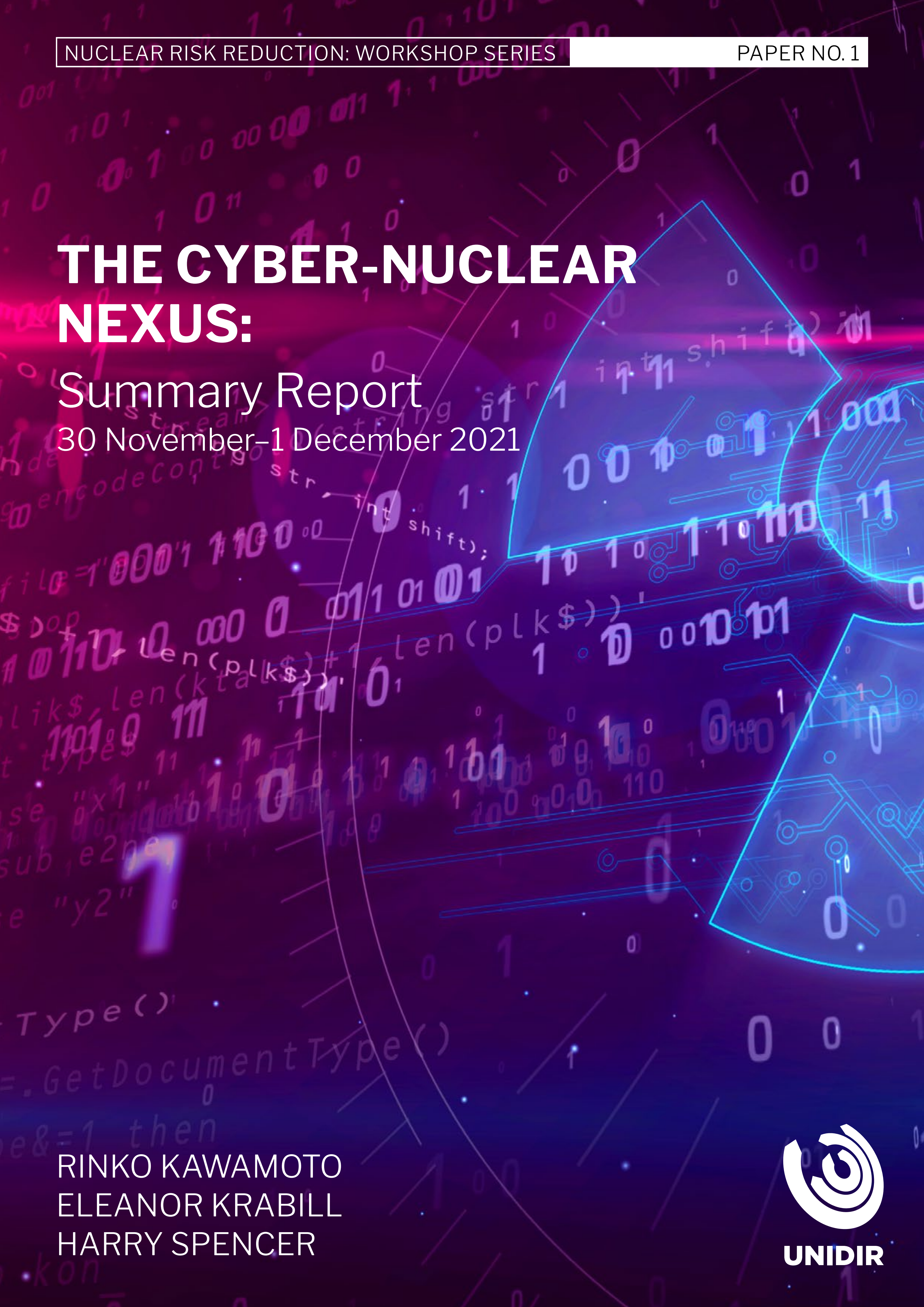
NUCLEAR RISK REDUCTION: WORKSHOP SERIES PAPER NO. 1



THE CYBER-NUCLEAR NEXUS:

Summary Report

30 November–1 December 2021

RINKO KAWAMOTO
ELEANOR KRABILL
HARRY SPENCER

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 would also like to thank the University of Leicester and Yale–NUS College for their partnership in the organization of this workshop, specifically Andrew Futter and Rohan Mukherjee, and recognize the support of the European Research Council.

UNIDIR's María Garzón Maceda, Alphonce Masinde Wanjala, James Revill, and Wilfred Wan all provided invaluable advice, support, and assistance on this paper. The authors would also like to acknowledge Alexi Drew, Senior Analyst at RAND Europe, and Jinghua Lyu, North East Asia Programme Director at the Centre for Humanitarian Dialogue, for their inputs, and to thank all of the participants at the workshop for their contributions.

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 the publication are the sole responsibility of the individual authors. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

CITATION

Kawamoto, Rinko, Eleanor Krabill, and Harry Spencer. 2022. "Nuclear Risk Reduction Workshop Series: The Cyber–Nuclear Nexus, Summary Report", UNIDIR, Geneva: Switzerland. https://doi.org/10.37559/WMD/22/NRR/01.

© Cover: www.shuttterstock.com/Skorzewiak

TABLE OF CONTENTS

ABOUT THE AUTHORS

Rinko Kawamoto is currently a second-year undergraduate studying global affairs and environmental studies at Yale–NUS College, Singapore. Her research interests include nuclear non-proliferation, environmental policy, and their intersections. Previously she has served as a student researcher on intersectionality and social change, as well as a public relations fellow at Justice Without Borders.

Eleanor Krabill was with UNIDIR's Graduate Professional Programme from June 2021 to January 2022. She has completed an MA in non-proliferation and terrorism studies at the Middlebury Institute of International Studies at Monterey, United States. Her research focuses on nuclear non-proliferation, nuclear security, and disarmament. She has 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.

Harry Spencer is a postgraduate MA scholar studying international relations at the University of Birmingham, United Kingdom, having gained a bachelor's degree in politics and international relations from the University of Leicester. His research focuses on nuclear strategic theory and advanced military technologies. His recent work includes a newly published study with British Pugwash into the operational effectiveness of the current generation of missile defence systems and the introduction of hypersonic weapons.

INTRODUCTION

In recent years, there has been increased concern among the policymaking and expert communities that the entangled interaction of nuclear and non-nuclear capabilities may prompt escalation to nuclear weapon use. Risk at the cyber–nuclear nexus has become a particular focal point – as nuclear systems are being increasingly digitalized and as the cyber domain is incorporated into military operations.

The identification of feasible, effective measures to reduce risks posed by interactions – direct and indirect – between cyber operations and nuclear capabilities first requires an understanding of those risks. It is important that policymakers and experts alike explore potential escalation pathways linked to the cyber–nuclear nexus.

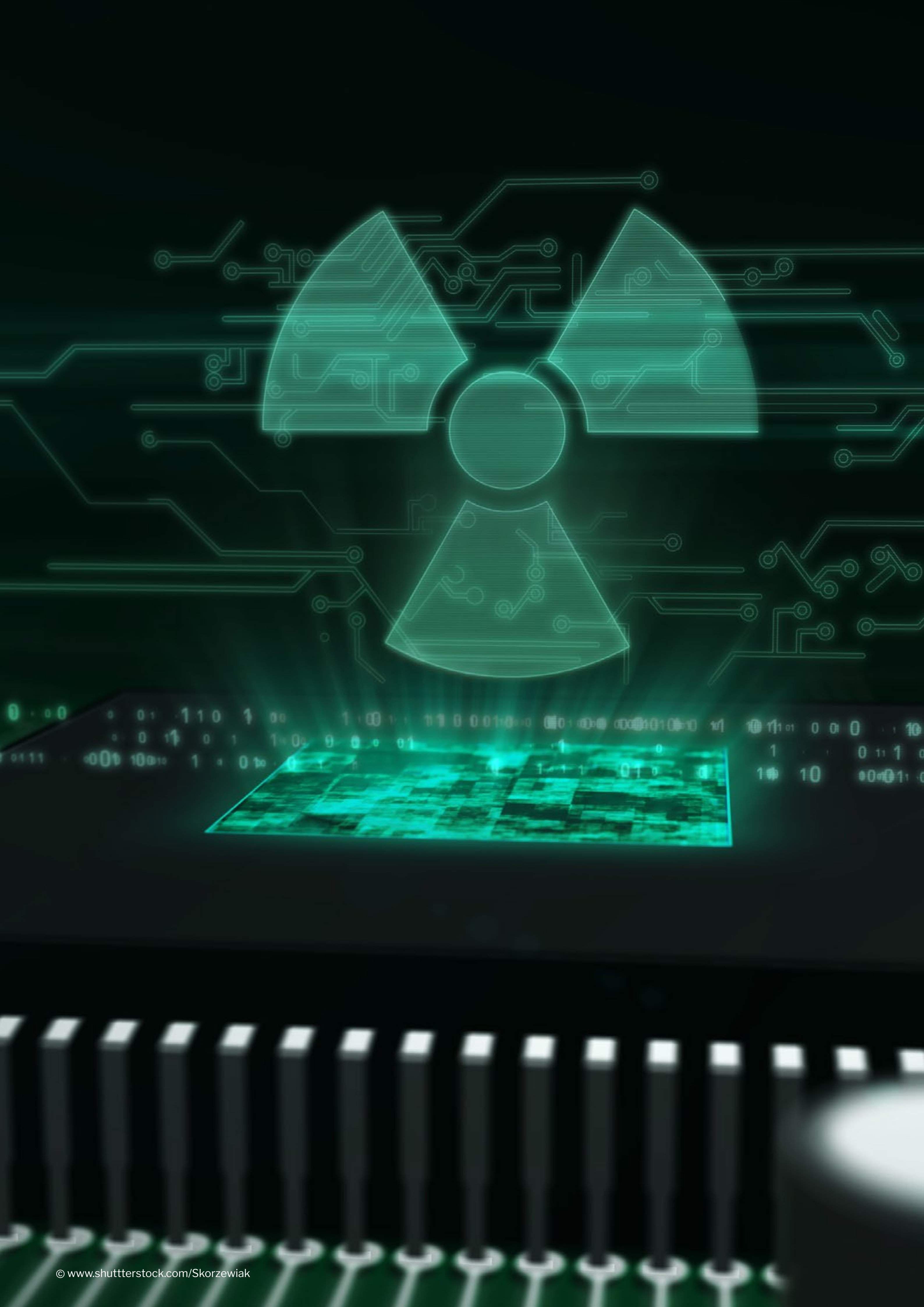
To facilitate engagement with these topics, UNIDIR convened a virtual workshop on the cyber–nuclear nexus, with partners from the University of Leicester (United Kingdom) and Yale–NUS College (Singapore).

The two-day workshop brought together members of the diplomatic community and experts in nuclear and cyber policy to jointly explore the cyber–nuclear nexus, identify areas of concern, and consider priorities and potential policy options to reduce risk.

A number of experts were invited to present on key themes ahead of interactive discussions among all participants. Practitioners and experts also engaged in focused discussions to facilitate a more active exchange of opinions and views.

To encourage open discussion, the meeting was held under the Chatham House Rule. As such, "participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed". The discussion over the course of the workshop is summarized in this document.

© https://commons.wikimedia.org



© www.shutterstock.com/Skorzewiak

SESSION 1: The state of cyber affairs

Cyberspace has increasingly become a focus of attention in policy discourse. As an inherently cross-domain field, cyber affairs are intertwined with nuclear and conventional capabilities, as well as non-military fields that have potential bearing on international peace and security. For instance, the WannaCry ransomware attacks in 2017, which targeted Microsoft Windows XP servers, affected components of several states' critical national infrastructure, including the United Kingdom's healthcare system. Operations in the cyber domain have advanced considerably as a function of technological developments; in addition, because of low barriers to entry, non-state actors, including private industry and criminal organizations, play an increasingly important role in the field.

As cyber is a fairly dynamic domain, substantial understanding of cyberspace and cybersecurity issues is still lacking. Experts and attendees during this first session of the workshop considered the state of play, including features of the cyber domain, how cyber operations may be deployed, and how those operations may have an impact on concepts of strategic stability and predictability.

CROSS-DOMAIN DETERRENCE

In recent years, there have been considerable developments in the deterrence strategies of states, fuelled in part by the rapid enhancement of cyber capabilities. Cross-domain cyber deterrence can take two distinct forms: the employment of capabilities from other domains to deter cyber operations and the use of cyber operations as a tool to deter attacks from other domains.

The first form mitigates the unpredictability of cyberspace. However, this type of cross-domain deterrence also faces challenges as cyber operations continue to proliferate. This is because deterrence by denial – that is, deterring an action by making it infeasible or unlikely to succeed – is difficult in the cyber realm, while deterrence by punishment encounters difficulties in attribution and the issuance of proportionate responses.

The second form of cross-domain cyber deterrence can be employed by military forces engaged in information, kinetic or psychological warfare to deter attacks in other domains; this form of deterrence is closer to coercion as it employs cyber advantages as offensive means. Notably, this form of deterrence is complicated by the intrinsic value of secrecy in cyber operations.

Both forms of cross-domain cyber deterrence can result in instability and horizontal expansion of tensions across other domains, mirroring the stability–instability paradox of the Cold War.[1] This is especially the case because of questions about intent in the cyber domain. The "cybersecurity dilemma" suggests that, when faced with a cyber intrusion, it is difficult for actors to readily and accurately determine if its purpose is espionage or sabotage.[2] Furthermore, the line between espionage and sabotage is often blurred, as espionage can be used as reconnaissance activity to collect information for subsequent sabotage.

Various factors influence state behaviour and thus escalation patterns. They contribute to frequent perception gaps about individual cyber operations, as well as on cyber capabilities more broadly. In this session, at least one participant proposed further that a state's reaction to an operation does not depend solely on its calculations of threat perception but also on national security culture. Historical factors were also noted as being relevant here.

In practice then, cross-domain deterrence requires state actors to match strategic objectives and means in different scenarios. They must adopt a comprehensive perspective integrating technological development and security concerns, rather than a dichotomous perspective of hardware versus software, or offline versus online security. Participants in this first session noted that avoiding cyber-related escalation is of vital importance.

[1] See, for example, G. Snyder, The Balance of Power and the Balance of Terror, 1965.

[2] For a detailed exploration of the cybersecurity dilemma, see B. Buchanan, The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations, 2017, https://doi.org/10.1093/acprof:oso/9780190665012.001.0001.

ATTRIBUTION

In a domain that lacks formal, codified frameworks or norms, attribution can allow actors to identify, establish, and regulate compliance with informal standards of behaviour. It has become apparent that attribution in cyberspace is technically possible: often, reverse-engineering malicious code allows analysts to trace the source of an operation. Tool sets, time stamps, languages used, and even IP addresses within the code itself can all be used to attribute cyber operations. These attributions may not always be made with absolute certainty, and their veracity may be questioned.

The question of attribution is instead often a political one: a state may not be willing to attribute publicly, as this action can risk revealing the extent of its cyber capabilities and intelligence-collection activities and compromise its own operations. This may help to explain different state policies on attribution. For instance, France generally does not make public attributions while the United States does so frequently. Further, information on incidents and attribution can often be released a long time after the incident; these processes are also commonly carried out by private industry. Different capabilities and policies on attribution can result in an imbalance in public information.

While many workshop participants observed that an agreement on binding rules surrounding cyber operations will be difficult to reach, some suggested a shared interest in the creation of an independent attribution platform. Some participants raised concerns that any such joint attribution will only be achievable in the long term and suggested the development of standards for attribution as a short- to medium-term solution and as a means for cyberspace stability. More research is necessary in this domain.

MOVING FORWARD

Many participants argued that a first step to stability in the cyber realm is to improve mutual understanding, which will require more knowledge and research. The international community is still identifying relevant issues and gaining a clearer understanding of the cyber domain.

Without a clearly defined set of threats, for example, it is difficult to develop robust policies. More discourse on what states seek to police in cyberspace will bring some stability to this domain. In addition, many critical terms, including attribution, still lack clear, agreed definitions. State postures regarding red lines are also still largely ambiguous. Clarification of what each state deems an unacceptable attack could have beneficial results. One participant called for more transparent state doctrines and policies regarding offensive cyber operations, such as the conditions under which it would rely on them. In the meantime, as regulations and norms develop at both the national and international levels, securing stability in the short term is paramount.

© https://commons.wikimedia.org

SESSION 2: Nuclear points of vulnerability

The second session of the workshop invited participants to explore potential points of cyber-related nuclear vulnerability. These have increased as a function of the modernization programmes undertaken by all nuclear-armed states that entail the increased computerization and digitalization of nuclear weapons and related capabilities.

A number of targets of possible disruption through cyber operations have potential implications for escalation to nuclear weapon use. For instance, there exists the possibility of direct interference with computer-based nuclear command, control, and communications (NC3) systems, or of gaining access to sensitive data on nuclear weapon systems, designs, and processes. The vastness of modern nuclear weapon enterprises also suggests that supply chains could be vulnerable to similar intrusion. Targets can also include the broader information ecosystem within which nuclear weapon decision-making takes place and, related, elements connected to the human operators of those systems.

VULNERABILITIES AND DEPENDENCIES

Several participants outlined the importance of clarifying the vulnerabilities of systems and overlapping asset dependencies. The reliance of NC3 on space-based satellite communications was cited as one area of particular concern. Cyber operations on such multi-use assets can risk escalation in crisis situations, especially given the aforementioned challenges linked to attribution and establishing intent.

Concerns over particular vulnerabilities and assets vary across actors. Accordingly, several participants emphasized the potential utility of dialogue in order to explore key assumptions about nuclear vulnerability (and their transferability across states). One participant noted that risk reduction requires a degree of transparency and dialogue that is currently absent. Others suggested there was value in diagnosing and drawing attention to existing issues and risks prior to taking other actions. This can help to create common ground that feeds into multilateral or bilateral agreements.

ENHANCING AWARENESS

Participants expressed concern that the relevant ideas and findings of the expert community were not being considered in the policymaking domain. It was important to challenge overconfidence or complacency in the cyber survivability of existing nuclear systems by governments and independent actors. Additionally, participants underlined the need for increased engagement across communities to identify risks that may otherwise not be considered. Some noted the specific issue of supply chain transparency (as a prerequisite to preventing supply chain intrusions), and the interrelated need for internal identification of nuclear-relevant software and systems developed and operated by non-governmental actors and entities.

Another concern raised by participants was the lack of governmental regulatory oversight on the cyber-awareness and vigilance of entities contracted with developing or maintaining sensitive information and communication technologies (ICTs). This is especially relevant as some participants noted that interconnected military and civil cyber spaces can create unique avenues of attack. As a result, operations carried out in public spaces may have significant repercussions for militaries or governments. In addition to “classic” threats posed to military cyber spaces then, both state and non-state actors may capitalize on disrupted public information channels – through hybrid tactics employing cyber capabilities, such as disinformation campaigns on social media networks – to further complicate a crisis.

MOVING FORWARD

A range of directions and policy options were expressed as means to address the vulnerabilities discussed in the session. Several participants coalesced on the need to manifest "epistemic communities" that would operate to create and inform discussions on issues within and beyond the cyber–nuclear nexus. Indeed, the issues at play are not strictly linked to the nuclear policy community; addressing them will require the assembly of multi-industry platforms and approaches to basic risk awareness, and management to prevent and mitigate crises and increase resilience.

In considering roll-on effects, including escalation pathways, many suggested the need for an increase in bilateral, plurilateral, and multilateral dialogue to address concerns and broaden understandings on respective national priorities. This could include cyber de-escalation mechanisms between major powers.

© Navy Petty Officer 1st Class Ronald Gutridg

SESSIONS 3 & 4: Cyber–nuclear interactions and risk scenarios

The proliferation of cyber operations and the possibility of cross-domain cyber interactions present a substantial challenge from the context of nuclear risk. In these two sessions (which included breakout groups), workshop participants considered the cyber-related escalatory risk scenarios they deemed most concerning. They also discussed perceptions of these risks and considered the possibility that cyber operations could be de-escalatory or stabilizing.

SETTING THE STAGE

It was observed that the identification and – for the most part – understanding of the nuclear capabilities and policies of nuclear-armed states and of their allies are fairly well developed (or purposefully left ambiguous). In contrast, the actors in the cyber domain are less clearly defined. It is also clear that advanced industrial powers are generally the most advanced cyber powers, but the key actors involved in this domain are not as clearly defined and the line between state and non-state actors is often blurred. Furthermore, as discussed in previous sessions, there is an array of entry points and spaces that could be involved in operations in the cyber domain.

TIMING MATTERS

Of great concern is the perceived risk of escalation resulting from misperception or miscalculation. In small group conversations, participants observed that the context in which cyber operations take place will have an impact on perceptions of intent. Activities, including espionage, that may not cause alarm in peacetime may, at times of tension, be perceived as indicators of battlefield preparation. This in turn could prompt significant escalation. Moreover, crisis situations may prompt the misreading of data, again driving escalatory pathways.

Many participants suggested that states should pursue communication channels in the cyber domain to minimize the possibility of misperception or miscalculation, including with the establishment of cyber hotlines. One of the small groups discussed the development of shared definitions, although the group recognized the difficulties with definitions faced in the Open-Ended Working Group (OEWG) process and in the pursuit of a P5 nuclear glossary. Many suggested that it will be broadly important to build state-level understandings of risks and to discuss how activities in cyberspace may be perceived by other actors.

INTENT AND DEGREE

While individual cyber operations are unlikely to reveal intent, mechanisms that make state behaviour in the domain more observable could help reduce the possibility of crisis onset and escalation. On this point, several participants reiterated the relative lack of communication between actors about their cyber capabilities or their cyber red lines. Some suggested that espionage activity in cyberspace is inevitable; accordingly, it is critical for states to build some tolerance for this – delineating the boundaries of “acceptable” behaviours can contribute to trust in a manner that prevents inadvertent escalation.

Complicating risk-mitigation efforts, however, is the fact that there are different perspectives as to what constitutes an offensive cyber capability. More transparent doctrines can help to make such issues easier to navigate. Bilateral engagements could also open up the dialogue, set a precedent, and prompt other states or multilateral bodies to follow suit. Another realistic way forward could be the pursuit of an agreement on transparency among like-minded states. At the same time, as one participant noted, given the challenges of verification, it is critical for states to follow through on the commitments made in multilateral discussions on transparency and other proposed risk-reducing activities. If they do not, they risk undermining the larger endeavour.

A CALL FOR ACTION

Recognizing the distinct nature of the cyber domain, there is a clear need for risk-reduction action. State-level understandings of cyber affairs and related risks must mature. At the international level, states must become more comfortable with discussing their cyber capabilities as means towards establishing stability across domains. However, many participants acknowledged that the best way to reduce risk at the cyber–nuclear nexus would be to reduce nuclear weapon risk overall through the pursuit of nuclear disarmament.

SESSION 5: Risk reduction options

The final session of the workshop was an in-depth exploration of the options for reducing the risk of nuclear weapon use linked to interactions, direct and indirect, between cyber operations and nuclear forces. Participants considered different means to limit potential escalation pathways and scenarios discussed over the course of the two days.

CRISIS PREVENTION AND MANAGEMENT

Participants were optimistic about a role for existing crisis-prevention and -management models as means to limit cyber-related nuclear escalation. This included the revival of the Cold War hotlines that allowed direct communication between political and military leaders across borders. These channels could be used during periods of heightened tension. Some also observed the possibility of new approaches. These include, for instance, the undertaking of mutual resilience-enhancing processes whereby states manage individual vulnerabilities (and the possibility of unintended escalation) by undertaking common measures. These measures can include isolating the networks used to maintain nuclear assets from civilian networks, the development of fail-safe mechanisms or the identification of red lines through dialogue processes. Many suggested the pursuit of these in existing frameworks and channels.

COMMON UNDERSTANDINGS

For many, an essential aspect of future cooperation on cyber–nuclear risks centres on achieving a common baseline of understanding about concerns and vulnerabilities. Scepticism was raised over the extent to which states would be willing to illustrate vulnerabilities to potential adversaries, and at least one participant noted that attempts might be handicapped by security concerns over the survivability of sensitive strategic systems. Still, a dialogue on such issues could be key in reducing risk and avoiding escalation. Some noted that states could find some common ground on measures to restrain malicious non-state actors and on technical oversight agreements on essential NC3 systems. These could provide a foundation for further cooperative discussion.

UNILATERAL RESTRAINT

Opportunities for unilateral restraint in the cyber domain could take a number of forms. These include the voluntary establishment of executive oversight protocols, in which head-of-state authorization would be required to conduct cyber operations against high-level targets, such as NC3-related infrastructure. In addition, states could also more systematically apply transparency and security reviews to relevant systems. More regular tests of the cyber resilience of certain systems, for instance, could identify risks linked to overlapping networks and assets. This could also feed into informed responses not only to vulnerabilities and risks, but also to incidents at the national level.

Dialogue at the bilateral, plurilateral, and multilateral levels can help facilitate and motivate effective unilateral action. Notably, participants observed that such inclusive dialogue should not be limited at the state level, but should instead take place across disciplines and sectors, across state agencies and involving private industry. An all-of-society approach is necessary given the scope of the issue; such a campaign can put further pressure on states to improve their cyber awareness and strengthen their cyber resilience. All of this can contribute to an overall reduction in cyber–nuclear risk.

© www.shutterstock.com/betibup33

CONCLUSIONS AND NEXT STEPS

Addressing risk at the cyber–nuclear nexus will require substantial cooperative effort from states, subject matter experts in the nuclear and cyber fields, and the broader security community alike. The workshop demonstrated the willingness of these communities to engage in dialogue about the unique threats posed by cyber operations to the nuclear domain.

While further efforts are required to gain a clearer understanding of the spectrum of risk at the cyber–nuclear nexus, this initial dialogue showcased significant areas of agreement within the expert and diplomatic communities. Notably, concerns about areas of vulnerability converged around the lack of communication, the absence of common understanding of risks, and differences in risk perception at the cyber–nuclear nexus. In particular, consensus formed around the need for increased transparency.

Identifying effective risk-reduction measures will also necessitate further discussion between relevant actors at the national, bilateral, and multilateral levels. Significant progress may be made through unilateral measures by states (especially from those with more advanced capabilities), or through bilateral arrangements to improve transparency and communication, including through the introduction of crisis hotlines. Over the course of the workshop, many noted the need for broader dialogues on standards for attribution, perceived threats and vulnerabilities, and greater candour about cyber doctrines and objectives; such dialogues will allow states to reach common understandings and facilitate the pursuit of future risk-reduction measures. Further, initiatives that bring together policymakers, subject matter experts, and private sector actors can play an important informative role by providing context, depth of understanding, and insight to discussions of risk that would otherwise be lacking.

While much remains to be done to reduce risk at the cyber–nuclear nexus, the willingness of participants to openly engage with and identify common threats and potential mitigation measures serves as a positive indicator for future risk-reduction efforts. This workshop also demonstrated a significant interest and enthusiasm for further engagement in both the diplomatic and expert communities on the topic. This ought to be encouraged and facilitated through similar initiatives in the near future.

© UN photo/Mark Garten

ANNEX 1: Workshop agenda

All times are CET.

DAY 1: TUESDAY, 30 NOVEMBER 2021

Introduction to the workshop
13:00–13:30
Opening presentation to outline the objectives and structure of the workshop and to set out basic concepts, followed by an interactive discussion on expectations and issues of interest with participants.

SESSION 1: THE STATE OF CYBER AFFAIRS

13:30–14:50
Presenters will explore the state of cyber capabilities and operations. They will consider cyberspace in the context of strategic stability, the possibility of cyber-induced crisis and escalation, and issues of attribution. Topics for the group to discuss may include:

- Concepts of cyber, cross- and multi-domain deterrence
- Use of cyber operations as a force multiplier for conventional capabilities
- Potential physical impact of cyber operations

Comfort break
14:50–15:00

SESSION 2: NUCLEAR POINTS OF VULNERABILITY

15:00–16:20
Presenters will examine the susceptibility of nuclear weapon systems to cyber operations. They will consider the known history of electronic/cyber warfare operations targeting nuclear forces as well as potential cyber-related “red lines”. Topics for the group to discuss may include:

- Critical nuclear “entry points” for cyber operations and ambiguities
- Vulnerability of supply chains linked to nuclear forces
- Left-of-launch and right-of-launch impacts

Closing Day 1
16:20–16:25

DAY 2: WEDNESDAY, 1 DECEMBER 2021

Introduction to Day 2
13:00–13:05
Outlining of plans for breakout session and introduction of small group facilitators.

Session 3: Cyber–nuclear interactions and risk scenarios
13:05–13:45
In small groups, participants will examine risk linked to interactions between cyber and nuclear forces (including nuclear weapons and delivery systems; nuclear command, control and communications; early-warning systems; and nuclear decision-making). Each group will consider different dimensions of risk scenarios, including:

- Potential escalatory or de-escalatory impacts of cyber–nuclear interactions
- Interaction of cyber capabilities with other technologies
- Processes of detection, attribution and potential nuclear response

SESSION 4: DISCUSSION OF RISK SCENARIOS

13:45–14:30
Participants will report on their findings from the small groups and discuss further risk scenarios. These may include cyber operations that do not have an impact on nuclear forces at all but may nevertheless drive consideration of nuclear response.

Comfort break
14:30–14:40

SESSION 5: RISK REDUCTION OPTIONS

14:40–16:20
Presenters will examine measures that fall under the rubric of cyber–nuclear risk reduction. These include means of limiting cyber–nuclear interactions and means of containing the consequences from these. Topics for the group to discuss may include:

- Development of common understandings of cyber–nuclear risk
- Applicability of normative or behavioural frameworks
- Stakeholder engagement, including at the national level and with the private sector

Concluding remarks and next steps
16:20–16:25

NUCLEAR RISK REDUCTION: WORKSHOP SERIES PAPER NO. 1

THE CYBER-NUCLEAR NEXUS:
Summary Report

30 November–1 December 2021

Concern that cross-domain entanglement may prompt nuclear weapon use has grown in recent years. Risk at the cyber–nuclear nexus has become a focal point, particularly as nuclear systems continue to be digitalized and as the cyber domain is increasingly incorporated into military operations. In order to identify and implement effective measures to reduce escalatory risks linked to interactions – both direct and indirect – between cyber and nuclear capabilities, it is important to first foster a common understanding of what those risks are.

To this end, UNIDIR convened a two-day virtual workshop with partners from the University of Leicester and Yale–NUS College. The workshop brought together members of the diplomatic community and experts in nuclear and cyber policy to jointly explore the cyber–nuclear nexus, identify areas of concern, and consider potential options to reduce risk. The discussion over the course of this two-day workshop is summarized in this report.

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.

Wan Wilfred, Andraz Kastelic and Eleanor Krabill. 2021. The Cyber–Nuclear Nexus: Interactions and Risks. Nuclear Risk Reduction, Friction Points Series Paper 2.

UNIDIR