EUROPEAN LEADERSHIP NETWORK

Protecting the Nuclear Non-Proliferation Treaty in turbulent times

Commentary collection: Volume 3
2025 NPT Preparatory Committee

April 2025

These commentaries have been published as part of the ELN's project Protecting the Non-Proliferation Treaty. The project seeks to preserve the multilateral nuclear non-proliferation regime and prevent further erosion of the nuclear taboo and the Nuclear Non-proliferation Treaty (NPT). Bringing together an intergenerational, pan-regional Network of experts, it works to identify pathways to success in the eleventh review cycle, taking a holistic approach to the NPT and its three pillars.

The online versions of these and other commentaries, which often contain links to additional sources and relevant background information, can be found by scanning the QR code below or following this link: https://europeanleadershipnetwork.org/publications/commentaries/.

This project is funded by:

Norwegian Ministry of Foreign Affairs

Contents

The CTBT: A success story and keystone for reinforcing the NPT regime ahead of the next 2026 NPT Review Conference

Eleonora Neri

The Comprehensive Nuclear-Test-Ban Treaty (CTBT) was opened to state signatures 28 years ago and, to this date, has not yet entered into force. On account of this, it has often been deemed a failure; however, on many metrics, the Treaty has nonetheless achieved some notable successes.

The Treaty enjoys near-universal support, with 187 countries having signed and 178 having ratified it, demonstrating widespread global support for the object and purpose of the CTBT. The CTBT has also established a firm and unchallenged norm against nuclear testing.[1] Only India, Pakistan and North Korea have conducted tests since it opened for signatures in 1996. In this century, only one State – North Korea – has breached the norm and tested nuclear weapons. Additionally, the International Monitoring System (IMS) – a key component of the CTBT's unique verification regime – is fully operational, ensuring no nuclear test goes undetected. Beyond its primary role in detecting nuclear explosions, the IMS generates valuable data with broad civil and scientific applications[2], including tsunami warning systems and nuclear emergency response.

In light of this, it is clear that the CTBT represents a global public good that must not be taken for granted, especially amid today's complex geopolitical landscape. We are witnessing rising global anxieties over nuclear threats,[3] including the potential use of nuclear weapons, possible further nuclear tests, and risks of nuclear proliferation with increased stockpiles of enriched uranium. This complexity was further highlighted by the recent de-ratification of the CTBT by the Russian Federation in November 2023. Yet, there has also been renewed momentum toward universalising the CTBT, with nine new ratifications and one additional signature in the past two years, underscoring that countries continue to recognise the CTBT's value.

While the CTBT has already demonstrated significant success, its full potential can only be realised with its formal entry into force. The CTBT has not formally entered force due to a strict entry-into-force provision. According to Article 14 of the Treaty, 44 States with nuclear capabilities (Annex II States) must ratify the Treaty for it to enter into force. Currently, nine out of 44 States have yet to ratify the CTBT. Of these, six States (China, Egypt, Iran, Israel, the United States, and the Russian Federation) have signed but not ratified the Treaty, while three States (India, Pakistan, and North Korea) have not yet signed. Only when the Treaty enters into force will States be able to fully leverage all four components of its verification regime: consultation and clarification, confidence-building measures, IMS, and On-Site Inspections (OSI). Therefore, achieving its entry into force remains essential, now more so than ever.

The CTBT remains a cornerstone of the non-proliferation and disarmament architecture, with a vital and complementary role alongside the landmark Non-Proliferation Treaty (NPT)

Despite these challenges, the CTBT remains a cornerstone of the non-proliferation and disarmament architecture, with a vital and complementary role alongside the landmark Non-Proliferation Treaty (NPT). In fact, the call to ban nuclear testing predates the call for the NPT. The Partial Nuclear Test Ban Treaty (PTBT) of 1963 marked the first international legal constraint on nuclear weapons by restricting nuclear testing underground, serving as a stepping stone to the NPT.

The CTBT is closely intertwined with the NPT[4], as reflected in the preambles of both treaties: the NPT Preamble envisions the CTBT, while the CTBT Preamble references Article VI of the NPT, which focuses on nuclear disarmament. The CTBT has been a fundamental component of every forward-looking adopted output in the NPT review process.

At the 1995 NPT Review and Extension Conference, the commitment to conclude CTBT negotiations by 1996 was a crucial element of the decision to extend the NPT indefinitely.

At the 2000 NPT Review Conference, two of the 13 practical steps were directly connected to the CTBT. These 13 steps were unanimously adopted to advance the effective implementation of Article VI of the NPT, as well as paragraphs 3 and 4(c) of the 1995 NPT Review and Extension Conference's second decision, titled "Principles and Objectives for Nuclear Non-Proliferation and Disarmament."[5]

Likewise, at the 2010 NPT Review Conference, as many as five action items in the NPT Action Plan were dedicated to the CTBT and nuclear testing. The Action Plan on Nuclear Disarmament outlines concrete steps for the total elimination of nuclear weapons. Actions 10, 11, 12, 13, and 14 directly support the CTBT's objectives.[6]

The CTBT plays a crucial role in advancing the NPT's first two pillars of the NPT: non-proliferation (Pillar I) and disarmament (Pillar II). Nuclear testing plays a crucial role in advancing nuclear weapons capabilities.[7] By prohibiting such tests, the CTBT effectively limits nuclear weapons proliferation, whether it involves new countries acquiring nuclear arms, existing nuclear states upgrading their arsenals, or the development of advanced nuclear weapon technologies—thus supporting non-proliferation both vertically and horizontally. The CTBT is essential to nuclear disarmament as it fosters confidence that any nuclear test would be detected.

Additionally, the IMS serves as a mechanism for engaging both NPT States Parties and Non-NPT States in constructive dialogue on disarmament issues. For example, Israel—a Non-Party to the NPT—is a Signatory State to the CTBT and hosts three certified IMS facilities. Similarly, despite announcing its de-ratification of the CTBT, the Russian Federation also declared the completion of its 32nd and final IMS station within its territory soon after.[8] Notably, Russia has remained a signatory to the Treaty and has expressed its intent to uphold the nuclear testing moratorium unless the US tests first while continuing to operate IMS stations on its territory.[9] Particularly during a time of heightened concern over the potential resumption of nuclear testing, the IMS plays a necessary role in encouraging other Annex II States, like China and the United States, to remain actively engaged in efforts to enhance monitoring and detection of potential nuclear test activity in the region.

The CTBT stands as a fundamental multilateral measure—non-discriminatory, inclusive, verifiable, and effective—advancing the goal of a nuclear weapons-free world.

In sum, the CTBT stands as a fundamental multilateral measure—non-discriminatory, inclusive, verifiable, and effective—advancing the goal of a nuclear weapons-free world. As we approach the 2026 NPT Review Conference, it is essential to elevate the CTBT's profile to support and reinforce the NPT regime. Below are some personal recommendations for all CTBT Signatory States to consider in pursuit of this goal:

Advancing universalisation of the CTBT

- The upcoming 30th anniversary of the CTBT in 2026 presents an important opportunity to promote a positive narrative about the Treaty and emphasise the critical importance of its entry into force.
- States should actively highlight the CTBT's achievements and its role in strengthening international security at relevant forums such as the Conference on Disarmament or by organising dedicated events to mark this milestone.
- Efforts by Signatory States should be intensified to engage with States that have not yet signed or ratified the CTBT. Signatory States should actively seek opportunities to foster diplomatic dialogue and implement targeted outreach initiatives, either independently or in conjunction with major international or regional meetings, to encourage non-signatory states to take concrete steps toward formalising their commitment to the Treaty.
- Signatory States should take ownership of the Treaty and act as its champions, recognising that achieving the CTBT's entry into force and universality is not solely the responsibility of the CTBTO but a shared obligation that rests with them as well.
- Signatory States should actively promote supportive and constructive language related to the CTBT at meetings of the Preparatory Commission for the Comprehensive Nuclear-Test-Ban Treaty Organisation (CTBTO) and across relevant forums, including the NPT Review Conferences and Preparatory Committees.
- Signatory States should lead efforts to raise awareness about the CTBTO Youth Group[10] to inspire the next generation within their respective countries to actively join efforts and contribute to the global call for a nuclear test ban. This includes promoting the Group's initiatives in schools or universities, as well as creating opportunities for collaboration and meaningful youth participation in the work of the CTBTO. Signatory States can also play a key role by providing funding to support and expand these efforts.

Signatory States should continue to highlight during NPT Review Conferences and Preparatory Committees that the prohibition of nuclear testing is an integral part of achieving the goals of the NPT.

Reinforcing the global norm against nuclear testing

- Signatory States should continue to highlight during NPT Review Conferences and Preparatory Committees that the prohibition of nuclear testing is an integral part of achieving the goals of the NPT, underscoring its role in advancing non-proliferation and disarmament efforts. Ideally, this should continue to be reflected in the outcome documents.
- Signatory States should encourage Annex II States to publicly reaffirm their commitment to maintaining the nuclear testing moratorium, demonstrating their dedication to global security and the objectives of the CTBT.
- Signatory States should reaffirm CTBT language from past NPT Review Conference documents and update it to reflect

current global security needs in drafting NPT final documents. In particular, reference to Action 11[11] of the 2010 NPT Review Conference, which urges States to refrain from any actions that would undermine the object and purpose of the Treaty until the CTBT enters into force.

Enhancing support for the CTBTO and completing the Verification System

- Signatory States should actively engage with the CTBTO to promote the installation and complete certification of IMS facilities within their territory. They should also ensure that Facility Agreements are signed if they are not already in place.
- Signatory States are urged to pay their assessed contributions to the CTBTO on time and in full, as this demonstrates political commitment and supports the activities of the CTBTO.
- Signatory States should make efforts to promote the use of CTBTO data for scientific research and civil applications within their respective countries, including the signing of Tsunami Warning Agreements.
- Signatory States should support the participation of more scientific experts in CTBTO capacity-building and training programs, as well as host CTBTO regional workshops to expand technical expertise.

The CTBT has proved to be a success story even prior to its entry into force, already making a profound positive impact while reinforcing the NPT's goals by curbing nuclear testing and promoting global security. With stronger support from Signatory States, it could unlock even greater potential, paving the way for a more robust non-proliferation and disarmament regime and a safer world.

30 January 2025

References

1. https://www.ctbto.org/our-mission/ending-nuclear-tests
2. https://www.ctbto.org/our-work/civil-and-scientific-applications
3. https://www.youtube.com/watch?v=7mtVEDXv2Is
4. https://vcdnp.org/75-years-after-trinity-the-nexus-between-the-ctbt-and-the-npt/
5. https://reachingcriticalwill.org/images/documents/Disarmament-fora/npt/GENERAL-DOCS/2000FD.pdf
6. https://www.reachingcriticalwill.org/images/documents/Disarmament-fora/npt/revcon2010/2010NPTActionPlan.pdf
7. https://www.ctbto.org/our-mission/ending-nuclear-tests
8. https://www.ctbto.org/news-and-events/news/russias-last-global-monitoring-system-station-installed-sending-data
9. https://www.armscontrol.org/blog/2023-11/nuclear-disarmament monitor
10. https://youthgroup.ctbto.org/

The politics of nuclear disarmament verification: How to advance nuclear disarmament

Michael Biontino

Nuclear Disarmament Verification, beyond its technical aspects, is an essential political element of nuclear disarmament since it prepares the ground for and enables disarmament agreements.

11. https://www.reachingcriticalwill.org/images/documents/Disarmament-fora/npt/revcon2010/2010NPTActionPlan.pdf

In its 79th session (2024), the UN Committee on Disarmament and International Security (1st Committee) adopted with an overwhelming majority a resolution[1] through which the Secretary General is tasked to seek the views of Member States on the establishment of a Group of Scientific and Technical Experts (GSTE) on Nuclear Disarmament Verification (NDV).

Indeed, both the technical and political aspects of NDV have been a longstanding item in international fora[2], prominently in the United Nations.

Throughout the discussion, it was recognised that the primary purpose and objective of Nuclear Disarmament Verification is to enable an evidence-based assessment of compliance by states parties to the obligations of a specific treaty and to ensure that appropriate and timely counter-measures can be taken in case of non-compliance, inter alia, to deny the violator the benefits of the violation.

Given the lack of substantive progress in pursuing disarmament commitments and obligations as required by Article VI of the NPT, the argument was brought forward that detailed further work on NDV only constitutes a distraction from the central issue of nuclear disarmament. Furthermore, and from a different perspective, it was argued that NDV can only be considered in detail, once a concrete nuclear disarmament instrument has been agreed upon.

However, given the fundamental security implications of nuclear disarmament, states relying on nuclear weapons in their security strategies can only be expected to engage in sustained nuclear disarmament if treaty obligations are verifiably and irreversibly adhered to. This requires effective and efficient NDV.

In the past, the more technical aspects of NDV were prominently explored in the International Partnership for Nuclear Disarmament Verification (IPNDV), which has aspired since 2014 to identify and develop practical solutions to the technical and procedural challenges associated with effectively verifying nuclear disarmament.[3]

Before this background, further open-ended scientific and technical work[4] in the framework of the United Nations seems to be the order of the day. A GSTE, whose “merits, objectives mandate and modalities” still need to be agreed upon, seems to be a promising venue.

However, NDV, beyond its technical aspects, is an essential political element of nuclear disarmament since it prepares the ground for and enables disarmament agreements. It is also an integral part of the implementation of such agreements and ensures that progress achieved in disarmament becomes irreversible.

Most recently, the UN Groups of Governmental Experts of 2019 (A/74/90)[5] and 2023 (A/78/120)[6] considered in depth the role of verification in advancing nuclear disarmament.

The overarching political objectives of NDV, beyond the implementation of specific arms control and disarmament norms, can be defined as improving the international security environment by generally re-establishing strategic trust, building confidence between nuclear weapons states (NWS) and non-nuclear weapons states (NNWS) and among NWS themselves, elevating the nuclear threshold, reducing the risk associated with any use of nuclear weapons, and thus serving as an intermediate step to engage in substantive discussions towards further nuclear arms control and disarmament norms and a world without nuclear weapons.

The following conceptual elements are of particular relevance in this context and especially underpin the consideration of how NDV would indeed advance Nuclear Disarmament:

Principles of NDV: Action 2 of the 2010 Action Plan[7] acknowledged the three principles of nuclear disarmament: transparency, verifiability, and irreversibility. The principle of transparency underpins the other two principles. Without transparency, nuclear disarmament cannot be verified, nor would NPT States Parties have complete confidence that nuclear disarmament measures have been accomplished in an irreversible manner.

Definition of NDV: Verification can be considered as the policy process of using available and collected data to assess whether a state party complies with the provisions of a specific arms control or disarmament agreement.

Objectives of NDV: For NDV to be considered effective, it would have to be able to detect a militarily significant violation of the underlying arms control or disarmament agreement in time. The success of the process is dependent on the subject and scope of NDV and the verification methods and instruments. The verification mechanism includes institutional, legal and technical arrangements, the skills and training of the inspectors, and the concluding assessment of the procedure by a verification authority/ body.

Scope of NDV: The scope of NDV should ideally cover the entire life cycle of a nuclear weapon. This could include material production, testing facilities, weapons assembly, weapons stockpile, weapons disassembly, storage disposition and the remaining fuel cycle. Furthermore, a conclusion will have to be reached if means of delivery, as well as nuclear command and information structures, should be part of the scope of NDV. Furthermore, the required verification measures may differ in terms of the applicable disarmament scenario. The closer we move to reaching and maintaining global zero, the higher the requirements in terms of transparency and intrusiveness will become.

Governance of NDV: Appropriate and effective governance will have to be a core element of further discussions of NDV. The various approaches to NDV include unilateral verification, a cooperative approach with active assistance from the inspected party, national verification – possibly open to third parties, verification by an international body, verification only by states parties, and an approach open at least in principle to other relevant/affected parties.

Compliance Mechanism: An effective NDV should form the basis for and create the ability to respond effectively to non-compliance and possibly include an ability to deny the violator the benefits of the violation. Therefore, an effective political and/or legal mechanism will have to be considered to decide about appropriate consequences. Relevant issues for a compliance mechanism would include, inter alia, the appropriate forum, who should participate in the decision making.

Considering that the deteriorating international security environment and lack of progress in the pursuit of nuclear disarmament obligations, obviously, the question arises if continued work on NDV, indeed, is not only a distraction from exactly these obligations. Given however, that effective NDV is indeed a necessary prerequisite for eventual progress in nuclear disarmament, it is quite appropriate to pursue interim measures, such as NDV, to pave the way.

4 December 2024

References

1. https://www.bing.com/ck/a?!&&p=416d9f940c909f-d632075d67fec91caac26f9405be02bad99d328af826a86744JmltdHM9MTczMzI3MDQwMA&ptn=3&ver=2&hsh=4&fclid=1895ff33-cef1-6acc-2987-ebf3cfe46bce&psq=A%2fC.1%2f79%2fL.67&u=a1aHR0cHM6Ly9kaWdpdGFsbGlcmFyeS51bi5vcmcvcmVjb3JkLzQwNjQ3MzIvZmlsZXMvQV9DLjFfNzlfTC42Ny1FTi5wZGY&ntb=12.
2. https://front.un-arm.org/wp-content/uploads/2019/09/A-51-182-Rev.1-E.pdf#page=37
3. https://europeanleadershipnetwork.org/commentary/10-at-10-10-lessons-learned-as-the-international-partnership-for-nuclear-disarmament-verification-turns-10/
4. https://www.bing.com/ck/a?!&&p=416d9f940c909f-d632075d67fec91caac26f9405be02bad99d328af826a86744JmltdHM9MTczMzI3MDQwMA&ptn=3&ver=2&hsh=4&fclid=1895ff33-cef1-6acc-2987-ebf3cfe46bce&psq=A%2fC.1%2f79%2fL.67&u=a1aHR0cHM6Ly9kaWdpdGFsbGlcmFyeS51bi5vcmcvcmVjb3JkLzQwNjQ3MzIvZmlsZXMvQV9DLjFfNzlfTC42Ny1FTi5wZGY&ntb=1
5. https://documents.un.org/doc/undoc/gen/n19/141/70/pdf/n1914170.pdf
6. https://documents.un.org/doc/undoc/gen/n23/183/95/pdf/n2318395.pdf

Taking responsibility: How NPT members can support justice for victims of nuclear weapons – and through this, the NPT

Jana Baldus and Dr Caroline Fehl

7. https://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede290115disarmamentactionplan_/sede290115disarmamentactionplan_en.pdf

Nuclear weapons harm humans – not only when used in war. Since the onset of the nuclear age, hundreds of thousands of people have suffered as a result of activities related to nuclear weapons development and production, including uranium mining, nuclear waste disposal, and nuclear weapons testing. Efforts to seek recognition and redress for affected individuals and communities have recently received growing public attention and have been addressed across various international fora.[1] Yet, engagement with the issue has so far been limited where the nuclear order is "at home": within the framework of the Nuclear Non-Proliferation Treaty (NPT). But NPT members can do more to further the cause of nuclear justice – not for purely altruistic reasons, but also in their own best interest.

Increasing awareness of nuclear legacies

Within the framework of the NPT, states have historically struggled to address the humanitarian and environmental consequences of nuclear weapons and have largely remained silent on the associated legacies of the nuclear past. However, there is an increased international interest in past and ongoing harm caused by nuclear weapons and in addressing its legacies. This interest has spread well beyond the membership of the Treaty on the Prohibition of Nuclear Weapons (TPNW), as reflected in two recent events.

On 10 December 2024, the Japanese organisation Nihon Hidankyo, founded by atomic bomb survivors (Hibakusha), will receive the 2024 Nobel Peace Prize. In announcing the award, the Norwegian Nobel Committee recognised that *"[t]he Hibakusha help us to […] grasp the incomprehensible pain and suffering caused by nuclear weapons" and that "[t]he fates of those who survived the infernos of Hiroshima and Nagasaki were long concealed and neglected"*.[2] The committee thus not only drew attention to the fates of the Hibakusha but also acknowledged their long-standing struggle for nuclear disarmament and their struggles for both recognition and material redress for the harm caused by nuclear weapons.

Less noticed, a month earlier, the UN Human Rights Council released a report on "Addressing the challenges and barriers to the full realization and enjoyment of the human rights of the people of the Marshall Islands, stemming from the State's nuclear legacy".[3] While the report specifically addresses the human rights implications of US nuclear testing in the Marshall Islands, it also draws attention to the ongoing consequences of nuclear weapons and human rights violations due to nuclear testing in many other places.

Coming to terms with the nuclear past: TPNW and beyond

Already during the negotiations on the TPNW, the testimonies of those affected by nuclear weapons were used to establish historical evidence on the consequences of nuclear weapons use and testing and were an important motivation for the treaty.

Reflecting these efforts, the TPNW is the first international framework in which nuclear justice is institutionalised, obliging its members to engage in victim assistance and environmental remediation (Articles 5 and 6). These "positive obligations" address a significant gap as bilateral measures to redress harm from nuclear weapons use and testing by nuclear weapons states have fallen short in multiple ways:[4] compensation programmes for affected communities are highly fragmented and restrictive, and to date, no nuclear weapon state has officially apologised for the consequences of nuclear weapons testing (with the exception of the US, which has apologised to its own citizens, but not to the citizens of the Marshall Islands).

Yet, for the foreseeable future, the TPNW will continue to be shunned by nuclear weapon states and many allied states benefitting from the latter's nuclear umbrellas. This implies that key players are unlikely to formally sign up to the treaty's victim assistance and environmental remediation principles. At the same time, divisions over the TPNW have added to already existing rifts within the membership of the NPT, which is being strained by crises ranging from Russian nuclear threats in the Ukraine war to regional proliferation threats, nuclear modernisation and nuclear build-ups. In this situation, taking up the issue of nuclear justice within the NPT framework can fulfil a dual purpose: broaden support for the cause of nuclear justice beyond the TPNW membership while at the same time serving as a bridge-building initiative between TPNW supporters and opponents in the NPT membership.[5]

Bringing discussions about the nuclear past into the NPT

One practical avenue for cooperation could lie in the proposed international trust fund to support communities and states affected by nuclear weapons,[6] currently being discussed by TPNW members under the leadership of Kazakhstan and Kiribati. If such a fund were to be established, it could help streamline existing assistance programmes and tailor support to the needs of affected communities. If opened up to non-TPNW members, it could also represent an important instrument of cooperation between the NPT and the TPNW. Such a cooperative approach is important, as some states are already pursuing unilateral initiatives – for fear of being too closely aligned with the TPNW. This, however, could be counterproductive as it could lead to a fragmentation of victim assistance and environmental remediation.

The aim should be to mainstream "nuclear justice" within the NPT, i.e. to include language on the consequences of nuclear weapons use and testing and the importance of coming to terms with nuclear harm with regard to different topics and in all documents.

In addition to facilitating cooperation and dialogue with the TPNW, states should strengthen efforts to address the nuclear past within the NPT Review process itself. In the run-up to the forthcoming NPT Review Conference, the aim should be to create joint statements on the topic, which highlight processes on coming to terms with the nuclear past and underline states' willingness to continue working on the topic. Even more easily, the topic could be integrated in existing working papers or declarations on issues such as nuclear testing or nuclear education. For instance, by highlighting the concrete consequences of resuming nuclear weapons testing, including underground testing, NPT members could help strengthen the anti-testing norm and emphasise the continued importance of the Comprehensive Nuclear-Test-Ban Treaty (CTBT). The aim should be to mainstream "nuclear justice"

within the NPT, i.e. to include language on the consequences of nuclear weapons use and testing and the importance of coming to terms with nuclear harm with regard to different topics and in all documents, similar to nuclear education and gender equality.

To realise this, the broadest possible participation of civil society in the NPT conferences is essential. Under no circumstances should access for affected communities be made more difficult; on the contrary, their contributions should be made central to the NPT conferences.

Prospects for discussions

The draft outcome document of the 2022 NPT Review Conference[7] already contained a section welcoming the increased attention to processes of victim assistance and remediation, as well as noting the presentation "of evidence on the humanitarian impact of nuclear weapons in fact-based discussions". This section was included in the document despite massive opposition from some nuclear weapons states, especially France, but later fell victim to Russia's rejection of the outcome document.

Building on this progress, states should aim to include endeavours to come to terms with the nuclear past in the outcome document of the upcoming NPT Review Conference. Such a section could include positive references to the 2023 and 2024 UN General Assembly resolutions on "Addressing the legacy of nuclear weapons"[8] and the Human Rights Council report[9] on nuclear legacies in the Marshall Islands. At best, such a section would also refer to and support the TPNW, especially the intersessional process to create an international trust fund.

However, to enable a genuine reappraisal of the nuclear past, states that are currently shying away from the TPNW – including European NATO members – must be prepared to cooperate with TPNW proponents and put aside their anxiety about participating in TPNW-inspired initiatives. Coming to terms with the nuclear past is a task for the entire international community, but also one that not only the nuclear weapon states but also the nuclear 'umbrella states' bear a special responsibility for.

10 December 2024

References

1. https://www.prif.org/publikationen/publikationssuche/publikation/beyond-the-ban
2. https://www.nobelprize.org/prizes/peace/2024/press-release/
3. https://www.ohchr.org/en/documents/thematic-reports/ahrc5777-addressing-challenges-and-barriers-full-realization-and
4. https://www.prif.org/publikationen/publikationssuche/publikation/beyond-the-ban
5. https://www.globalpolicyjournal.com/articles/conflict-and-security/npt-2022-opportunity-advance-nuclear-justice
6. https://humanrightsclinic.law.harvard.edu/wp-content/uploads/2023/01/011323%20Trust-Fund-Report-Combined.pdf.

The non-proliferation considerations of nuclear-powered submarines

Alexander Hoppenbrouwers

7. https://reachingcriticalwill.org/images/documents/Disarmament-fora/npt/revcon2022/documents/CRP1_Rev2.pdf
8. https://www.wagingpeace.org/unga-nuclear-justice/
9. https://www.ohchr.org/en/documents/thematic-reports/ahrc5777-addressing-challenges-and-barriers-full-realization-and

Since its announcement in late 2021, the AUKUS security partnership has sparked heated debate about its impact on global security. Critics of the partnership argue that it would provide nuclear-powered submarines fuelled with high-enriched uranium to Australia, a non-nuclear weapon state under the Treaty on the Non-Proliferation of Nuclear Weapons (NPT). Non-nuclear weapon states can conclude a so-called Article 14 arrangement in such situations, which means that routine safeguard measures by the International Atomic Energy Agency (IAEA) to ensure that the fuel is not diverted for the production of nuclear material for a weapons programme would temporarily not be applied. Some states have called this a nuclear proliferation risk.[1]

The political and legal considerations in Article 14 arrangements have been, and continue to be, extensively discussed.[2] Relatively little attention has been paid to the technical factors related to the nuclear-powered submarine programme that would influence an Article 14 arrangement. Exploring technical issues shows that the main potential proliferation risks associated with an Article 14 arrangement are located outside of the actual use of nuclear material to fuel the submarine, and that the IAEA will need to ensure that classification concerns do not stand in the way of adequate verification measures during this period.

Article 14 and diversion

Article 14 refers to a standard part of the safeguards agreement[3] that non-nuclear weapon states must conclude with the IAEA. Under an Article 14 arrangement, routine safeguards procedures are not applied to nuclear material to be used in non-proscribed military activities (as opposed to the proscribed use as nuclear explosives) since applying them would reveal classified military information. They are replaced by other measures that allow the IAEA to provide credible assurance that this nuclear material is not diverted. When evaluating the risk of diversion, much of the current literature focuses on the scenario where a state uses the non-application of safeguards as an opportunity to covertly remove the nuclear material from the submarine.

The main potential proliferation risks associated with an Article 14 arrangement are located outside of the actual use of nuclear material to fuel the submarine.

Looking at technical issues shows the challenge associated with such diversion. In the case of AUKUS, to remove nuclear material, the metal submarine hull designed to withstand tremendous water pressure would need to be cut open with heavy machinery.[4] The submarine's fuel would then be extracted from the reactor, requiring specialised facilities. Fuel for a nuclear submarine, however, cannot easily be used for the production of nuclear material for a weapons programme: it comes in the form of fuel rods surrounded by metal[5] or ceramic[6] cladding rather than the uranium or plutonium metal form used in weapons programmes. The uranium in this fuel would need to be chemically separated from other materials before it could be used to produce nuclear material for a weapons programme. All the above steps cannot be carried out quickly enough to outpace international reaction, so it would have to be done in covert facilities without alerting other states to the fact

that a submarine worth billions of euros had disappeared and an underground weapons programme had been launched. Hatches in the hull can provide easier access to the nuclear material, but the fuel used by submarines with hatches consists of uranium that is lower enriched[7] – and thus less proliferation-sensitive – than the uranium AUKUS submarines will use.

This suggests that two other technical issues will decide the diversion risks of an Article 14 arrangement. Firstly, how easy it is to use the fuel in question to produce nuclear material for a weapons programme. In addition to the ease of separating uranium from other materials mentioned above, this ease is determined by the enrichment of uranium. This refers to the percent of the total material that is fissile. Nuclear-powered submarines make use of uranium enriched to levels between around five and 97 percent, while weapons programmes generally require enrichment of 90 percent or higher.[8] Secondly, how much access the state has to the type of nuclear facilities needed for the production of nuclear material for a weapons programme. Enrichment and reprocessing facilities play a key role in this regard.[9]

The ability of the IAEA to carry out verification related to these two technical issues may be limited by classification concerns. Knowing the technical specifications of submarine fuel can help outsiders deduce what the submarine's capacities, such as speed or operational range, might be. To avoid this, states may try to limit verification measures that could reveal technical specifications, such as routine safeguards. This could also apply to activities outside of the fuel's use in the submarine, for example when the fuel is being fabricated.

What diversion risks should Article 14 discussions focus on?

Considering the above technical concerns, three main diversion risks present themselves. First, a state could use an excuse to remove nuclear fuel from the submarine when it returns to port. For instance, the state could claim that the submarine is undergoing maintenance unrelated to the nuclear material, which would reveal classified information if observed. A believable excuse may allow the state to gain a head start in the lengthy process of removing nuclear material described earlier by reducing international scrutiny.

Second, a state could attempt to divert nuclear material that is still in the fuel cycle. If it successfully argues that safeguards should not be applied to some nuclear facilities, reduced oversight offers an opportunity: for instance, the state could try to divert nuclear material being converted into fuel.

Third, a state could use the nuclear-powered submarine programme as an excuse to develop its nuclear capabilities. If a state domestically produces fuel for a submarine that requires high-enriched uranium, it has a chance to build a reserve of nuclear material—not yet converted into submarine fuel—that could be diverted before the international community has an opportunity to respond.

The negotiations of the document on which Article 14 is based give the IAEA solid arguments to apply safeguards to nuclear material when it is not used as fuel in the submarine, including during transportation between facilities.

These diversion risks suggest that an Article 14 arrangement should pay close attention to four key measures:

- There should be minimal and ideally no non-application of safeguards outside of the use of fuel in the submarine.
- Oversight should be given over the transportation of nuclear material, and its presence in facilities should be verified, including in a classified form.
- Verification measures should be carried out when nuclear material is placed in and removed from the submarine.
- The nuclear material's presence in the submarine should regularly be verified.

Furthermore, discussions on Article 14 arrangements should consider a submarine programme's impact outside the arrangement itself. In this context, any potential increase in a state's ability to produce nuclear material for a weapons programme should be met with increased international monitoring.

What could the IAEA's approach to Article 14 negotiations be?

The closer verification measures get to the finished form of the fuel and to the submarine, the more a state will object to them due to their potential to reveal information about the submarine's operational capacity. When the IAEA pursues its goal of providing credible assurance that nuclear material is not diverted, the main obstacle it will encounter is the need to balance its objective with Article 14's enshrinement of the protection of classified knowledge.

The IAEA can insist on at least the first three of the four points laid out above. The negotiations of the document on which Article 14 is based clearly established[10] that the non-application of safeguards does not extend to activities that are not intrinsically military, specifically naming enrichment and reprocessing. While the status of fuel fabrication activities is less clear, this gives the IAEA solid arguments to apply safeguards to nuclear material when it is not used as fuel in the submarine, including during transportation between facilities. It also suggests that the IAEA should be able to verify that fuel has entered an intrinsically military activity, namely when it is installed in the submarine. Regarding the fourth point, it is unlikely that the IAEA will regularly be able to carry out verification measures in or around the submarine. However, seeing the submarine in operational use would confirm the presence of nuclear material on board. The IAEA could, therefore, seek to ensure that it can carry out some verification measures whenever

References

1. https://www.reuters.com/world/china-aukus-countries-clash-iaea-over-nuclear-submarine-plan-2022-09-16/
2. https://vcdnp.org/wp-content/uploads/2021/10/Safeguards-and-naval-fuel-JC-211008.pdf
3. https://www.iaea.org/topics/safeguards-agreements
4. https://uploads.fas.org/2016/12/Frances-Choice-for-Naval-Nuclear-Propulsion.pdf
5. https://www.jstor.org/stable/resrep22545.19?seq=7
6. https://fissilematerials.org/blog/2020/04/us_study_of_reactor_and_f.html
7. https://uploads.fas.org/2016/12/Frances-Choice-for-Naval-Nuclear-Propulsion.pdf
8. https://www.nti.org/analysis/articles/expanding-nuclear-propulsion-challenges/
9. https://www.acq.osd.mil/ncbdp/nm/NMHB2020rev/docs/NMHB2020rev_Ch15.pdf
10. https://nationalsecuritytraining.pnnl.gov/fois/doclib/IAEA_153_Negotiating_History.pdf

In Russia's perceived war with the West, arms control is collateral damage

Nicholas Lokker

Russia seemingly perceives previously established arms control agreements as elements of the broader Western-dominated political and security order that it aims to overturn.

the submarine returns to port for longer-than-usual periods of time, adjusted based on how long the extraction of nuclear material from the submarine is estimated to take.

29 October 2024

As Russia's full-scale invasion of Ukraine approaches its third anniversary, relations between Moscow and the West have continued to deteriorate. Following the White House's approval[1] in November of Ukrainian strikes inside Russia with U.S-supplied ATACMs, the Kremlin once again escalated[2] its nuclear threats, formally updating Russian doctrine to lower the threshold for nuclear use in response to a subjectively determined threat to sovereignty and territorial integrity. This latest threat fits into a pattern[3] of more aggressive nuclear posturing from Moscow following the full-scale invasion—including a systematic dismantling of the arms control regime.

The most glaring example is New START—the last remaining treaty between Russia and the United States that sets restrictions on nuclear weapons. Though the March 2021 agreement[4] to extend the treaty was a notable achievement, things quickly took a turn for the worse after the February 2022 full-scale invasion. After first refusing[5] to submit to on-site inspections in the summer of 2022, Moscow later cancelled[6] its participation in the New START Bilateral Consultative Commission meeting that November. The most decisive step came the following February, when Moscow officially suspended its participation in the treaty. Russia has since signalled its disinterest in negotiating a successor to New START following its expiration in 2026, having rejected a U.S. proposal at the start of this year for bilateral conversations on a new treaty without conditions. Moscow's destruction of the arms control regime also extends to the conventional domain, having formally withdrawn from the Conventional Armed Forces in Europe (CFE) Treaty in November 2023.

Russian Foreign Minister Sergey Lavrov justified[7] rejection of the U.S. offer to resume a strategic arms control dialogue by arguing that "the United States has cast aside the principles on which our countries once agreed to establish cooperation, including on arms control". This statement reveals the fundamental driver of Russia's recent approach to arms control—namely, the intention to subsume it within its larger conflict with the West. Russia seemingly perceives previously established arms control agreements as elements of the broader Western-dominated political and security order that it aims to overturn. Deputy Foreign Minister Sergey Ryabkov made this linkage explicit when he stated[8] in January 2023 that the condition for Russia's return to New START compliance would be U.S. acceptance of Russian demands for security guarantees made in late 2021.

Russia's refusal to compartmentalise arms control also stems from an assessment of its coercive value vis-à-vis the West. Assuming—not without reason—a lower risk tolerance in the West than in Russia, the Kremlin has sought to instil fear with the goal of compelling Washington and its European allies to limit support for Kyiv. By linking arms control talks with the conflict in Ukraine, Moscow has signalled to Western governments that the breakdown of these talks is the price for their involvement in the war. For Russia, then, arms control represents a key tool at its disposal to

attempt to enhance its position vis-à-vis Ukraine.

Admittedly, Russia has not abandoned all aspects of arms control. Despite its suspended participation in New START, the latest U.S. annual assessment concluded[9] that Moscow likely continues to abide by the treaty's numerical limits—though the lack of inspections makes this increasingly difficult to verify. This continued observance of New START's central provisions suggests that Moscow may see remaining utility in limiting strategic nuclear capabilities, an interest that could grow should concerns in Russia rise about the costs of unconstrained nuclear competition with the United States. In a February 2024 speech[10], Putin warned of "Western attempts to draw [Russia] into an arms race, thereby exhausting us, mirroring the strategy they successfully employed with the Soviet Union in the 1980s". Moscow has also maintained[11] its interest in new agreements that would limit NATO's deployment of U.S. intermediate-range missiles (whether armed conventionally or with nuclear warheads) on European soil, including a proposal that Vladimir Putin himself made in 2019[12]—although this only came after Russia sought additional leverage by deploying its own intermediate-range missile in violation of the INF treaty. Finally, Russia has continued to engage in risk reduction efforts by notifying the United States of its strategic exercises and ballistic missile launches—including ahead of the notable use[13] of an intermediate-range ballistic missile against the Ukrainian city of Dnipro in late November 2024.

Moreover, while Russian disinterest in arms control seems to be increasingly entrenched, certain developments could change this in the future. Economic factors, such as a lack of resources stemming from sanctions and exhaustion from its war against Ukraine, could lead Russia to refrain from ambitious modernisation or numerical expansion of its arsenal and, therefore, incentivise it to seek limitations. More forceful interventions by Russia's international partners—most notably China, but also India—could also convince Moscow that greater engagement on arms control is necessary to keep its most important relationships intact. Finally, in the longer term, a successor to Putin could seek to return to the table, playing the arms control card to rehabilitate Russia's image within the international community. NATO's latest Strategic Concept, published in 2022, explicitly recognises[14] the potential role of arms control in enhancing deterrence and defence, and the alliance should not abandon hopes of using arms control as a tool to increase its security down the line.

Nevertheless, the United States and its NATO allies must, for the foreseeable future, be prepared for the absence of arms control with Russia, including the various dangers associated with that absence. This may mean pursuing more modest efforts[15] to reduce risk and increase predictability in the interim, including transparency and verification measures that do not require active cooperation from Moscow. And while the West should remain open to a renewed willingness to engage in arms control by Russia, it should not seek a new agreement at any price. There is a particular risk that this could occur after Donald Trump returns to the White House next January, given his apparent sympathy for key Russian demands to renegotiate the European security architecture, including a potential freeze[16] on discussions surrounding Ukrainian

accession to NATO membership. Yet Russia's linkage of arms control with these issues does not mean the West should respond in kind—and Trump would do well to remember that no deal is often better than a bad deal.

13 January 2025

References

1. https://apnews.com/article/biden-ukraine-long-range-weapons-russia-52d424158182de2044ecc8bfcf011f9c
2. https://www.reuters.com/world/europe/putin-issues-warning-us-with-new-nuclear-doctrine-2024-11-19/
3. https://www.cnas.org/publications/reports/assessing-the-evolving-russian-nuclear-threat
4. https://www.armscontrol.org/act/2021-03/news/us-russia-extend-new-start-five-years
5. https://www.armscontrol.org/act/2022-09/news/russia-further-pauses-new-start-inspections
6. https://www.cnn.com/2022/11/28/politics/us-russia-arms-control-talks/index.html
7. https://www.kommersant.ru/doc/6456037
8. https://www.kommersant.ru/doc/5785723
9. https://www.state.gov/2023-report-to-congress-on-implementation-of-the-new-start-treaty/
10. http://en.kremlin.ru/events/president/news/73585
11. https://www.reuters.com/world/russia-says-proposed-moratorium-former-inf-pact-missiles-will-end-soon-2023-11-03/
12. https://www.rferl.org/a/report-putin-sends-nato-proposal-for-moratorium-on-missile-deployment-to-europe/30182957.html

Bluff and bluster: Why Putin revised Russia's nuclear doctrine

Rishi Paul

13. https://www.c-span.org/video/?c5142975/pentagon-russia-notified-us-ballistic-missile-strike-ukraine
14. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf
15. https://europeanleadershipnetwork.org/commentary/bluff-and-bluster-why-putin-revised-russias-nuclear-doctrine/
16. https://www.kyivpost.com/post/41884

On 24th September 2024, Russian President Vladimir Putin announced[1] significant updates to Russia's nuclear doctrine in response to what Moscow perceives as increased Western interference in Ukraine. A few months later, on Tuesday 19th November, Putin formalised the changes as official policy[2] of the Russian Federation.

The revised doctrine, titled "Fundamentals of State Policy of the Russian Federation in the Field of Nuclear Deterrence",[3] N°991, expands Russia's conditions for nuclear weapon use. Moscow is now prepared to use nuclear weapons in retaliation to nuclear attacks, as well as conventional attacks[4] that threaten the sovereignty or territorial integrity of Russia or Belarus. The policy shift from the 2020 doctrine[5] is evident, as the previous stance also allowed for a nuclear response to conventional weapon attacks, but only under circumstances where "the very existence of the state is threatened."[6]

Notably, the policy explicitly extends Russia's nuclear protection to Belarus,[7] framing this as a commitment under the Union State agreement between the two nations. In 1999, Moscow and Minsk signed the Union State treaty, which outlined cooperation across various areas, including defence, while preserving the independence of both nations. Moscow's extended deterrence guarantee to Belarus is logical, given that Belarusian leader Alexander Lukashenko had permitted Russian-controlled tactical nuclear weapons to be stationed in Belarus, a move that was downplayed by some in the West as "purely a political message".[8]

In addition, Paragraph 10[9] of the revised doctrine states that: "The aggression by any state from a military coalition (bloc, alliance) against the Russian Federation and (or) its allies shall be considered as aggression by this coalition (bloc, alliance) as a whole". This line tacitly references NATO, emphasising that any aggression against Russia by a member of a military bloc or coalition is seen as aggression by the entire bloc. Furthermore, Paragraph 11[10] specifies that: "Aggression against the Russian Federation and (or) its allies by any non-nuclear state with the participation or support of a nuclear state shall be considered as their joint attack". According to the doctrine, this qualifies as grounds for nuclear retaliation. However, it remains unclear whom such retaliation would target.

What's pushed Putin to implement these changes and, in so doing, lower the nuclear threshold? In a nutshell, it's a consequence of the cautionary tale of "the boy who cried wolf"[11] — in this case, Putin's overreliance on the use of nuclear threats to induce Western caution — with the West's knack for strategically sidestepping Russia's red lines in Ukraine.

Since the outbreak of the war, Putin's repeated nuclear sabre-

rattling demonstrates bluff and bluster, and the Western powers have shown they can carefully walk the line without crossing it, at least in Moscow's eyes. Although the US initially took Putin's nuclear threats seriously — "this is not a bluff"[12] — Putin' use of nuclear intimidation has received mixed results. The West has managed a delicate balancing act by combining various initiatives ranging from communication with Russia via intelligence channels[13], providing targeted economic aid, and supplying Kyiv with increasingly advanced weaponry, such as the Anglo-French Storm Shadow cruise missile[14] for Russian targets within Ukraine, and F-16 fighter jets.[15]

This approach creates a core challenge for Putin; while Russia's nuclear deterrent prevents direct NATO involvement, it doesn't stop the West from operating just below this threshold.[16] Through these calibrated moves, Western allies continually test Russia's red lines, gradually eroding the credibility and effectiveness of Moscow's deterrence without triggering a direct confrontation. This slow but steady erosion of red lines by the West places Russia in a difficult position, as each step subtly undercuts its strategic leverage over Ukraine and undermines the effectiveness of its deterrent.

But what does Russia's revised nuclear doctrine and the looming threat of escalation reveal about how Putin views nuclear weapons? During the Cold War, the leaders of the US and Russia mostly held the view that nuclear weapons offered no real political or military edge against an adversary with secure second-strike capabilities. Beginning with the outbreak of the war, Putin shifted this paradigm by wielding nuclear weapons as tools of coercion,[17] aiming to manipulate shared nuclear risks for intimidation and political leverage. In his view, nuclear threats serve as instruments of deterrence and psychological warfare, calculated to pressure opponents while avoiding outright use.

Although Putin's nuclear threats have influenced the timing and nature of Western support for Ukraine, they have not fundamentally reshaped Western policies or deterred the ongoing expansion of aid. Instead, they underscore the limitations of nuclear coercion[18] as a tool for shaping adversaries' behaviour, highlighting its inherent bluntness and lack of precision in achieving political and strategic outcomes.

Putin's initial announcement on doctrinal changes was also timed to coincide with discussions at the United Nations, where Ukrainian President Volodymyr Zelensky was pressing for permission[19] to use advanced Western-supplied weaponry against high-value targets deep inside Russian territory. Zelensky's appeal reflects a strategic shift, as Ukraine seeks not only to defend its own territories but also to weaken Russia's capacity for continued aggression by targeting military infrastructure within Russia itself.

In Putin's view, nuclear threats serve as instruments of deterrence and psychological warfare, calculated to pressure opponents while avoiding outright use.

With Zelensky's request, western powers had to weigh the potential escalation risks against the benefits of allowing Ukraine broader operational freedom. In this context, Putin's 24th September announcement served as a counter-warning, subtly reminding the UN and NATO members of the dangers of pushing Moscow's red lines too far. Yet, despite this warning, on 17th November the US approved Kyiv's request for authorisation to use ATCMS missiles outside its own borders, and shortly after, the UK followed suit in lifting restrictions on Ukrainian use of British cruise Storm Shadow missiles on targets inside Russia.

After Biden's approval, Ukraine fired six ATACMS and Storm Shadow missiles into Russia, indicating that the US and UK both believed Putin was bluffing in his 24th September statement, which warned that aggression against Russia by a non-nuclear state, if supported by or involving a nuclear state, would be treated as a joint attack on the Russian Federation and could provoke a nuclear response.

But why has the US decided to push against Russia's red lines? This could be down to the fact that President-elect Trump has repeatedly expressed dissatisfaction with continued US military and economic support for Ukraine, arguing that it does not align with US national interests. Throughout his campaign, Trump claimed[20] he would end the conflict on the first day of his presidency. Without meaningful US backing, the West would face significant challenges in marshalling resources to support Ukraine, which would cede military advantages to Russia. Paradoxically, while this decreases the likelihood of Putin escalating the war through nuclear means, it significantly increases the risk of Ukraine losing more territory to Russia.

With a countdown of less than two months before an incoming Trump administration, the Biden administration is essentially signalling to Ukraine that it will support its efforts to retain the small portion of Russian territory it currently holds, to use it as a significant bargaining chip in potential future negotiations.

In response, Putin formalised Russia's revised nuclear doctrine "in a timely manner,"[21] doubling down on his position to underscore the seriousness of Russia's political and military boundaries while seeking to deter further Western military involvement without provoking direct confrontation. Following this, Putin retaliated by launching a nuclear-capable experimental ballistic missile with a range of several thousand kilometres against the Ukrainian city of Dnipro. This signalled a warning to Kyiv's allies: a broader conflict may loom unless the West adjusts its policy.

Despite Putin's readiness to escalate through advanced weaponry, Moscow's decision to notify the US Threat Reduction Center, only 30 minutes prior, clearly aimed to prevent misinterpretation and mitigate the risk of immediate nuclear escalation.[22] This reflects Putin's recognition of the dangers of miscalculation and unintended escalation, highlighting his intent to avoid inadvertently triggering a nuclear war.

However, the possibility of Putin escalating with the use of low-yield nuclear weapons on the battlefield cannot be entirely ruled out. Although unlikely, such a decision might come as a nuclear warning shot over a remote area in Ukraine if Putin perceives an imminent threat to his regime or, as stated in the revised doctrine, the "sovereignty and/or territorial integrity"[23] of Russia and Belarus is at stake. Yet, the term "sovereignty" in the revised doctrine is deliberately ambiguous and could be interpreted to include regime security. This mirrors the vagueness of Russia's earlier 2020 doctrine,[24] which permits nuclear use if "the very existence of the state is threatened."

Putin's use of studied ambiguity — lack of specificity — is a deliberate tactic aimed at sowing doubt in the minds of his adversaries. Whilst the use of ambiguity in nuclear doctrine is not

unique to Russia and is employed by other nuclear-armed states, Putin's application stands apart due to its context, as it is tailored specifically to an ongoing war and is therefore formulated broadly to avoid a firm commitment to use nuclear weapons and keep Putin's options open.

Finally, any use of nuclear weapons by Russia would risk triggering retaliation in kind and could fundamentally shift the war's dynamics by drawing NATO into the conflict—an outcome contrary to Putin's interests. Currently, Russia holds conventional military superiority[25] over Ukraine, a position that would be undermined if NATO were to intervene directly and fight alongside Ukraine.

25 November 2024

References

1. http://en.kremlin.ru/events/president/news/75182
2. http://en.kremlin.ru/events/president/news/75598
3. http://publication.pravo.gov.ru/document/0001202411190001?index=1
4. https://www.themoscowtimes.com/2024/11/19/putin-lowers-threshold-for-using-nuclear-weapons-in-updated-doctrine-sparking-escalation-concerns-a87059
5. http://www.kremlin.ru/acts/bank/45562
6. http://www.kremlin.ru/acts/bank/45562
7. https://www.themoscowtimes.com/2024/11/19/putin-lowers-threshold-for-using-nuclear-weapons-in-updated-doctrine-sparking-escalation-concerns-a87059
8. https://foreignpolicy.com/2024/03/14/russia-nuclear-weapons-belarus-putin/
9. http://publication.pravo.gov.ru/document/0001202411190001?index=4
10. http://publication.pravo.gov.ru/document/0001202411190001?index=4
11. https://en.wikipedia.org/wiki/The_Boy_Who_Cried_Wolf
12. https://caspiannews.com/news-detail/president-putin-declares-partial-military-mobilization-2022-9-22-0/
13. https://carnegieendowment.org/russia-eurasia/politika/2024/09/russia-nuclear-doctrine-blackmail?lang=en
14. https://news.sky.com/story/ukraine-strikes-russian-submarine-and-landing-ship-in-audacious-assault-on-crimea-naval-base-12960336
15. https://www.chathamhouse.org/2024/09/are-ukraines-f-16s-another-case-too-little-too-late
16. https://carnegieendowment.org/russia-eurasia/politika/2024/09/russia-nuclear-doctrine-blackmail?lang=en
17. https://www.independent.co.uk/voices/putin-russia-nuclear-weapons-risk-ukraine-b2031955.html
18. https://www.cambridge.org/gb/universitypress/subjects/politics-international-relations/international-relations-and-international-organisations/nuclear-weapons-and-coercive-diplomacy?format=HB&isbn=9781107106949
19. https://theconversation.com/the-world-isnt-taking-putins-nuclear-threats-seriously-the-history-of-propaganda-suggests-it-should-239942
20. https://www.bbc.co.uk/news/articles/ced961egp65o

Nuclear vs cyber deterrence: why the UK should invest more in its cyber capabilities and less in nuclear deterrence

Nikita Gryazin

Cyber-attacks, state-sponsored disinformation campaigns, and other non-kinetic forms of warfare have become more prevalent and pose a more immediate risk to national security.

21. https://www.bbc.co.uk/news/articles/cj4v0rey0jzo
22. https://www.theguardian.com/world/2024/nov/22/russia-ukraine-war-ballistic-missile-warning
23. http://publication.pravo.gov.ru/document/0001202411190001?index=6
24. http://www.kremlin.ru/acts/bank/45562
25. https://news.sky.com/story/why-is-there-talk-of-world-war-three-13256716

The strategic environment after Russia's full-scale invasion of Ukraine in 2022 presents a stark contrast to the Cold War era when nuclear weapons were the ultimate deterrent. Today, the threats that the UK faces are more nuanced and diverse, ranging from state-sponsored cyber-attacks to sophisticated disinformation campaigns. These challenges require a shift in focus from traditional nuclear deterrence to modern defensive and offensive cyber capabilities, arguably more effective in safeguarding national security.

The changing nature of threats

The primary argument against significantly enhancing the UK's nuclear deterrent lies in the changing nature of global threats. Opponents of shifting investment from nuclear deterrence to cyber capabilities would argue that nuclear weapons provide a proven and robust deterrent against existential threats, with decades of strategic stability behind them. Indeed, the nuclear age has not gone anywhere: Russia continues using nuclear weapons for blackmail,[1] has stationed nuclear weapons in Belarus,[2] and some Russian experts are calling for a preventive nuclear strike.[3] Even a slight reduction in nuclear deterrent investments could be considered as a vulnerability by allies and as an opportunity by adversaries. However, we are now in the cyber age[4] where there is another layer of competition and warfare between state and non-state actors –cyberspace. This has altogether evolved the threat landscape. Cyber-attacks, state-sponsored disinformation campaigns, and other non-kinetic forms of warfare have become more prevalent and pose a more immediate risk to national security.

The UK has already experienced the consequences of these new types of threats coming from Russia and China. Recent cyber-attacks on the UK's critical national infrastructure have highlighted the vulnerability of the UK's digital systems. London's Transport for London was subject to cyber-attacks twice in the last two years: in July 2023[5] and September 2024.[6] In May 2024, the target was the Ministry of Defence: the Defence Secretary confirmed that a 'malign actor' gained access to part of the MoD payment network,[7] and in March, the Defence Secretary's RAF plane's GPS signal was 'jammed' near Russia's Kaliningrad.[8] Most recently, in July 2024, the Russian-based hacking group Qilin (believed to be part of a Kremlin-protected cyber army) stole patient data in a cyber-attack on NHS England systems,[9] resulting in a major data hack and thousands of patient appointments and operations postponed.

These attacks on the UK's critical defence and social infrastructure not only disrupt services but also undermine public confidence in the government's ability to protect its citizens. Moreover, there is a

strong nexus between cyberattacks and disinformation campaigns, as both are often used together in coordinated efforts to disrupt, destabilise, or manipulate targets. The recent disinformation campaigns about the Southport stabbing on 29 July, possibly linked to Russia-based actors,[10] have fuelled far-right protests and nearly destabilised the country, underscoring the power of information warfare to disrupt society.

The diminishing utility of nuclear weapons

While nuclear weapons continue to serve as a deterrent against existential threats, their utility in addressing the challenges of the 21st century is limited. Nuclear weapons are primarily designed to deter or respond to large-scale military aggression, primarily from other nuclear-armed states. However, the likelihood of such conflicts is relatively low even in today's geopolitical environment.

In contrast, cyber threats are far more immediate and pervasive. While nuclear weapon use in war happened only once in history, cyber-attacks have been recorded daily since the very first cyber incident in 1988.[11] Cyber-attacks can be launched remotely, often with plausible deniability, making them an attractive option for state and non-state actors alike. Furthermore, the consequences of a successful cyber-attack can be devastating, ranging from the disruption of critical infrastructure and theft of sensitive information to the sowing of division and chaos in society. Unlike nuclear weapons, cyber capabilities are more dynamic, flexible, and efficient.

The case for greater investments in cyber capabilities

Given the evolving threat landscape, the UK would benefit from a greater focus and investment in its cyber capabilities rather than expanding and modernising its nuclear arsenal. There are several reasons for this:

- Modernising nuclear weapons is an expensive and resource-intensive process. According to the Nuclear Information Service,[12] the total cost of the UK's nuclear weapons programme between 2019 and 2070 is £172bn. In contrast, the UK's National Cyber Strategy 2022[13] is £2.6bn over three years. As cybercrime is estimated to cost the UK economy £27bn per year,[14] some costs associated with maintaining and upgrading the UK's nuclear arsenal could be better spent on enhancing cyber defences and developing offensive cyber capabilities.

- The institutions are already in place. The UK has already embraced the use of offensive cyber capabilities, as outlined in its National Cyber Strategy,[15] which sees these tools as essential for national security and deterrence. The UK's approach has evolved from a largely defensive posture to recognising the need for proactive measures, such as disrupting adversaries' cyber operations. The UK's National Cyber Force (NCF), established in 2020, conducts offensive cyber operations under the authority of international law, particularly the UN Charter, and is subject to domestic legal frameworks like the Intelligence Services Act 1994 and the Investigatory Powers Act 2016, ensuring that operations are lawful and proportionate. The announced Cyber

Security and Resilience Bill[16] should further expand the scope of the current cyber regulations.

- Nuclear weapons are inherently indiscriminate, causing massive destruction and inevitable collateral damage, both immediate and long-term. Even with advancements in technology, the lethality of nuclear weapons cannot be precisely controlled, and they are largely static in their role as deterrents. Cyber weapons, in contrast, offer precision and adaptability. Cyber operations can be designed to target specific systems, networks, or capabilities, avoiding widespread physical harm and ensuring minimal collateral damage. The flexibility of cyber tools allows the UK to respond to emerging threats with a degree of proportionality that nuclear weapons cannot offer, addressing security challenges in a measured, dynamic, and controlled way. By prioritising cyber capabilities, the UK can tailor responses to achieve strategic objectives without the humanitarian and environmental consequences that nuclear weapons bring.

- The rapid pace of technological advancement means that the nature of cyber threats is constantly evolving. Today, cyber is increasingly driven by AI, so investing more in AI-powered cybersecurity would make monitoring, analysing, detecting, and responding to cyber threats more efficient.

- By prioritising cyber capabilities, the UK can position itself as a global leader in cybersecurity. For this, institutions are already in place, such as the National Cyber Security Centre (NCSC) and the CYBERUK annual conference, established in 2016. If better funded,[17] it would enable the UK to play a more prominent role in shaping international norms and standards in cyberspace. In contrast, increased funding of the nuclear deterrent contributes to global instability and undermines efforts to promote nuclear disarmament.

The strategic environment has shifted, and the threats facing the UK today require a more nuanced approach. As a result, the new UK Labour government should focus on cyber capabilities over nuclear deterrence. Investing in cyber, both defensive and offensive, offers a more effective means of protecting the UK from the growing threats of cyber-attacks and disinformation campaigns. Unlike nuclear weapons, which are largely symbolic, cyber capabilities provide real-time, actionable solutions to the challenges of our cyber age.

23 September 2024

References

1. https://cepa.org/article/putins-nuclear-blackmail-a-kremlin-addiction/
2. https://tass.ru/mezhdunarodnaya-panorama/21240501
3. https://profile.ru/politics/primenenie-yadernogo-oruzhiya-mozhet-uberech-chelovechestvo-ot-globalnoj-katastrofy-1338893/
4. https://www.cambridge.org/core/books/security-in-the-cyber-age/E541018084AB8EA99569AFAE6EDE1323#fndtn-information
5. https://www.london.gov.uk/who-we-are/what-london-assembly-does/questions-mayor/find-an-answer/tfl-russian-hack
6. https://www.bbc.co.uk/news/articles/cd9dpek1883o

The flexibility of cyber tools allows the UK to respond to emerging threats with a degree of proportionality that nuclear weapons cannot offer, addressing security challenges in a measured, dynamic, and controlled way.

7. https://www.theguardian.com/uk-news/video/2024/may/07/grant-shapps-confirms-cyber-attack-on-ministry-of-defence-video
8. https://www.bbc.co.uk/news/uk-68569676
9. https://www.bbc.co.uk/news/articles/czd9glyx414o#:~:text=NHS%20England%20declared%20it%20a,and%20major%20data%20security%20concerns.&text=The%20Russian%2Dbased%20hacking%20group,demanded%20a%20%C2%A340m%20ransom.
10. https://www.politico.eu/article/uk-probes-whether-state-actors-stoked-far-right-riots/
11. https://www.fbi.gov/history/famous-cases/morris-worm#:~:text=At%20around%208%3A30%20p.m.,grinding%20computers%20to%20a%20halt.
12. https://www.nuclearinfo.org/article/dreadnought-vanguard-astute-dismantling-aldermaston-burghfield-barrow-devonport-faslane#:~:text=This%20method%20estimates%20the%20total,building%20four%20new%20Dreadnought%20submarines.
13. https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience

Nuclear posture and cyber threats: Why deterrence by punishment is not credible – and what to do about it

Eva-Nour Repussard

Whilst the British nuclear posture is meant to deter cyber-attacks—the number of cyber-attacks has continued to increase in recent years.

14. https://assets.publishing.service.gov.uk/media/5a78e882e5274a2acd18ab84/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf
15. https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#part-1-strategy
16. https://www.ncsc.gov.uk/blog-post/legislation-help-counter-cyber-threat-cni
17. https://www.thetimes.com/business-money/technology/article/decision-to-withhold-report-on-national-cyber-security-centre-slammed-by-tds-n98w8vvkk

The United Kingdom's latest nuclear doctrine suggests that severe cyber-attacks on their national or critical infrastructure could provoke a nuclear response. Despite this, cyber-attacks against the UK have surged over the past decade. This increase can be partly attributed to the perceived lack of credibility in the UK's nuclear retaliation threat towards cyber-attacks. With regard to cyber-attacks, the strategy of deterrence by punishment is ineffective for two main reasons: i) the threshold for transitioning from a cyber to a kinetic response remains hard to meet in times of relative peace between two countries, and ii) the inherent challenges in attributing cyber-attacks to specific state actors. Instead of deterrence by punishment, the UK should seek to increase its resilience to cyber-attacks and focus on a strategy of deterrence by denial regarding cyber threats.

Nuclear postures are increasingly explicit about the conditions under which nuclear weapon states might use nuclear weapons in response to non-nuclear threats, particularly from emerging technologies or emerging threats. This is evident in the United Kingdom's 2021 Integrated Review,[1] which states that they "will not use, or threaten to use, nuclear weapons against any non-nuclear weapon state party to the Treaty on the Non-Proliferation of Nuclear Weapons 1968 (NPT)", but then continues by stating that they "reserve the right to review this assurance if the future threat of weapons of mass destruction, such as chemical and biological capabilities, or emerging technologies that could have a comparable impact, makes it necessary". Arguably, the French posture on "core interests",[2] Russia's Principle on Deterrence,[3] and the United States' 2022 Nuclear Posture Review,[4] all hint at a similar posture in regard to nuclear weapons and "emerging threats".

Whilst the British nuclear posture is meant to deter cyber-attacks—the number of cyber-attacks has continued to increase in recent years. According to the Information Commissioner's Office, the UK experienced more cyber-attacks in 2023 than ever.[5] Several reports also warn that the UK is especially vulnerable to cyber-attacks on its critical infrastructure. For example, according to the Joint Committee on the National Security Strategy, "the UK could face a crippling cyber-attack on its critical national infrastructure (CNI) at any moment",[6] whilst, for example, the Office of the Nuclear Regulator has "repeatedly found gaps in Sellafield's cybersecurity from 2019 to 2023 that could not be fully resolved during that time".[7] Arguably, nuclear retaliation to cyber-attacks is not credible—and such a lack of credibility also weakens the credibility of the British deterrent altogether.

The first reason for the lack of credibility is that the threshold for transitioning from a cyber to a kinetic response remains hard to meet and assess in times of relative peace between two countries. Recent history is full of examples in which critical

cyber-attacks—even when attributed with high confidence—have not been met with kinetic retaliation. Some of the most famous examples being Stuxnet, a cyber-attack targetting Iran's Natanz uranium enrichment plant, attributed to the United States and Israel; and the WannaCry Ransomware attack, attributed to North Korea. These cyber-attacks, despite their criticality, have not met kinetic retaliation. The reason for the lack of kinetic retaliation is not solely due to the attribution problem (that I will cover in the next paragraph) but also due to the fact that cyber-attacks and kinetic attacks still differ significantly—notably in terms of gravity—making proportional and justified kinetic retaliation extremely complex. Whilst the International Criminal Court recently started to investigate[8] whether alleged Russian cyber-attacks on Ukrainian civilian infrastructure could be deemed war crimes, such a decision is taking place whilst an ongoing kinetic conflict is already happening between Russia and Ukraine. In times of peace between two countries, whether cyber-attacks can be deemed war crimes, or acts of war, is still yet to be seen, as it is still highly complex to assess at which point a cyber-attack could be met with kinetic retaliation. Whilst the threshold certainly exists, it has yet to be assessed and agreed upon with regard to international law.

Second, the issue of attribution is inherently problematic in cyberspace, and is the main reason why kinetic retaliation is near impossible in practice. High-confidence attribution is common (through diplomatic, intelligence and technical means), but identifying the sponsor of a cyber-attack with absolute certainty is extremely challenging, rendering nuclear retaliation too high of a risk for the affected country to undertake—regardless of the severity of the cyber-attack. In cyberspace, it is much harder to identify the sponsor behind an attack: have such attacks been decided and sponsored by a nuclear weapons state? Or have they been carried out independently by a group of hackers or 'hacktivists'? Indeed, contrary to the kinetic domain, the cyber domain has a low barrier to entry, and any 'patriot' can carry out cyber-attacks without requiring sponsorship or approval from a state. What complicates the task is that—regardless of their potential sponsorship—alleged sponsor states have always denied cyber attacks and have claimed plausible deniability.

Lately, this has been seen with the Killnet group in Russia[9] and Anonymous in Western states. Furthermore, false attributions are also common in cyberspace and states increasingly conduct 'false-flag' attacks, that is, attacks designed to deflect attribution to an uninvolved party. For example, during the 2018 Pyeongchang Winter Olympic Games in South Korea, the Russian GRU targeted the Games with the "OlympicDestroyer" cyber-attack[10]; however, the Russian group designed its attack to appear as if it had been the work of North Korea. A kinetic retaliation from South Korea—if wrongly attributed to North Korea—would have been an unprovoked act of war against North Korea and could have led to a conflict with its neighbour. Whilst this false-flag attack has been rightly attributed to the Russian GRU, other cyber-attacks might have been wrongly attributed.

Therefore, whilst such a nuclear posture may appear concerning at first, it lacks credibility and fails to provide effective deterrence against cyber-attacks. Instead, the UK should consider removing "emerging technologies" from their nuclear posture, or be more specific in its references to "emerging" threats, and clearly state

which emerging threat it is seeking to deter through nuclear retaliation. Furthemore, the the current ambiguity does not give the UK a strategic advantage, but rather the lack of credibility with regard to cyber-attacks weakens the overall credibility of the British deterrent.

Cyberspace intrinsically differs from the kinetic arena; thus, cyber problems require cyber solutions. Regarding cyber threats, rather than deterrence by punishment and kinetic retaliation, the UK should focus its energies on prevention rather than punishment, and seek to achieve 'deterrence via denial' whereby the feasibility of a successful cyber-attack is so low that the threat is sufficiently mitigated. The UK should seek to increase the cost and difficulty for potential aggressors to successfully enact a cyber-attack on its critical infrastructure. This can be achieved through cybersecurity measures such as reducing the attack surface (i.e., reducing the number of points where an attacker can try to access a system), such as air-gapping systems, modern encryption and zero trust architecture. Air-gapping can effectively increase the cost of a cyber operation, making it extremely costly for future attackers. As the cyber expert Kim Zetter wrote in her book "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon", Stuxnet cost hundreds of millions of dollars to carry out, and several years to plan.

Though deterrence by denial is not infallible, cyber resilience is the other important tool in the UK toolkit. The need for cyber resilience is the recognition that some attacks will still happen, and the UK will need to be prepared for these, i.e. be resilient enough to minimise their impact and be able to recover. In most cases, this can be achieved through backup systems that operate independently from cyber. In other cases, such as the British nuclear deterrence ability, cyber resilience can be built with its Allies—France and the United States—which could ensure deterrence if the British nuclear-powered ballistic missile submarines were incapacitated by cyber-attacks.

Thus, to effectively address the rising threat of cyber-attacks, the UK must shift from relying on nuclear retaliation to focusing on bolstering its cyber defences. By enhancing resilience and deterrence by denial, the UK can render potential cyber-attacks impractical and unlikely to succeed.

19 September 2024

References

1. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf
2. https://www.frstrategie.org/sites/default/files/documents/publications/recherches-et-documents/2020/202004.pdf
3. https://www.mid.ru/en/foreign_policy/international_safety/1434131/
4. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF#page=33
5. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/05/organisations-must-do-more-to-combat-the-growing-threat-of-cyber-attacks/#:~:text=Over%203%2C000%20cyber%20breaches%20were,learnt%20from%20common%20security%20mistakes.

By enhancing resilience and deterrence by denial, the UK can render potential cyber-attacks impractical and unlikely to succeed.

The unintended consequences of deterring cyber attacks through nuclear weapons and international law

Verena Jackson

The use of nuclear weapons to deter cyber attacks poses unique legal issues under both international law and the global non-proliferation regime.

6. https://www.theguardian.com/technology/2023/dec/13/uk-at-high-risk-of-catastrophic-ransomware-attack-report-says
7. https://www.chathamhouse.org/2024/07/uk-needs-move-faster-nuclear-energy-cybersecurity
8. https://www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14/
9. https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/
10. https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/

The nexus of cyber threats and nuclear deterrence

In today's security landscape, the rising cyber capabilities of (potential) adversaries have urged concern. Not only are policy considerations being discussed, but also the legal implications of cyber threats – from both offensive and defensive perspectives – are yet to be explored. The Cyber-Nuclear Nexus[1] is mainly discussed when assessing the threats from cyberspace to nuclear weapons. Few studies[2] have examined the role of nuclear weapons as an active part of the nexus: nuclear weapons as a means of deterrence against cyber attacks. Deterrence with nuclear weapons against cyber attacks poses new legal questions to international law and the global non-proliferation regime.

For the past decades (the prevention of) conflicts between nuclear-armed states were focused on deterrence by state-owned nuclear arsenal: the bigger the better, the more the merrier. In a technological era where deterrence needs to go beyond this concept and where advanced cyber capabilities are increasingly available to a wider range of states, non-state actors and proxies,[3] and nuclear disarmament efforts stalling,[4] there needs to be a more systematic understanding of the legal and policy mechanisms through which modern cross-domain deterrence can be operationalised more effectively but within the international legal framework. But international law doesn't exactly give the green light for cyber-nuclear deterrence.

The nature and scope of cyber threats

The evolution of cyber threats has progressed from simple espionage and disruption, jeopardising a state's sovereignty, to complex, large-scale operations capable of causing harm to millions of people. State-sponsored cyber attacks, like the 2010 Stuxnet operation[5] aimed at Iran's nuclear facilities, have showcased the capacity of cyber warfare to inflict physical damage and unsettle global politics. Additionally, the growing interconnection of critical infrastructure with digital networks, including power grids, financial systems, health care providers and military command structures, has amplified the vulnerability of nations to severe cyber disturbances.

The dawn of cyber warfare is rapidly transforming the nature of conflict. Unlike traditional warfare, which relies primarily on kinetic forces and visible actors, cyber attacks—as means of cyber warfare—are often covert, instantaneous, and capable of causing widespread disruption without the need for conventional military assets. As states and critical infrastructures become increasingly

digitised, cyber attacks not only represent a real threat to national security, economic stability, and public safety but also seem like a convenient and impactful means of warfare.

The use of nuclear weapons to deter cyber attacks poses unique legal issues under both international law and the global non-proliferation regime. In particular, it raises questions about the applicability of existing legal frameworks to non-kinetic threats, the proportionality of a nuclear response to a cyber attack, and the practicality of attributing cyber attacks to a specific state actor in a timely and accurate manner.

Cold War nuclear deterrence applied in a digital world

The rationale for applying nuclear deterrence to cyberspace stems from Cold War-era deterrence theory, specifically the principle of Mutually Assured Destruction (MAD).[5] This strategic principle states that the threat of total annihilation through nuclear retaliation deters all parties from initiating a nuclear conflict, ensuring that no rational actor would risk such catastrophic escalation.

One might argue that, like how the fear of nuclear retaliation prevented widespread conventional warfare during the Cold War, it could also deter major cyber attacks on critical infrastructure today. However, deterring cyber threats by using nuclear weapons presents distinct obstacles.

Unlike conventional attacks (e.g., missiles), cyber attacks frequently lack clear attribution, as they are often carried out through intermediates, making it difficult to trace the origin and assign responsibility to a specific nation or state entity. The potential deployment of nuclear arms in reaction to a cyber attack raises concerns regarding the appropriate level of response and the potential for unmanageable escalation. This may interfere with legal and moral boundaries.

International legal frameworks and nuclear-cyber deterrence

The UN Charter and the use of force against cyber attacks

Applying established legal frameworks to the field of cyber-nuclear deterrence exposes a fundamental dilemma: Is the threat of nuclear retaliation ever justifiable or necessary in response to a non-physical cyber operation? The Tallinn Manual on the International Law Applicable to Cyber Warfare[6] provides guidance, suggesting that responses to cyber attacks should align with established principles of the law of war, even though it does not explicitly address nuclear deterrence.

Article 2(4) of the UN Charter[7] explicitly forbids the intimidation or employment of force against the (territorial) sovereignty of any state. Nevertheless, Article 51[8] acknowledges "the inherent right of individual or collective self-defence if an armed attack occurs". The first legal uncertainty emerges in determining whether a cyber attack constitutes such an "armed attack" and thus may trigger a response justified under Article 51.

Established interpretations stem from a "pre-cyber era" and focus on kinetic force and physical destruction. And even then, a certain threshold of severity must be passed to justify a state's response under Article 51. In the context of cyber, this threshold needs to be tailored to the specifics of cyber attacks for them to be considered significant enough to trigger a military or legal response. Only attacks causing substantial damage (to critical infrastructure) or posing a direct threat to national security could comply with the existing criteria. If the scale and effect of a cyber attack are comparable to those of a kinetic attack—resulting in significant damage, casualties, or disruption—it may constitute a justification for the use of force under Article 2(4) of the UN Charter, potentially justifying self-defence under Article 51. Granted, a cyber attack does trigger a state´s right to self-defence, but it remains disputed[9] if a nuclear response (or threat) could ever comply with Article 2(4) of the UN Charter. The principles and rules of humanitarian law also have to be considered.

Attribution of cyber attacks and state responsibility

States can only be held legally responsible for cyber attacks when they are attributable to them.

A state´s responsibility in cyberspace arises when cyber attacks can be attributed to the state, either through direct involvement of state organs or via proxies[10] acting under its effective control. Adversaries use third-party systems, proxy servers and VPNs, or even "false flags" to cover their operations. This makes presenting clear evidence linking an attack to a particular state difficult, although this is necessary under international law to prevent unjustified retaliation. The level of evidence required for legal attribution, which serves as the basis for lawful countermeasures under international law, is notably higher than what is needed to hold a state politically responsible.

This complexity of attribution due to the anonymity of cyber operations presents additional legal and operational challenges in determining the legality of deterrence through nuclear weapons. Considering the nature of nuclear weapons as the epitome of weapons of mass destruction, there cannot be any uncertainty about the origin of a cyber attack.

Treaty law: The Non-Proliferation Treaty (NPT)

There is only one international treaty that requires nuclear states to pursue nuclear disarmament and prevent the spread of nuclear weapons: the Treaty on the Non-Proliferation of Nuclear Weapons (NPT).[11] All other legal frameworks dealing with arms control or disarmament are either defunct or have not been joined by nuclear-armed states. Using nuclear deterrence to prevent or respond to a cyber attack would thwart these objectives, as it broadens the conditions for the potential use of nuclear weapons. It might cause unnecessary escalation and undermine the NPT's goal of reducing the role of nuclear weapons. While not explicitly prohibited, using nuclear deterrence against cyber threats could be seen as contrary to the spirit of this treaty.

Legal-ethical and strategic considerations

The very essence of nuclear weapons lies in their indiscriminate nature and the disproportionate devastation they inflict, thus contradicting the legal and ethical imperative to mitigate harm to non-combatants. Cyber attacks, in the vast majority of cases, will not justify a reaction that has the potential to cause the deaths of millions. These ethical considerations are reflected in the humanitarian law principles of proportionality and discrimination.

Bringing nuclear deterrence into cyberspace could prove the stability-instability paradox right. This paradox suggests that while the threat of nuclear retaliation deters large-scale wars, it may encourage adversaries to engage in lower-level conflicts, assuming such actions would not provoke a nuclear response. Applying this concept to cyberspace, adversaries could (rightfully) interpret the nuclear deterrence threshold as high, encouraging cyber attacks that remain below that threshold. This dynamic could increase both the frequency and intensity of cyber conflicts.

Considering the challenging West-Russia relationship today, Russia has consistently demonstrated assertiveness in employing hybrid threats, including cyber attacks, as part of its broader geopolitical strategy.[12] Its diverse toolbox[13] includes interference in foreign elections,[14] large-scale disinformation campaigns,[15] and cyber attacks on critical infrastructure in Western states.[16] Unlike traditional military confrontations, these hybrid operations are often conducted in the "grey zone"[17] below the threshold of conventional armed conflict, making them difficult to attribute and respond to within existing legal frameworks.

In this context, nuclear deterrence faces a unique challenge. While it may deter direct, large-scale attacks, the nature of hybrid threats, especially those involving cyber attacks, allows adversaries to operate in this "grey zone" with easy deniability and test thresholds without crossing clear (legal) red lines. For instance, Russia's willingness to deploy sophisticated cyber tools, as demonstrated in the NotPetya attack,[18] highlights the limitations of conventional deterrence strategies. Even when such actions disrupt global systems or undermine national security, they often fail to trigger a response proportional to nuclear deterrence.

Moreover, relying on nuclear deterrence against cyber attacks holds a relatively high risk of escalation. Given the covert and fast-paced nature of cyber attacks, the odds of misattribution or misjudgement are significant. Russia, for example, has already demonstrated its willingness to exploit this uncertainty in the attribution process.[19] This could lead to a nuclear response being misdirected or unjustified. Such a scenario would not only violate international law but also further destabilise the global order.

The nature of hybrid threats, especially those involving cyber attacks, allows adversaries to operate in this "grey zone" with easy deniability and test thresholds without crossing clear (legal) red lines.

Towards a normative framework for cyber deterrence – without nuclear weapons

The reliance on nuclear deterrence as a countermeasure to cyber threats is loaded with legal, ethical, and strategic complexities that question its legitimacy and efficacy. International law, in particular the principles of proportionality and discrimination and the prohibition of the use of force enshrined in Article 2(4) of the UN Charter, might allow the deployment of nuclear weapons to

deter cyber attacks only in exceptional cases. International law imposes very high thresholds and prerequisites. Additionally, when assessing the legality of using nuclear weapons in cyber deterrence, some unsolved legal questions about traditional nuclear deterrence intertwine with unsolved legal questions about cyberspace, and so nuclear weapons do not serve as an effective cross-domain means of deterrence against cyber attacks.

From an ethical standpoint, the disproportionate effects of nuclear weapons do not align with fundamental moral principles. On a strategic level, using nuclear weapons as a deterrent against cyber threats poses the risk of heightening the potential for catastrophic confrontation and escalation.

Considering these practical and legal complexities, addressing cyber attacks requires a context-aware approach. This involves redefining existing international norms for cyberspace, improving attribution mechanisms (both technically and legally), and – above all – fostering resilience against cyber operations rather than expanding the scope of nuclear deterrence. Only by acknowledging the unique characteristics of hybrid threats, the international community can develop effective and legally sound strategies to counter them.

6 February 2025

References

1. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://unidir.org/files/2021-11/NRR-CyberNuclear.pdf&ved=2ahUKEwjP3tn__
2. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://static.rusi.org/cyber_threats_and_nuclear_combined.1.pdf&ved=2ahUKEwia16qLg5uKAxXaXvEDHYf6KN44ChAWegQIHhAB&usg=AOvVaw0dRsupqEi24d8NtnD-2qfb
3. https://www.orfonline.org/expert-speak/states-use-of-non-state-actors-in-cyberspace
4. https://www.chathamhouse.org/2023/10/why-stalling-npt-wake-call-global-security
5. https://www.britannica.com/topic/mutual-assured-destruction
6. https://ccdcoe.org/research/tallinn-manual/
7. https://www.un.org/en/about-us/un-charter/full-text
8. https://www.un.org/en/about-us/un-charter/full-text
9. https://www.icj-cij.org/case/95
10. https://eurepoc.eu/pl/publication/security-through-obfuscation-why-governments-use-proxies-in-cyber-conflicts/
11. https://disarmament.unoda.org/wmd/nuclear/npt/
12. https://www.nato.int/docu/review/articles/2024/04/26/russias-hybrid-war-against-the-west/index.html
13. https://frivarld.se/rapporter/tracking-the-russian-hybrid-warfare-cases-from-nordic-baltic-countries/
14. https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence
15. https://rusi.org/explore-our-research/publications/commentary/russia-winning-global-information-war
16. https://statescoop.com/russian-cyberattack-wastewater-tipton-indiana/
17. https://lieber.westpoint.edu/challenges-twilight-international-law/?utm_source=chatgpt.com
18. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
19. https://www.politico.com/news/2024/09/05/us-allied-nations-russia-cyberattacks-ukraine-nato-00177542?utm_source=chatgpt.com

Authors

Eleonora Neri, Project & Research Coordinator at the United Nations Office for Disarmament Affairs (UNODA)

Michael Biontino, Former Permanent Representative to the Conference on Disarmament and ELN senior network member

Jana Baldus, ELN Policy Fellow

Dr Caroline Fehl, Interim Professor of International Politics at Helmut-Schmidt Universität/Unversität der Bundeswehr Hamburg

Alexander Hoppenbrouwers, Research Intern at the Vienna Center for Disarmament and Non-Proliferation (VCDNP)

Nicholas Lokker, Researcher at the Centre for a New American Security

Rishi Paul, ELN Senior Policy Fellow

Nikita Gryazin, ELN Policy Fellow

Eva-Nour Repussard, Policy Fellow at BASIC

Verena Jackson, Lawyer & Researcher at University of the Armed Forces of Germany (UniBw)

The European Leadership Network (ELN) is an independent, non-partisan, pan-European network of over 450 past, present and future European leaders working to provide practical real-world solutions to political and security challenges.

Published by the European Leadership Network, April 2025.

European Leadership Network
8 St James's Square
London, SW1Y 4JU
United Kingdom

Email: secretariat@europeanleadershipnetwork.org
Tel: 0203 176 2555
Website: europeanleadershipnetwork.org

Follow us