Verification in an Era of Rapid Technological Change

FOCUS

Introduction: Verification in an Era of Rapid Technological Change

In the current security environment, only few arms-control-related treaties with formal verification regimes remain in place, and geopolitical tensions and power shifts require flexible approaches to old and new security problems. In this world, verification has to be understood in a broader and more inclusive way as it remains ever more crucial to keep producing reliable and internationally available knowledge on activities that could destabilize peace and security regionally or globally. New technologies can help improve these processes: by optimizing the remaining verification mechanisms of existing regimes, by enabling non-governmental actors to participate in OSINT-based knowledge production, and by ensuring that new, non-intrusive verification mechanisms are available when the international situation permits the establishment of new regimes. Artificial intelligence (AI) will play a particular role in this regard, as it has the potential to bring a new level of quality to the verification of arms control treaties in many areas. At the same time, however, the challenges must be considered. For instance, some new technologies may reveal unnecessary confidential or proprietary information and thus cross the line between necessary transparency and undue intrusiveness.

- **Support implementation of new technology in verification.** New technologies can advance current verification mechanisms, especially by increasing accuracy and reducing costs. They should also be considered when negotiating new or updating existing regimes – what was previously difficult to detect may become accurately verifiable.
- **Invest in an ecosystem for the development of verification technologies.** Tailored measures are necessary for a more effective transition of promising emerging technologies from basic research towards implementation. Here, a gap currently exists that should be closed.
- **Use new creative approaches to generate knowledge relevant to security policy.** Opportunities exist beyond the state-led verification methods practiced to date: e.g. less formal processes to gain a better understanding of compliance, or the provision of information by civil society and its integration into compliance assessments.

Beyond the Black Box: Conditions for Credible Use of AI in Verification

Artificial intelligence (AI) is increasingly being integrated into arms control, disarmament, and non-proliferation verification, offering new capabilities for processing large volumes of data, detecting anomalies, and supporting compliance assessments. However, concerns about the "black box" nature of AI have raised questions about the reliability of AI-supported verification. Explainability alone is not the decisive criterion; instead, the key challenge is whether AI systems can be designed and governed in a way that preserves credibility in a limited-trust environment. Reproducibility, integrity, transparency, decentralization, and robust security emerge as the central requirements for the credible use of AI in verification regimes.

- **Focus on credibility and reproducibility of AI.** The black box nature of AI should not prevent its use in arms control verification. For artificial intelligence to become a valuable verification tool, credibility and reproducibility should be treated as the primary design objectives.
- **Agree on standards.** The development of AI-supported verification systems should be guided by agreed standards for data integrity, transparency, reproducibility, and cybersecurity.
- **Enable independent validation.** Participating actors should be able to independently validate AI-generated results through shared datasets, transparent algorithms and procedures, and decentralized technical infrastructures.

Verification with Quantum Sensing

Quantum sensing is an advanced measurement approach that uses quantum mechanics to detect objects over long distances or in noisy environments. It could become relevant to verification where it can strengthen specific tasks, including testing declarations against observations, locating anomalies that warrant follow-up, documenting where and how measurements were taken, and gathering evidence without excessive intrusiveness. Its potential value is practical rather than transformative: more stable field measurements, more selective screening, and more reproducible inspection records. Cold-atom interferometry may support local gravimetry and inertial navigation; NV-center and atomic magnetometers may improve local magnetic-anomaly mapping; and nonlinear interferometers based on induced coherence can probe mid-infrared molecular fingerprints while using visible or near-infrared detection. None of these applications has yet been established in treaty inspections. Operational value will depend on a demonstrable advantage over mature instruments, workable measurement times, agreed data rules, and acceptance by the states and organizations involved.

- **Fund mission-driven validation.** Comparative field trials should be carried out, benchmarking performance against established classical instruments at represen-

tative sites, and testing false positives, false negatives, calibration stability, ruggedness, operator burden, and data protection requirements.

- **Prioritize bounded pilot cases.** Such pilot cases should include local gravimetry and magnetometry for anomaly mapping, quantum-assisted inertial navigation for GPS-denied inspections, and nonlinear-interferometer mid-infrared screening with visible or near-infrared readout for follow-up chemical analysis.
- **Define the verification question before deployment.** For any new instrument, the performance threshold, evidentiary role, managed-access safeguards, and approval route should be agreed.

From Images to Insights: Data Integration in Satellite Surveillance

Soon after the launch of Sputnik I in 1957, gathering information from space for national security purposes became a major driver of exploration of the "final frontier." Both nuclear superpowers, as well as an increasing number of other states, have invested heavily in satellite-based reconnaissance. However, the most recent developments in the fields of artificial intelligence (AI) and the fusion of data from various space-based observation technologies have the potential to take space surveillance to a new level, including, for example, the space-based detection of stealth assets. In addition, data fusion will enhance societal verification based on commercial satellites and private access to satellite images. Although these advances create new opportunities for verification, they also entail emerging risks. To fully assess the risks and opportunities associated with the use of satellite imagery, it is necessary to understand the current technological limits of the different technologies in use.

- **Invest in AI-enabled intelligence.** Strategic advantage increasingly depends on integrating and analyzing multisensor data rather than collecting imagery alone. Policymakers should prioritize AI, data fusion, and analytical capacity.
- **Maintain rigorous technology assessments.** National spectrum authorities, defense research organizations and the European Defence Agency (EDA) should ensure systematic and independent assessment of novel sensing technologies and emerging uses of the radio spectrum to determine their technical credibility, rate of development, and potential security implications, including the circumstances under which they could become strategically significant.
- **Review remote sensing policy.** Germany should reassess whether its National Data Security Policy for Space-Based Earth Remote Sensing Systems remains fit for purpose in an increasingly international commercial Earth observation market, and whether the current framework continues to effectively address national security objectives while preserving the scientific, commercial, and humanitarian benefits of commercial Earth observation.

Novel Particle Probes in Nuclear Verification

Nuclear energy is experiencing a global resurgence, including the development of novel advanced reactor designs and deployment concepts. Accommodating these innovations would require major modifications to existing nuclear safeguards as well as additional personnel. In light of this, researchers and academic institutions are exploring new nuclear verification techniques, with new non-destructive assay (NDA) approaches looking particularly promising for addressing future safeguards scenarios. These efforts build on advances in industrial technologies and ongoing research and development (R&D) in signal detection and data processing. Analyzing the evolution of frontier verification techniques enables us to identify common technological drivers and the approaches fueling their development.

- **Include nuclear verification in security-focused programs.** Governments should ensure that nuclear verification is included in their security-focused R&D funding programs and schemes, while simultaneously maintaining an emphasis on the civil security aspect, would foster trust through balance and transparency and promote collaborative innovation.
- **Recognize the benefit and impact of adapting basic physics research to verification applications.** Adapting innovations in detection technologies emerging from fundamental physics research has enabled novel tools forming the building blocks of new nuclear verification techniques – this spin-off benefit and impact needs to be more clearly recognized by academic institutions such as universities involved in fundamental research to support making such research attractive to scientists.
- **Support interdisciplinary research environments.** Sustaining innovation for verification purposes by providing continual support for interdisciplinary maturation environments is likely to be the most effective pathway for leveraging existing R&D efforts; however, while interdisciplinary funding and exchange is available, it often competes, to its detriment, in funding schemes with single-discipline focused research or trends.

Genetic Engineering Attribution: Contribution to Verification and Practical Limitations

Genetic engineering attribution (GEA) remains relevant to ongoing biosecurity and verification discussions. Recent work suggests that engineered biological material may contain detectable traces of design choices and laboratory practices. However, much of this progress relies on curated datasets, such as plasmid repositories, which differ

substantially from real-world incidents. Current methods may help with screening and narrowing down possibilities but using them for verification will require better data, more realistic testing, and careful interpretation.

- **Improve data standards for engineered biological sequences.** Biosecurity and attribution initiatives should support more consistent documentation of construct type, vector system, backbone, engineering method, and relevant depositor context in biological repositories and sequence databases.
- **Match real-world conditions in evaluations.** Research programs supporting GEA should prioritize testing under conditions closer to real-world incidents, including partial, degraded, mixed, or poorly documented samples, and distinguish engineering detection from source attribution.
- **Combine GEA with other methods.** Investigators and verification practitioners using GEA should interpret its results alongside epidemiological, environmental, and investigative evidence rather than as standalone proof.

Trust but Verify: Autonomous Spacecraft and the Verification Challenge

Satellite autonomy (the ability to operate and navigate with limited dependence on ground control) is simultaneously beneficial and risky. On one hand, it improves resilience, redefines in-orbit verification, and operational independence. On the other hand, it introduces new governance and security challenges. As fewer decisions can be directly attributable to human operators, it becomes harder to determine whether behavior is accidental, emergent, negligent, or deliberate. In contested orbital regions, autonomous rendezvous and proximity operations (RPO) could heighten mistrust and contribute to escalation between states. A key concern is the risk of miscalculation under conditions of uncertainty, particularly where strategic interpretation is already difficult. Existing governance frameworks and norms have not kept pace with technical capability, limiting their ability to effectively manage emerging autonomous systems.

- **Develop shared verification protocols and minimize ambiguity.** Verification-related maneuvers, trajectories, and approach velocities should be transparent and observable to minimize ambiguity and reduce perceptions of threat.
- **Establish open-ended working group for inspector satellites.** The UN First Committee could task an open-ended working group, in consultation with technical verification bodies such as the International Atomic Energy Agency (IAEA), with developing proposals for a fleet of internationally sanctioned inspector satellites.
- **Specify information barriers.** Space-faring states should establish agreed limits on verification sensors and inspection activities (information barriers) to ensure that orbital verification can be conducted without enabling intrusive surveillance.

What Cyberspace Regulation can Learn from Traditional Arms Control

Cyber operations are increasingly being used for military purposes, particularly in the context of hybrid warfare. However, no binding international regulatory framework for cyberspace currently exists. Drawing on the Chemical Weapons Convention (CWC), often described as one of the most successful arms control regimes, the regulation of cyberspace should focus less on specific technological applications and more on harmful behavior and contexts of use.

- **Focus on behavior and intent.** Cyber arms control should focus on regulating harmful behavior, intended effects, and context of use, rather than specific technological applications.
- **Establish an attribution mechanism for cyber attacks.** An independent but globally recognized attribution mechanism similar to stateless attribution practices proposed in the literature could become a practical alternative to traditional verification approaches in cyberspace.
- **Include soft law and norm building.** Since soft law instruments and norm building are likely to be prerequisites for future binding cyber arms control agreements, they should be included in approaches to regulate cyberspace.

Systems for Implementation Review

Systems for implementation review (SIRs) are international or regional institutions and mechanisms through which parties to a multilateral agreement share information on implementation, compare their implementation activities, review one another's performance, learn from implementation experience, address noncompliance or poor compliance, and, where useful, adjust their commitments. Experience has shown that the development and operation of SIRs can make important contributions to treaty or regime effectiveness, particularly for complex multilateral agreements. Systems for implementation review improve implementation and compliance by helping to mobilize timely international attention and expert responses to emerging problems or opportunities in national implementation of international commitments. They have proved particularly effective in the context of environmental agreements. Although SIRs operate across several multilateral arms control and disarmament regimes, they remain relatively unrecognized and are often inadequately developed. Greater focus on developing and using SIRs could help to improve the dynamism and effectiveness of arms control efforts.

- **Include SIRs in efforts to enhance multilateral arms control and disarmament agreements and soft law.** The German Foreign Ministry and its European Union

and international partners should devote greater attention to the development and more purposeful use of SIRs in their efforts to

- improve the dynamism and effectiveness of existing multilateral arms control and disarmament agreements, including the CWC, BWC, NPT, and humanitarian arms control agreements; and
- develop international codes of conduct and good-practice guidelines as part of their soft law approaches to promoting international cooperation on safety and security issues in outer space, as well as to limiting the risks posed by the use of cyber weapons and misuse of emerging technologies.

Societal Verification

With the widespread use and increasing accessibility of satellite imagery, societal verification, which assigns analysts outside the government–intelligence nexus a role in producing verification-relevant knowledge, has experienced renewed interest. The monitoring of North Korean nuclear facilities and the tracking of Iranian sites by non-state actors, including nongovernmental organizations (NGOs), think tanks, and independent researchers, illustrates how analysis produced by NGOs feeds into public debate and media coverage. Interviews with open-source intelligence (OSINT) analysts from NGOs and think tanks as well as government officials indicate that societal verification initiatives have two distinct effects: (1) informing the public about pressing security issues, thereby also releasing new information for government actors to use; and (2) stimulating and shaping domestic debates about security policies. Improved dialogue between non-state and governmental experts would help policymakers make better use of information produced by think tanks and NGOs. It could also help alleviate public fears and reduce reliance on worst-case assumptions by addressing the existing gap in reporting on threats and security issues that the intelligence sector and the government only reluctantly fill.

- **Dialogue between non-state actors and governments.** Non-state actors using OSINT and governments should intensify their dialogue to broaden debates and involve more stakeholders in the production of verification-relevant knowledge.
- **The verification-relevant knowledge produced by non-state actors should inform government actors in their decision-making.** Analyses produced by non-state actors provide additional perspectives and context for the public about policy impact and threat potential, at times taking a more critical stance than government releases.
- **Engagement between state and non-state actors should aim at increasing the credibility of future verification approaches and arms control policies.** This could also enhance public support for political measures.

TRENDS

Artificial Intelligence and Semiconductors – Key Developments Since 2025

Semiconductors are no longer merely an economic concern; they have increasingly become a matter of national and international security. Competition over artificial intelligence (AI) capabilities is closely tied to control over semiconductor supply chains, critical raw materials, and the infrastructures required to support advanced computing. Strengthening resilience across semiconductor ecosystems—including manufacturing capacity, energy provision, and international partnerships—has therefore become a key strategic objective for states and firms alike.

- German foreign policy should treat semiconductor supply chains and AI compute infrastructure as core issues of economic security and critical infrastructure protection.
- Germany and the EU should strengthen and diversify international partnerships across the semiconductor value chain, from critical minerals and manufacturing equipment to advanced chips and memory.
- International coordination should improve resilience against geopolitical disruptions by strengthening cooperation on supply security, export controls, and access to critical semiconductor and AI infrastructure.

AI in the Lab: From Biological Design to Biological Access Control

As artificial intelligence (AI) tools become increasingly important in the life sciences, the policy debate is shifting from general dual-use concerns to more practical questions of control, access, and implementation. This includes access to sensitive pathogen data, managed access to higher-risk biological AI tools, stronger nucleic acid screening, and deployment controls at frontier AI firms. The central policy question is how to govern access, oversight, and accountability before riskier capabilities become routine.

- The EU should support stronger and more consistent requirements for nucleic acid screening and customer verification across member states.
- National and EU frameworks should support managed access to higher-risk biological AI tools and sensitive pathogen datasets.
- International coordination should promote compatible standards for nucleic acid screening, biological AI governance, reporting, and evaluation.

Artificial Intelligence in Chemistry and Chemical Weapons Control: Fragmentation and the "Execution Gap"

Although artificial intelligence (AI) is advancing rapidly in chemistry, its application in research and its use in chemical weapons control remain fragmented and underregulated. While many models are being developed, they are rarely integrated into stable workflows. Meanwhile, the widespread availability of open-source and poorly secured tools is facilitating the discovery of novel synthetic routes and toxic molecules. Opportunities for verification, forensic analysis, and mission planning remain largely untapped. To preserve the strength of the Chemical Weapons Convention (CWC), closer alignment between technical capabilities and the policy framework is crucial.

- States and the Organisation for the Prohibition of Chemical Weapons (OPCW) should systematically monitor the application of AI in chemistry to identify and mitigate, at an early stage, the risks posed by fragmented and unregulated models.
- The OPCW and relevant national authorities should develop targeted capabilities for the operational use of AI in verification, analysis, and mission planning to narrow the current "execution gap."
- Developers, research institutions, and policymakers should work together to establish and enforce binding safeguards and access restrictions for particularly sensitive applications, such as toxic molecules, retrosynthetic planners and autonomous laboratories.

Scaling Disinformation with AI: A Threat for the Chemical Weapons Prohibition?

Agent-based, large language model-driven artificial intelligence (AI) can make disinformation more scalable, cheaper, and harder to detect. This undermines trust in institutions and democratic processes. This development has a particularly significant impact on chemical weapons control. The Organisation for the Prohibition of Chemical Weapons (OPCW) has long been the target of coordinated campaigns seeking to weaken accountability, institutional legitimacy, and governance structures. Traditional methods of detecting disinformation campaigns using bots are ineffective against new technical developments. Therefore, what is needed are resilient institutions capable of detecting attacks early, communicating transparently, and developing counterstrategies cooperatively, rather than relying on technical censorship measures.

- The OPCW should establish a monitoring and analysis framework to systematically track, assess, and address AI-enabled disinformation campaigns aimed at attacking its credibility.
- The organization and its member states should continue to promote proactive and transparent communication strategies that clearly explain the OPCW's procedures, mandates, and limitations. This will strengthen resilience against delegitimizing narratives.
- States, international organizations, platform operators, and AI providers should work together to develop methods for detecting AI-based "swarm" campaigns and implement coordinated measures to flag or mitigate such activities, particularly during sensitive events.

Innovation at Drone Speed—How the War against Ukraine is Shaping Future Warfare

Over the last two years, we have reported on the rapid development of drones in the war in Ukraine. This trend still holds true and has even developed more momentum. Major developments include, amongst others, the rising importance of counter-drones hunting other drones, the significant increase in uncrewed ground vehicles (ground drones) and the fact, that Ukraine has become a world leader in drone and counter-drone technology, changing from an importer of security to an international provider.

- Given the poor prospects for the international regulation of drone warfare and the dynamic trends of technological development, special attention must continue to be paid to drone defense, both in the military and the civilian spheres.

Mirror Life Moves from Warning to Governance Debate

Although no self-replicating mirror organism is known to exist, mirror life has become an active governance concern. Since last year's CNTR Monitor, UNESCO, the UN Scientific Advisory Board, UK officials, funders, and the Mirror Biology Dialogues Fund have advanced discussions on moratoria, precursor technologies, and safeguards. Recent synthetic-cell progress and debate about ecological constraints reinforce the need for targeted rules that prevent self-replicating mirror organisms while preserving lower-risk work on non-replicating mirror molecules.

- Governments and international scientific bodies should maintain a strong norm against creating self-replicating mirror organisms.
- Policymakers, funders, and research institutions should develop governance for precursor technologies that could make mirror organisms easier to build.
- Lower-risk work on useful non-replicating mirror molecules should continue under rules that clearly distinguish it from work toward self-replicating mirror organisms.

Technology Preferences of Six Military Innovator Countries: An Updated Analysis of Security Policy Technology Strategies

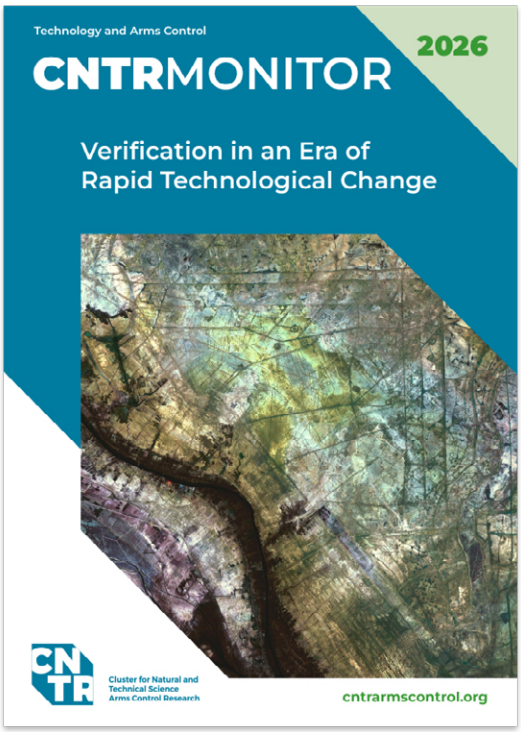
The nature of warfare is constantly and rapidly changing – and new technologies play a significant role in this. But which technologies have been, and continue to be, regarded by states as particularly significant in military terms? An analysis of strategy papers from six selected states between 2016 and 2025 shows that the further development of traditional conventional weapon systems is important alongside the development of new military technologies such as improved command and control systems, novel sensors, AI-based analysis and networking. In addition, there has been a growing interest in (ballistic) missiles, particularly in recent years. However, the analysis also reveals that discussions on future military technology vary greatly across the states analyzed. Whilst, for example, Australia engages in high-quality discussions both in terms of quantity and depth, Germany lags behind both in terms of the number of documents and the depth of their content.

- The increased interest in ballistic missiles is a cause for concern and should be discussed at an international level, initiated by the EU countries.
- An open discourse on military and military-technical orientation is appropriate in democracies and also serves to secure legitimacy. Consequently, those countries that have so far shied away from entering into such a discourse, including Germany's Ministry of Defense, should intensify it.

About the CNTRMONITOR 2026:

Rapid scientific and technological advancements may change the verification landscape of the future. Only few arms control treaties with formal verification regimes remain in place. Still, producing collective knowledge on activities that could destabilize peace and security remains crucial. The CNTR Monitor 2026 examines new opportunities for verification—with and without treaties.

Verification knowledge needs to be reliable and internationally accessible. New technologies can help improve existing verification regimes but also present novel challenges. By analyzing selected technologies and political shifts, the CNTR Monitor 2026 sheds light on the dynamics that shape verification in the new security environment.



Göttsche, M., Jakob, U., & Schörnig, N. (Eds.). (2026). *Verification in an Era of Rapid Technological Change. CNTR Monitor – Technology and Arms Control 2026*. PRIF – Peace Research Institute Frankfurt.

Authors: Philip Gasse, Malte Göttsche, Markus Gräfe, Owen Greene, Una Jakob, Abdullah Kasim Korkusuz, Anja-Liisa Krichbaum, Sarah McKee, Robin E.Möser, Luis Pazos Clemens, Helene Pleil, Lukas Rademacher, Thomas Reinhold, Kadri Reis, Christian Reuter, Yan-Jie Schnellbach, Niklas Schörnig, Adhitya Sekhar, Liska Suckau, Fabian Unruh

Gefördert durch:
Auswärtiges Amt
aufgrund eines Beschlusses des Deutschen Bundestages