case of a counterforce attack by an adversary.[107] But through the prism of escalation, these systems also present entry points—especially due to increased digitalization—through which cyber operations could directly drive deterrence failure. The integration of cyber capabilities with other technologies has already enhanced the ability of States to hunt down mobile missile systems.[108] The possibility may not pose an existential threat for nuclear-armed States that have achieved true nuclear triads. But for those States whose deterrent is based on less diverse nuclear arsenals, concerted cyber operations that threaten their mobile missiles could represent a red line, prompting a decisive response and in particular circumstances even providing potential justification for considering nuclear response.

A related entry point is the systems that facilitate the ability of States to preserve their nuclear forces, absorb initial attack, and consequently exercise their retaliatory capability. These include NC3 and early warning, which as discussed have been prone to malfunction in the past. Decision makers in some nuclear-armed States have expressed concerns about the susceptibility of their own systems to cyber operations. A UK House of Lords Select Committee called for an inquiry into NC3 resilience.[109] A US classified cybersecurity assessment drove a "significant increase in focus" in the area,[110] while the 2018 Nuclear Posture Review also noted "considerable [external] effort to design and use cyber weapons against networked systems", including NC3.[111] This is significant, given that current US nuclear doctrine refers specifically to cyber operations on its NC3 and early warning capabilities as a red line.[112] There already exists evidence that the classified satellite communications channel of at least one nuclear-armed State (India) has been previously penetrated by cyber operations.[113] Some experts suggest a blurry line between electronic and cyber warfare here, which could expand the spectrum of escalation possibility—especially as some States pursue directed-energy weapons that can be employed against satellite sensors.[114]

3.2.2. Vital Interests and Critical Infrastructure

The deterrent role of nuclear weapons provides a critical means through which certain cyber operations could drive consideration of nuclear use. Among the entry points for nuclear use are threats to the sovereign State. As mentioned, phrases like 'self-defence', 'vital interests', and the 'existence of the State' are inherently subjective and context dependent; for instance, France highlights that central to its concept of vital interests is "the protection of our people";[115] the United States lists as potential extreme circumstances attacks on its "civilian population or infrastructure".[116] General references to attacks on the State or its people present a space in which massive cyber operations could infringe, especially with increasing perceptions of cyberspace as a warfighting domain. Indeed, referencing the collective defence clause, the NATO Secretary General acknowledged that a "serious cyberattack could trigger Article 5" (and thus elicit a potential response from the nuclear alliance), even as he noted the wide range of such attacks.[117]

---

107 A. Bodrov, "Reducing the U.S. and Russian Nuclear Arsenals: Yesterday, Today, Tomorrow", in A. Pavlov and L. Deriglazova (eds), *Nuclear Russia: International and Domestic Agendas*, 2020, p. 40.

108 P. Bracken, "The Cyber Threat to Nuclear Stability", Orbis, vol. 60, no. 2, 2016, p. 189, https://doi.org/10.1016/j.orbis.2016.02.002.

109 House of Lords Select Committee on International Relations, "Rising Nuclear Risk, Disarmament and the Nuclear Non-Proliferation Treaty: Government Response", https://www.parliament.uk/globalassets/documents/lords-committees/International-Relations-Committee/NPT-and-Nuclear-Disarmament/Government-Response-Risng-nuclear-risk-disarmament-and-the-Nuclear-Non-Proliferation-Report.pdf.

110 Office of the Director, Operational Test and Evaluation, "FY19 Cybersecurity: Cyber Assessments", 2019, p. 230, https://www.dote.osd.mil/Portals/97/pub/reports/FY2019/other/2019cyber-assessments.pdf?ver=2020-01-30-115600-800.

111 US Department of Defense, "Nuclear Posture Review 2018", 2018, p. 57, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEWFINAL-REPORT.PDF.

112 Ibid, p. 21.

113 T. Harrison et al., "Space Threat Assessment 2019", CSIS, 2019, https://aerospace.csis.org/wp-content/uploads/2019/04/SpaceThreatAssessment2019-compressed.pdf.

114 D. Stefanovich, "Russia's Basic Principles and the Cyber-Nuclear Nexus", European Leadership Network Commentary, 14 July 2020, https://www.europeanleadershipnetwork.org/commentary/russias-basic-principles-and-the-cyber-nuclear-nexus; Congressional Research Service, "Defense Primer: Energy-Directed Weapons", 20 July 2021, https://fas.org/sgp/crs/natsec/IF11882.pdf.

115 Government of France, "Defence and National Security Strategic Review", 2017, p. 52, https://cd-geneve.delegfrance.org/Defence-and-National-Security-Strategic-Review-1890.

116 US Department of Defense, "Nuclear Posture Review 2018", 2018, p. 2, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEWFINAL-REPORT.PDF

117 Cyberattacks "can inflict billions of dollars' worth of damage to our economies, bring global companies to a standstill, paralyse our critical infrastructure, undermine our democracies and cripple our military capabilities"; J. Stoltenberg, "NATO will Defend Itself", *Prospect*, October 2019, p. 4, https://www.prospectmagazine.co.uk/content/uploads/2019/08/Cyber_Resilience_October2019.pdf.

The intertwined nature of the security of the State and its people in some nuclear doctrines and strategies has significant implications for escalatory risk, manifesting in the concept of 'critical infrastructure'.[118] After all, attacks on assets "essential for the maintenance of functions vital to the well-being of a given society" would seem by their nature to threaten vital interests, constitute extreme circumstances, and threaten the State itself.[119] National definitions largely correspond with this general concept.[120] Both United Nations processes dedicated to ICT in the context of international security, the Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG), have paid particular attention to the protection of critical infrastructure. The former observed specifically that a cyber operation against a critical infrastructure asset "can have cascading domestic, regional and global effects [posing] an elevated risk of harm to the population, and can be escalatory, possibly leading to conflict".[121] On this point, President Biden at the Geneva Summit provided President Putin a list of 16 critical infrastructure sectors that were meant to be "off-limits".[122]

---

118 J. Moteff and P. Parfomak, "Critical Infrastructure and Key Assets: Definition and Identification", CRS Report for Congress, 2004, https://apps.dtic.mil/sti/pdfs/ADA454016.pdf.

119 A. Kastelic, "International Cooperation to Mitigate Cyber Operations against Critical Infrastructure: Normative Expectations and Emerging Good Practices", UNIDIR, 2021, p. 1, https://unidir.org/criticalinfrastructure.

120 See UK Centre for the Protection of National Infrastructure, "Critical National Infrastructure", 2021, https://www.cpni.gov.uk/critical-national-infrastructure-0: Critical infrastructure is comprised of "[t]hose critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in: a) Major detrimental impact on the availability, integrity or delivery of essential services—including those services whose integrity, if compromised, could result in significant loss of life or casualties—taking into account significant economic or social impacts; and/or b) Significant impact on national security, national defence, or the functioning of the state". For the Russian definition see: Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации, 2012, http://www.scrf.gov.ru/security/information/document113.

121 General Assembly, "Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", UN document A/76/135, 14 July 2021, para. 42, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

122 V. Soldatkin and H. Pamuk, "Biden Tells Putin Certain Cyberattacks Should be 'Off-Limits'", *Reuters*, 17 June 2021, https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16.

Ultimately, every State determines the scope of its critical national infrastructure.[123] And indeed, any definition of critical infrastructure is highly dependent on the national context; as some States dependent on particular industries may consider qualifying assets as critical infrastructure, others, less dependent on the same sector, may not.[124] Generally speaking, water management, food, energy, healthcare, transport, manufacturing, finance, and communications are sectors frequently considered to qualify as national critical infrastructure.[125] The same is the case for the defence and government sectors, which are officially recognized as critical infrastructure in many nuclear-armed States. A number of regional organizations have also put forward definitions of critical infrastructure in the last decade.[126] Ultimately though, there remains a degree of uncertainty as to which assets targeted by cyber operations would in fact cause a nuclear-armed State to consider nuclear response; it is likely that any such consideration would depend not only on the target of the operation but also the scope of the negative consequences on the well-being or safety of a given State and its people.

3.3. DEVELOPING RISK

The ongoing development and potential use of emerging technologies in nuclear weapons and related systems will create new entry points for cyber operations. Nuclear forces are becoming more digitalized and networked, while early warning and NC3 systems are likely to incorporate more automation and machine learning.[127] Such trends impact on vulnerability: for instance, the US Department of Defense, in testing its weapons systems under development, "routinely found mission-critical cyber vulnerabilities" despite utilizing tests "limited in scope and sophistication"; the document finds especially concerning that the results were sometimes "discounted … as unrealistic.[128] Already a number of nuclear-armed and nuclear-allied States are deploying uncrewed vehicles, in air, land, and sea, some tasked with functions central to the practice of nuclear deterrence, and all of which must be supported by other complex systems.[129] The Russian Federation has commissioned submarines it plans to equip with dual-capable Poseidon uncrewed underwater vehicles, a strategic system aiming to strengthen its second-strike capability.[130] For its part, the United States has focused its uncrewed underwater vehicle programme on anti-submarine warfare capabilities: the role of that force is to "hold the adversary's strategic assets at risk from the undersea."[131] Such auto-nomous naval systems rely on data (including in navigation) that can be susceptible to sophisticated attacks. The fact that these will be considered "prime targets" for cyber operations underlines the possibility of deterrence failure stemming from direct cyber–nuclear interactions—interactions that are likely to increase.[132]

123 This is confirmed in Security Council resolution 2341, 13 February 2017, p. 2.
124 See United Nations Counter-Terrorism Committee Executive Directorate and United Nations Office on Counter-Terrorism, 2018, *The Protection of Critical Infrastructures against Terrorist Attacks: Compendium of Good Practices*, as of 7 September 2021, https://unrcca.unmissions.org/publication-%E2%80%9C-protection-critical-infrastructure-against-terrorist-attacks-compendium-good-practices.
125 See Russian Federation, Federal Law No. 187-FZ, "On the Security of the Critical Information Infrastructure of the Russian Federation", 26 July 2017; UK Centre for the Protection of National Infrastructure, "Critical National Infrastructure", 2021, https://www.cisa.gov/critical-infrastructure-sectors; SGDSN, "The Critical Infrastructure Protection in France", 2017, www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf; Government of India, "National Critical Information Infrastructure Protection Centre", https://nciipc.gov.in.
126 Including the Shanghai Cooperation Organization, the Inter-American Committee against Terrorism, and the African Union.
127 J. Hruby and M.N. Miller, "Assessing and Managing the Benefits and Risks of Artificial Intelligence in Nuclear-Weapon Systems", NTI Paper, 2021, https://media.nti.org/documents/NTI_Paper_AI_r4.pdf; J. Johnson and E. Krabill, "AI, Cyberspace, and Nuclear Weapons", War on the Rocks, 31 January 2020, https://warontherocks.com/2020/01/ai-cyberspace-and-nuclear-weapons.
128 US Government Accountability Office, "Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities", 2018, p. 21, https://www.gao.gov/assets/gao-19-128.pdf, p. 21.
129 L. Xiang, "Artificial Intelligence and its Impact on Weaponization and Arms Control", in L. Saalman (ed.), The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, Volume II: East Asian Perspectives, SIPRI, 2019, https://www.sipri.org/publications/2019/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-ii-east-asian.
130 V. Kashin, "Artificial Intelligence and Military Advances in Russia", in L. Saalman (ed.), *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*, Volume II: East Asian Perspectives, SIPRI, 2019, https://www.sipri.org/publications/2019/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-ii-east-asian.
131 US Navy, "Commander's Intent for the United States Submarine Force and Supporting Organizations", 2018, p. 10, https://www.csp.navy.mil/Portals/2/documents/about/Commanders-Intent-201803.pdf.
132 N. Mazzucchi, "Cyber, A Particular Field of Naval Thought", Études Marines, no. 17, 2020, p. 77, https://cesm.marine.defense.gouv.fr/images/etude/EM17_-EN__NUM.pdf.

4. INDIRECT NUCLEAR ESCALATION RISK

Direct engagement between cyber capabilities and nuclear forces has clear potential to drive escalatory pathways towards the use of nuclear weapons. This is a function both of the nature of nuclear deterrence, and the interpretation of nuclear doctrines and strategies. Accordingly, there exist different ways in which cyber operations can be perceived by nuclear-armed and nuclear-allied States as crossing the threshold that would lead to the consideration of nuclear response. In addition, even without direct engagement of nuclear forces, cyber capabilities and operations can have second-order effects that impact on nuclear weapons capabilities, deterrence, and decision-making. This section briefly explores how indirect interactions at the cyber–nuclear nexus present another source of escalatory risk.

4.1. CYBER AS FORCE MULTIPLIER

Aside from its independent strategic value, some experts have argued that the military promise of cyber capabilities is primarily as a force multiplier for conventional capabilities.[133] The US Chairman of the Joint Chiefs of Staff published a guide on cyberspace operations that cites cyberspace attack capabilities as being "generally most effective when integrated with other [capabilities]", with examples of such integrated actions including the "disruption of enemy air defense systems … insertion of messages into enemy leadership's communications, degradation/disruption of enemy space-based and ground-based precision navigation and timing systems, and disruption of enemy [command and control]".[134] This is not isolated thinking—some experts argue that Chinese cyber doctrine similarly stresses "leveraging the asymmetric power of [counterforce cyber capabilities] as force multipliers".[135]

Actions in cyberspace to deny adversaries access to their systems or to manipulate the information in them can enable operations in traditional domains or extend their effects. Israel, for instance, allegedly undertook cyber operations against Syrian air defences in 2007, allowing its fighters to fly undetected—despite not being equipped with stealth technology—to conduct a successful strike on a suspected nuclear reactor site.[136] Military missions that incorporate cyber operations in such a manner effectively extend existing conventional capabilities; for instance, cyber operations could enable conventional weapons (such as hypersonic glide vehicles or precision-guided missiles) to execute missions previously reserved for nuclear weapons.[137] All of this suggests new vulnerabilities for all States, including nuclear-armed States and their allies. Integrated operations thus create more pathways to nuclear deterrence failure by posing new threats to nuclear forces.

4.2. CYBER AND COMMUNICATION

As mentioned, early examples of interference with computer systems linked to nuclear weapons and their operations centred on communications, in the form of electronic operations that targeted radar systems. There are myriad ways in which cyber operations can impact similarly on communications, exacerbating the 'fog of war' which in turn can affect the practice of nuclear deterrence. The strain of the 'always–never dilemma' with respect to nuclear

---

133 M. Smeets, "The Strategic Promise of Offensive Cyber Operations", *Strategic Studies Quarterly*, vol. 12, no. 3, 2018, https://www.jstor.org/stable/10.2307/26481911.

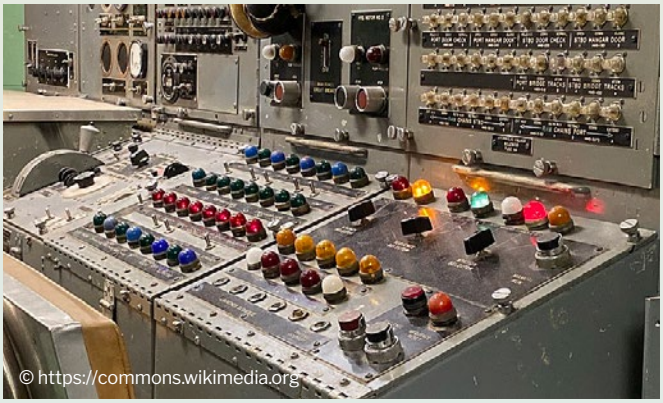
134 Chairman of the Joint Chiefs of Staff, "Cyberspace Operations", Joint Publication 3-12, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

135 W. Matheson, "The Cyber-Nuclear Nexus in East Asia: Cyberwarfare's Escalatory Potential in the US–China Relationship", *Intersect*, vol 14, no. 1, 2020, p. 11.

136 See appendix.

137 J. Borrie, "Nuclear Risk and the Technological Domain: A Three-Step Approach", in W. Wan (ed.), *Nuclear Risk Reduction: Closing Pathways to Use*, UNIDIR, 2020, https://doi.org/10.37559/WMD/20/NRR/01.

weapons—the essential assurance that they will "always work when directed" and at the same time "never be used in the absence of authorized direction"[138]—suggests potentially devasting impacts of cyber operations able to penetrate or muddle the requisite clear communication.[139] This extends both to internal and external channels.


© https://commons.wikimedia.org

With respect to internal communication, cyber operations that succeed in calling into question the reliability of NC3 could artificially create situations reminiscent of the Arkhipov incident during the Cuban Missile Crisis, when a decision not to launch was made on-board because a Soviet submarine captain had reportedly lost contact with Moscow.[140] Operations leading to malfunctions that impact chain of command in a similar manner could drive launch decisions without directly interacting with nuclear forces or necessarily requiring a lot of resources. Another scenario can be linked to the sheer prominence of cyber operations; as one form, information warfare can complicate the nature of signalling both within and among nuclear-armed and nuclear-allied States. In 2016 for instance, a fake news report about Israel threatening nuclear retaliation in the Syrian context led the Pakistani defence minister to make a nuclear threat against Israel on Twitter. The Israeli Ministry of Defence responded (and de-escalated the situation) by pointing out the attributed quote was never said.[141] In times of tension, such operations—including those outside of the public eye—can easily exacerbate crisis and even contribute to escalation.

4.3. CYBER AND DECISION-MAKING

An interrelated source of escalatory risk can be traced to the broader impact of cyber operations on nuclear decision-making. The aforementioned US Joint Chiefs of Staff guide acknowledges basic "challenges to determining the exact origins of cyberspace threats", rendering it "difficult to determine how, when, and where to respond".[142] The timeline of operations and their attribution in the Stuxnet case reflects this characterization. As mentioned, attribution issues linked to cyber operations might in some instances prevent rash decision-making and even escalatory responses; however, the secrecy of the domain also creates fundamental ambiguity that can contribute to unpredictability and undermine perceptions of strategic stability. Some experts argue that offensive cyber operations are not effective deterrence tools since they are inherently "asymmetric and unknown until their use".[143] This characteristic can have destabilizing effects in certain circumstances, for instance with the uncovering of operations compressing crisis and escalation time frames (akin to a 'bolt from the blue' attack), and putting pressure on decision makers to take forceful action. In response to a wave of ransomware attacks in 2021, for instance, the United States acknowledged it considered "all options", including military.[144] Such situations also open the door for possible errors, both human and technical. And, as discussed, existing cyber and nuclear doctrines in many instances do provide clear space for a military or even nuclear response.


© https://commons.wikimedia.org

138 P.D. Feaver, "Command and Control in Emerging Nuclear Nations", *International Security*, vol. 17, no. 3, 1992–1993, https://www.jstor.org/stable/2539133.

139 J.R. Lindsay, "Cyber Operations and Nuclear Weapons", Nautilus Institute, 2019, https://nautilus.org/napsnet/napsnet-special-reports/cyber-operations-and-nuclear-weapons.

140 S.V. Savranskaya, "New Sources on the Role of Soviet Submarines in the Cuban Missile Crisis", *Journal of Strategic Studies*, vol. 28, no. 2, 2005.

141 R. Goldman, "Reading Fake News, Pakistani Minister Directs Nuclear Threat at Israel", *New York Times*, 24 December 2016, https://www.nytimes.com/2016/12/24/world/asia/pakistan-israel-khawaja-asif-fake-news-nuclear.html.

142 Chairman of the Joint Chiefs of Staff, "Cyberspace Operations", Joint Publication 3-12, 2018, p. I-12, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

143 W. Matheson, "The Cyber-Nuclear Nexus in East Asia: Cyberwarfare's Escalatory Potential in the US–China Relationship", *Intersect*, vol 14, no. 1, 2020, p. 11.

144 US Mulling Military Response to Ransomware Attacks, Biden Officials Say", *The Guardian*, 6 June 2021, https://www.theguardian.com/technology/2021/jun/06/us-military-response-ransomware-attacks-biden-russia-putin.

5. RECOMMENDATIONS

Governance of the cyber–nuclear nexus is complicated by the sensitivity of each space. There is an understandable reluctance by States to reveal much about the nature of their capabilities, exacerbated in the cyber domain by blurred lines between what is considered offensive and defensive. In addition, the conduct of cyber operations is inherently secretive. Secrecy of course is also a prominent feature of nuclear weapons programmes, especially pertaining to the components most relevant from a cyber perspective: NC3, early warning, and onboard systems. Accordingly, policy recommendations to reduce the risk of nuclear weapon use linked to the interaction of cyber and nuclear forces must account for the high barriers to transparency—let alone verification.

At the same time, the severe nature of risk linked to cyber–nuclear interactions—as recognized by States themselves—demands a proportionate policy response. States will have to engage at all levels—national, bilateral, regional, multilateral—both 1) to minimize those interactions, direct and indirect, and 2) to ensure that any interactions taking place do not escalate to potential nuclear use. This section explores the means by which States can achieve these dual objectives. Fortunately, there exists a foundation of nuclear risk reduction activities upon which States can build. In addition, the emergence of a normative framework in cyberspace can be critical in addressing risks discussed in this paper. One sign of progress is the recent 2021 consensus reports of the GGE and OEWG on ICT in the context of international security—if they are properly implemented.[145]

5.1. STRENGTHEN NATIONAL CYBERSECURITY

Among the most consequential risk reduction actions, and a focus of both the GGE and OEWG reports, involves national-level policy—that in this context aims to strengthen the physical and cyber security of critical infrastructure, which includes nuclear weapons and related systems. The civil nuclear industry provides a public parallel: experts in that field argue for an understanding of all "threat vectors".[146] Accordingly, an effective cyber risk management approach has to be wide-ranging, taking form in State regulatory guidance, industry norms, security culture, best practices, and consensus standards and frameworks. Applied to the capabilities of nuclear-armed States, this could encompass further elaboration of national cybersecurity and nuclear doctrines and strategies, regular assessments of the cyber resilience of existing systems, diversification of critical systems, rigorous testing of capabilities under development, and intensive training of operators (including through use of 'red team' exercises that emulate the actions of malicious cyber actors).[147] Preparing human operators to step in should automated functions be compromised can provide a firewall against cascading effects from malfunctions.[148]

© https://commons.wikimedia.org

An increasing private sector role requires that States not only elaborate but enforce high standards across the entirety of their supply chains. A basic risk assessment of technologies acquired and actors involved—across contractors and subcontractors—marks a key step.[149] Overall, to account for the vastness of the nuclear enterprise, States should be actively engaged

---

145 General Assembly, "Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", UN document A/76/135, 14 July 2021; General Assembly, "Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security", UN document A/AC.290/2021/CRP.2, 10 March 2021.

146 D. Decker, K. Rauhut, and M. Fabro, "Prioritizing Actions for Managing Cybersecurity Risks", Stimson Center, 2020, https://www.stimson.org/wp-content/uploads/2020/02/DECKER_etal_IAEA-CC-352.pdf.

147 G. Perkovich and A. Levite, "How Cyber Ops Increase the Risk of Accidental Nuclear War", Defense One, 21 April 2021, https://www.defenseone.com/ideas/2021/04/how-cyber-ops-increase-risk-accidental-nuclear-war/173523.

148 For more on the United States, see H. Lin, "Cyber Risk Across the US Nuclear Enterprise", *Texas National Security Review*, vol. 4, no. 3, 2021, http://dx.doi.org/10.26153/tsw/13986.

149 Y. Afina, C. Inverarity, and B. Unal, "Ensuring Cyber Resilience in NATO's Command, Control and Communication Systems", Chatham House, 2020, https://www.chathamhouse.org/2020/07/ensuring-cyber-resilience-natos-command-control-and-communication-systems-0.

at the national level towards ensuring cybersecurity in "sourcing, vendor management, supply chain continuity and quality, transportation security and many other functions" linked to their weapons capabilities.[150] One method of implementation is to mainstream cybersecurity practices in nuclear modernization programmes—this is likely already taking place in some cases, as seen in the United States' 'NC3 Next' improvements (entailing dynamic reconfiguration of software, shifts from incompatible legacy systems, and other steps to enhance cyber resiliency).[151] In addition, nuclear-armed and nuclear-allied States can deploy a similar approach to their critical infrastructure—however they define it.

As suggested, cybersecurity activities in this vein may centre on the individual State (or alliance) yet will require collaborative behaviour. This includes close engagement with the private sector. In addition, multilateral cooperation and transparency measures such as those proposed in the GGE and OEWG reports—strengthening networks around national points of contact, engaging in dialogue and consultation (including on incidents), and sharing views around critical national infrastructure—can bolster the global cybersecurity culture.[152] This could create follow-on effects in the nuclear sphere, as exchange on good practices and approaches (including on detection, attribution, and response; as well as risk management principles and operating procedures) would benefit States individually and simultaneously strengthen global supply chains.[153] Increased transparency can also feed into common understandings of the cyber threat among States.

5.2. DEEPEN COMMON UNDERSTANDINGS

There remains a worrisome ambiguity surrounding critical entry points in the nuclear sphere. The continued militarization of cyberspace can upend an already fragile international security order. Dialogue among nuclear-armed and nuclear-allied States on cyber–nuclear interactions can—at the very least—reinforce the scope of the issue and the urgency of fostering cooperative approaches to address it.[154] Additionally, States may be able to jointly explore the complications cyberspace brings to efforts to "understand one another's interests, redlines, and willingness to use force".[155] The 2021 GGE recognized the importance of such confidence-building measures, which "can promote stability and help to reduce the risk of misunderstanding, escalation and conflict" and thus foster trust, cooperation, transparency and predictability.[156] A senior-level exchange of views about the implications of cyberspace as a warfighting domain, including the impact on strategic signalling, is warranted.[157] This could entail discussion of risk perceptions around the cyber–nuclear nexus, including the specification of the types of activities that States see as destabilizing, and clarification of intended missions linked to cyber capabilities of concern.[158] Naturally, greater transparency around doctrines—both cyber and nuclear—and on the cyber-related conditions in which States would consider nuclear weapon use would further this endeavour for common understanding.

---

150 V. Giaurov, "The Cyber-Nuclear Security Threat: Managing the Risks", Vienna Center for Disarmament and Non-Proliferation, 2017, p. 14, http://large.stanford.edu/courses/2017/ph241/bunner2/docs/giaurov_2017.pdf; see also P. Mohan, "Ensuring Cyber Security in India's Nuclear Systems", ORF Issue Brief, no. 412, 2020, https://www.orfonline.org/wp-content/uploads/2020/10/ORF_Issue-Brief_412_Cyber-Nuclear-Security.pdf.

151 T. Hitchens, "NC3 Next Will Improve Nuke Cyber Defenses, Says STRATCOM", Breaking Defense, 5 January 2021, https://breakingdefense.com/2021/01/nc3-next-will-improve-nuke-cyber-defenses-says-stratcom.

152 General Assembly, "Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", UN document A/76/135, 14 July 2021; General Assembly, "Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security", UN document A/AC.290/2021/CRP.2, 10 March 2021.

153 A. Futter, "Managing the Cyber-Nuclear Nexus", European Leadership Network Policy Brief, 2019, https://www.europeanleadershipnetwork.org/wp-content/uploads/2019/07/26072019-Managing-the-Cyber-Nuclear-Nexus.pdf; B. Buchanan and F.S. Cunningham, "Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis", *Texas National Security Review*, vol. 3, no. 4, 2020, http://dx.doi.org/10.26153/tsw/10951.

154 P.O. Stoutland and S. Pitts-Kiefer, "Nuclear Weapons in the New Cyber Age", Nuclear Threat Initiative, 2018, https://media.nti.org/documents/Cyber_report_finalsmall.pdf.

155 E. Gartzke and J.R. Lindsay, "Thermonuclear Cyberwar", *Journal of Cybersecurity*, vol. 3, no. 1, 2017, p. 42, https://doi.org/10.1093/cybsec/tyw017.

156 General Assembly, "Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", UN document A/76/135, 14 July 2021, §VI.

157 A. Futter, "Cyber Threats and Nuclear Weapons: New Questions for Command and Control, Security and Strategy", RUSI Occasional Paper, 2016, https://nsarchive.gwu.edu/sites/default/files/documents/3460884/Document-07-Andrew-Futter-Royal-United-Services.pdf.

158 Stefanovich, "Russia's Basic Principles and the Cyber-Nuclear Nexus", European Leadership Network Commentary, 14 July 2020, https://www.europeanleadershipnetwork.org/commentary/russias-basic-principles-and-the-cyber-nuclear-nexus.

Bilateral strategic stability dialogues—and cyber stability-focused dialogues—present natural venues in which nuclear-armed and nuclear-allied States could deepen their engagement on cyber–nuclear risk. The topic also seems to fit in the P5 process, especially as the group of nuclear-weapon States has announced plans to continue discussion on strategic risk reduction into the next review cycle of the NPT.[159] Cyber operations can significantly alter the calculus and time frames of State decision-making, feeding into the kind of risks "caused by misunderstandings and misjudgments" that have been a focus of that venue.[160] At the same time, the conversation on cyber–nuclear risk must expand to include all nuclear-armed States. India, Israel, and Pakistan participate in the United States-initiated Creating an Environment for Nuclear Disarmament (CEND) initiative, which has spotlighted nuclear risk reduction; further development of its agenda can present an opportunity to introduce more focused discussion of cyber risks. Broader discussion on strategic technologies and cyber capabilities, and the development of confidence- and security-building measures in those areas, provides an alternative pathway to address issues of cyber–nuclear risk outside the purview of the NPT.

5.3. ENHANCE RESTRAINT IN CYBERSPACE

As more States perceive cyberspace as an operational domain, they should consider incorporating cyber capabilities into the framework that specifies proper conduct of military operations. This includes the conflict-prevention and -management toolkit that stems from the Cold War.[161] Bilateral agreements on the Prevention of Incidents on and over the High Seas and on the Prevention of Dangerous Military Activities establish rules, prohibit actions, and elaborate on operational procedures for the militaries for both parties, helping to address behaviours that could otherwise be perceived as provocative. Notably, several agreements of this kind have recently been updated in accordance with increased air and maritime activity.[162] States should examine the viability of extending provisions on lasers to include other non-kinetic capabilities, such as cyber operations, especially in the context of communication and radar systems. Political declarations or memorandums of understanding (of a voluntary and non-binding nature) could constitute a stepping stone towards formal agreements on rules of conduct.

As cyber military exercises (including joint exercises) become regular fixtures on the calendar, States may also want to consider them as they do other large-scale military activities. Bilateral cyber 'hotlines' established by the United States with both the Russian Federation and China are intended to provide advanced warning on such activities.[163] But States could also pursue more comprehensive agreements that include annual exchanges of calendars of these activities, notification and information-exchange regarding particulars of individual exercises, and established procedures for external observation and consultations around such exercises.[164] Even public

---

159 A. Liddle, "Disarmament Blog: The P5 Meet in London", British Foreign, Commonwealth and Development Office, 21 February 2020, https://blogs.fcdo.gov.uk/aidanliddle/2020/02/21/disarmament-blog-the-p5-meet-in-london.

160 Ministry of Foreign Affairs of the People's Republic of China, "Five Nuclear-Weapon States Hold a Formal Conference in Beijing", January 30 2019, https://www.fmprc.gov.cn/mfa_eng/wjbxw/t1634793.shtml.

161 See J. Nye, Jr., "Nuclear Lessons for Cyber Security?", *Strategic Studies Quarterly*, vol. 5, no. 4, 2011, https://www.jstor.org/stable/26270533.

162 See T. Nilsen, "Norway & Russia Update Agreement to Avoid Dangerous Aircraft, Warship Encounters", *The Barents Observer*, 7 June 2021, https://thebarentsobserver.com/en/security/2021/06/norway-and-russia-update-agreement-avoid-dangerous-encounter-between-aircraft-and; "Russia, UK to Update Agreement on Prevention of Incidents at Sea", TASS Russian News Agency, 14 August 2017, https://tass.com/politics/960250.

163 S.E. Miller, "Nuclear Hotlines: Origins, Evolution, Applications", *Journal for Peace and Nuclear Disarmament*, vol. 4, sup. 1, 2021, https://doi.org/10.1080/25751654.2021.1903763.

164 P. Meyer, "Cyber-Security through Arms Control: An Approach to International Cooperation", *The RUSI Journal*, vol. 156, no. 2, 2011, https://doi.org/10.1080/03071847.2011.576471.

notification about the execution of such exercises, especially offensive operations, could help confidence by demonstrating to the adversary a State's control over its capabilities.[165] Reminiscent of developments in confidence- and security-building measures during the Cold War, this kind of transparency could eventually build towards an overarching framework, along the lines of the Conventional Forces in Europe Treaty or the OSCE Vienna Document. Regardless, any information-exchange around these exercises can reinforce national-level efforts to strengthen cybersecurity around systems of significance and serve to address concerns about cyber capabilities.

Political agreements provide another means of signalling restraint. For instance, in 2015 the United States and China pledged not to "conduct or knowingly support cyber-enabled theft of intellectual property" against one another, and committed to cooperating on investigating cybercrimes, including with the establishment of a high-level joint dialogue mechanism.[166] China followed up with a similar agreement with the United Kingdom.[167] While recent events and accusations call into question the degree to which those States abide by their provisions, these agreements can still help to provide broad contours for a parallel agreement on cyber–nuclear interactions.[168] As mentioned, US officials reportedly considered the prospect of an agreement with the Russian Federation to place NC3 'off limits' from cyber operations. Experts have examined the logistics of implementing this in the United States–China context, such as formulating generic descriptions of core components, exchanging lists of relevant aspects, and establishing notification systems should incidents occur.[169] The India–Pakistan Agreement on the Prohibition of Attack against Nuclear Installations and Facilities provides a model, in that the language referring to "destruction or damage" lends itself to the inclusion of cyber operations as well.[170] Pledges of individual or mutual cyber restraint among nuclear-armed and nuclear-allied States could also focus on particular assets, for instance early-warning or strategic submarine communications systems. There is some precedent: agreements on non-interference with critical infrastructure would build off a norm (13f) established by the 2015 GGE and reaffirmed in 2021.[171] The provision of reassurance that any decisions to conduct such operations would take place at the highest levels of government (a 'launch authority' parallel) could further underscore their severity and limit their consideration.[172]

---

165 E.D. Borghard and S.W. Lonergan, "Confidence Building Measures for the Cyber Domain", *Strategic Studies Quarterly*, vol. 12, no. 3, 2018, https://www.jstor.org/stable/10.2307/26481908.

166 The White House, "Fact Sheet: President Xi Jinping's State Visit to the United States", 25 September 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

167 A. Segal, "The U.S.–China Cyber Espionage Deal One Year Later", Council on Foreign Relations Blog, 28 September 2016, https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later.

168 See "U.S. Accuses China of Violating Bilateral Anti-Hacking Deal", *Reuters*, 9 November 2018, https://www.reuters.com/article/us-usa-china-cyber-idUSKCN1NE02E; E. White and C. Shepherd, "Cyber Hits Back at US-Led Accusations over Cyber Attacks", *Financial Times*, 20 July 2021, https://www.ft.com/content/fe589e37-2f85-428e-a0ef-cbb5a5211157.

169 A. Levite et al., "China–US Cyber-Nuclear C3 Stability", Carnegie Endowment for International Peace, 2021, https://carnegieendowment.org/files/Levite_et_all_C3_Stability.pdf.

170 Agreement on the Prohibition of Attack against Nuclear Installations and Facilities, 31 December 1988, https://fas.org/nuke/guide/india/doctrine/nucl.htm.

171 General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", UN Document A/70/174, 22 July 2015. Some argue that cyberattacks on critical infrastructure would violate international legal principles of sovereignty and non-intervention; see H. Moynihan, "The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention", Chatham House, 2019, https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf.

172 J. Acton, "Cyber Warfare & Inadvertent Escalation", *Daedalus*, vol. 149, no. 2, 2020, https://direct.mit.edu/daed/article/149/2/133/27317/Cyber-Warfare-amp-Inadvertent-Escalation.

5.4. CONCLUSION

This section discusses a variety of options for States to enhance common understandings around cyber–nuclear risks, threats, and vulnerabilities. It outlines strategies to reduce the likelihood of unintended cyber–nuclear interactions that can drive escalatory risk scenarios. Progress in these areas will contribute to a normative framework around cyber behaviours as it pertains to nuclear weapons systems, which in turn could facilitate more far-reaching risk reduction measures. Some argue that de-alerting could help to ensure that decisions are not "made in haste after a false warning" linked to cyber interference;[173] common understandings of cyber risk can provide impetus to address the high alert status of some deployed nuclear weapons.[174] Others note that future arms control and disarmament agreements will have to account for 'emerging' and 'disruptive' technologies; incorporating cyber capabilities into discussions around these may propel innovation in those agreements and reinvigorate the endeavour.[175] Of course, the complexities and risks associated with cyber–nuclear interactions underline that the ultimate risk reduction measure will remain complete nuclear disarmament. In the foreseeable future, however, it seems likely that such interactions will continue to take place. Minimizing them and mitigating their effects will help to lessen escalatory pathways, reducing the risk of nuclear weapon use.

---

173 P.O. Stoutland and S. Pitts-Kiefer, "Nuclear Weapons in the New Cyber Age", Nuclear Threat Initiative, 2018, p. 23, https://media.nti.org/documents/Cyber_report_finalsmall.pdf.

174 M.V. Ramana and M. Kurando, "Cyberattacks on Russia—the Nation with the Most Nuclear Weapons—Pose a Global Threat", *Bulletin of the Atomic Scientists*, vol. 75, no. 1, 2019, https://doi.org/10.1080/00963402.2019.1556001.

175 A. Futter, "Managing the Cyber-Nuclear Nexus", European Leadership Network Policy Brief, 2019, https://www.europeanleadershipnetwork.org/wp-content/uploads/2019/07/26072019-Managing-the-Cyber-Nuclear-Nexus.pdf.

APPENDIX: CYBER AND NUCLEAR-ADJACENT INTERACTIONS

There is a category of cases that concern the apparent use of cyber operations targeting activities suspected to be linked to the development of nuclear weapons and related materials. Some of these cases involved critical national infrastructure (specifically nuclear facilities). This annex outlines three prominent cases—including a State possessing nuclear weapons—of what might be considered cyber and nuclear-adjacent interactions. While it is difficult to extrapolate from the perspective of escalation risks, these cases offer insight as to how cyber operations could be used to counter perceived nuclear weapons threats.

TARGET: THE DAIR ALZOUR SITE IN THE SYRIAN ARAB REPUBLIC (2007)

A joint cyber and conventional strike took place in 2007 on the Dair Alzour site in the Syrian desert suspected to be housing a nuclear reactor. The cyber and information warfare component allegedly targeted Syrian air defence, allowing a squadron of aircraft to enter Syrian airspace, conduct a raid, and exit without being detected. Two hypotheses as to the nature of the operation have emerged. The Israel Defense Forces—which in 2018 took responsibility for destroying the reactor—was believed to either 1) employ methods such as jamming in combination with network infiltration capabilities to disable air defence, or 2) take advantage of a 'back door' embedded in the air defence system to render it useless.[1]

Israeli intelligence suggested at the time that a reactor, modelled on the Yongbyon gas-cooled graphite-moderated reactor, was being constructed on site and would be capable of producing weapons-grade plutonium; it was estimated to become operational within the year.[2] As such, Israel saw it as a clandestine nuclear site, with weapons purposes.[3] Statements from Israeli government and military officials have framed the operation as pre-emptive, to "deter hostile countries and organizations" from "developing abilities that threaten the existence of the state of Israel".[4] Former Prime Minister Ehud Barak described the successful elimination of "an actual existential threat to Israel".[5]

TARGET: THE NATANZ FUEL ENRICHMENT PLANT IN THE ISLAMIC REPUBLIC OF IRAN (2009)

First reported in June 2010, the Stuxnet 1.001 malware was a worm active in 2009 and 2010 (and was believed to have been in development since 2006).[6] It reportedly was designed to damage centrifuges at the Natanz fuel enrichment plant and slow the fissile material production capabilities of the Islamic Republic of Iran; the steam turbine at the Bushehr nuclear power plant may have been an additional target.[7] Stuxnet manipulated specific logic controllers to change the frequency of motor operations, causing damage over prolonged periods. It also targeted centrifuges, turbines and other hardware, intercepted sensor data that may have indicated malfunctions, and inserted false input signals to evade damage detection from the control room.[8] By November 2009, Stuxnet was believed to have taken a fifth of the plant's production capacity offline.[9]

Stuxnet took effect against a backdrop of Iranian enrichment activity, which came despite criticism from the IAEA Board of Governors and Security Council resolutions calling for this activity to cease;[10] there were concerns that Tehran was moving towards a

---

1 D. Horschig, "Cyber-Weapons in Nuclear Counter-Proliferation", *Defense & Security Analysis*, vol. 36, no. 3, 2020, p. 359, https://doi.org/10.1080/14751798.2020.1790811; T. Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, vol. 35, no. 1, https://doi.org/10.1080/01402390.2011.608939.

2 J.A. Gross, "Ending a Decade of Silence, Israel Confirms it Blew up Assad's Nuclear Reactor", *The Times of Israel*, 21 March 2018, https://www.timesofisrael.com/ending-a-decade-of-silence-israel-reveals-it-blew-up-assads-nuclear-reactor.

3 Ibid.

4 Israel Defense Forces, "Lt. Gen. Gadi Eisenkot Speaks on the Syrian Nuclear Facility Attack", 21 March 2018, https://www.idf.il/en/minisites/press-releases/lt-gen-gadi-eisenkot-speaks-on-the-syrian-nuclear-facility-attack/.

5 J.A. Gross, "Ending a Decade of Silence, Israel Confirms it Blew up Assad's Nuclear Reactor", *The Times of Israel*, 21 March 2018, https://www.timesofisrael.com/ending-a-decade-of-silence-israel-reveals-it-blew-up-assads-nuclear-reactor.

6 The Stuxnet worm was first identified by Belorussian security firm VirusBlokAda on 17 June 2010; see the original report: VirusBlokAda, "Rootkit.TmpHider", 17 June 2010, https://anti-virus.by/en/tempo.shtml.

7 T. Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, vol. 35, no. 1, 2011, p. 18, https://doi.org/10.1080/01402390.2011.608939.

8 Ibid, p. 19.

9 D. Horschig, "Cyber-Weapons in Nuclear Counter-Proliferation", *Defense & Security Analysis*, vol. 36, no. 3, 2020, p. 360, https://doi.org/10.1080/14751798.2020.1790811.

10 Security Council resolutions 1737 (2006), 1747 (2007), 1803 (2008) and 1835 (2008).

11 US Mission to International Organizations in Vienna, "U.S. Statement on Iran IAEA Board of Governors Meeting September 7-11, 2009", 9 September 2009, https://vienna.usmission.gov/090909iran.

"dangerous and destabilizing possible breakout capacity".[11] Iranian officials have suggested that Stuxnet was a joint United States–Israeli effort; neither State has claimed responsibility.[12] Israeli Prime Minister Ehud Olmert reportedly unsuccessfully asked for the United States to green light a strike on Iranian nuclear facilities in 2008.[13] The United States under President Barack Obama expressed an intent in 2010 of "reversing the nuclear ambitions" of the Islamic Republic of Iran.[14] Regardless of origin, Stuxnet was costly beyond the immediacy of physical damage: it introduced economic costs by forcing the early replacement of centrifuges, and had demoralizing effects for Iranian scientists.[15]

TARGET: MISSILE LAUNCHES IN THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA (2016)

In 2017, the New York Times reported on a US cyber campaign to sabotage missile launches by the Democratic People's Republic of Korea, with interference allegedly contributing to the failure of 88 per cent of Musudan (Hwasong-15) tests.[16] Little is known about the operation, and the United States has not claimed responsibility. However, the report tied a series of intermediate-range ballistic missile test failures to an integrated air and missile defence programme first discussed in a US Joint Chiefs of Staff report. That 2013 report envisaged the use of cyber and other non-kinetic capabilities; while not indicating potential targets, it included an illustrative map featuring a missile of the Democratic People's Republic of Korea.[17] The programme is also discussed in a 2014 memorandum to the US Secretary of Defense and in 2016 testimony before a US House of Representatives Committee, with its intent being to "deter an adversary from employing their aircraft and missile capabilities, and failing that, to prevent an adversary from effectively employing them".[18]

The ballistic missile programme of the Democratic People's Republic of Korea has long been intimately linked to its nuclear weapons programme. The United States referenced these together in warning statements issued to Pyongyang following past missile tests, in which it suggested "swift credible action" and heavy consequences for further testing; President Obama described both programmes as a "threat to U.S. national security and to international peace and security".[19] In intelligence circles, there was concern as early as 2013 that the Democratic People's Republic of Korea had miniaturized its capabilities for delivery by ballistic missile.[20] Regardless, the perceived threat from such missile launches was clear, and the series of failures in 2016—whether from 'left of launch' operations or not—constituted heavy time and resource costs.

---

12 J. Harte, "Retired U.S. General Pleads Guilty to Lying to FBI in 'Stuxnet' Leak Case", *Reuters*, 17 October 2016, https://www.reuters.com/article/us-usa-iran-cyber-idUSKBN12H25M; M.A. Kamiński, "Operation 'Olympic Games.' Cyber-Sabotage as a Tool of American Intelligence Aimed at Countering the Development of Iran's Nuclear Programme", *Security and Defence Quarterly*, vol. 29, no. 2, 2020, https://doi.org/10.35467/sdq/121974.

13 J. Steele, "Israel Asked US for Green Light to Bomb Nuclear Sites in Iran", *The Guardian*, 25 September 2008, https://www.theguardian.com/world/2008/sep/25/iran.israelandthepalestinians1; D.E. Sanger, "U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site", *The New York Times*, 10 January 2009, https://www.nytimes.com/2009/01/11/washington/11iran.html.

14 US Department of Defense, "Nuclear Posture Review Report", 2010, p. 9, https://dod.defense.gov/Portals/1/features/defenseReviews/NPR/2010_Nuclear_Posture_Review_Report.pdf.

15 This notion was suggested by German researcher Ralph Langner, who first identified the target of Stuxnet. See P.W. Singer, "Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons", *Case Western Reserve Journal of International Law*, vol. 47, no. 1, 2015, https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1009&context=jil; "Better than Bunker Busters: The Virtual Chinese Water Torture", Langner, 15 November 2010, https://www.langner.com/2010/11/better-than-bunker-busters-the-virtual-chinese-water-torture.

16 D.E. Sanger and W.J. Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles", *The New York Times*, 4 March 2017, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html.

17 Ibid.; Joint Chiefs of Staff, "Joint Integrated Air and Missile Defense: Vision 2020", 5 December 2013, p.1, https://www.jcs.mil/Portals/36/Documents/Publications/JointIAMDVision2020.pdf.

18 J.W. Greenert and R. T. Odierno, "Memorandum for the Secretary of Defense- Subject: Adjusting the Ballistic Missile Defense Strategy", 5 November 2014 https://news.usni.org/2015/03/19/document-army-navy-memo-on-need-for-ballistic-missile-defense-strategy; US Government Publishing Office, "Subcommittee on Strategic Forces Hearing on the Missile Defeat Posture and Strategy of the United States", 2016, p. 100 (testimony of Rear Admiral Edward Cashman), https://www.govinfo.gov/content/pkg/CHRG-114hhrg20080/pdf/CHRG-114hhrg20080.pdf.

19 The White House, "2015 United States–Republic of Korea Joint Statement on North Korea", 16 October 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/10/16/united-states-republic-korea-joint-statement-north-korea; The White House, "Statement by the President on North Korean Announcement of Nuclear Test", 12 February 3013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/statement-president-north-korean-announcement-nuclear-test; The White House, "Statement by the President on North Korea's Nuclear Test", 9 September 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/09/09/statement-president-north-koreas-nuclear-test.

20 D. Alexander and M. Hosenball, "UPDATE 5-Pentagon Report on NKorea Nuclear Capability Stirs Worry, Doubts", *Reuters*, 12 April 2013, https://www.reuters.com/article/korea-north-usa/update-5-pentagon-report-on-nkorea-nuclear-capabilities-stirs-worry-doubts-idUSL2N0CY26920130412; Testimony on the US Defense Intelligence Agency report was downplayed, however, by the Director of National Intelligence: Office of the Director of National Intelligence, "DNI Statement on North Korea's Nuclear Capability", 11 April 2013, https://www.odni.gov/index.php/newsroom/press-releases/press-releases-2013/item/839-dni-statement-on-north-korea-s-nuclear-capability; Even today there remains some debate about whether this development has yet taken place, though some experts have argued this has been the case for years. H. M. Kristensen and R. S. Norris, "North Korean Nuclear Capabilities, 2018", *Bulletin of the Atomic Scientists*, vol. 74, special issue, 2018, https://doi.org/10.1080/00963402.2017.1413062.

THE CYBER-NUCLEAR NEXUS:
Interactions and Risks

This publication is the second in a series that profiles different 'friction points' among nuclear armed and nuclear-allied States, examining issues of contention in their relations that can spark potential conflict and nuclear escalation. It traces trends both in the development of cyber capabilities and the digitalization of nuclear weapons systems that could drive more frequent interactions at the cyber–nuclear nexus. It considers how these interactions, direct and indirect, might impact on escalatory risk scenarios—drawing upon State doctrines, postures, and capabilities in the nuclear and cyber spheres. It then outlines a series of recommendations for States both to minimize cyber–nuclear interactions and to mitigate their effects when they do occur. As part of UNIDIR's ongoing research on nuclear risk reduction, this paper is intended to feed into the dialogue on taking forward risk reduction—and on the development of practical and feasible measures that can help to close pathways to use.

SELECTED UNIDIR PAPERS ON NUCLEAR RISK REDUCTION

Borrie, John, Caughley, Tim, and Wan, Wilfred [eds]. 2017. "Understanding Nuclear Weapons Risks."

Wan, Wilfred [ed]. 2020. "Nuclear Risk Reduction: Closing Pathways to Use."

Panda, Ankit. 2020. On 'Great Power Competition' (Nuclear Risk Reduction Policy Brief No. 1).

Borrie, John. 2020. Strategic Technologies (Nuclear Risk Reduction Policy Brief No. 2).

Kühn, Ulrich 2020. Perceptions in the Euro-Atlantic (Nuclear Risk Reduction Policy Brief No. 3).

Ogilvie-White, Tanya. 2020. The DPRK Nuclear Programme (Nuclear Risk Reduction Policy Brief No. 4).

Wan, Wilfred. 2021. Nuclear Risk Reduction: Engaging the non-NPT Nuclear-Armed States (Nuclear Risk Reduction Policy Brief No. 5).

Wan, Wilfred. 2021. Nuclear Escalation Strategies and Perceptions: The United States, The Russian Federation, and China. Nuclear Risk Reduction, Friction Points Series Paper 1.