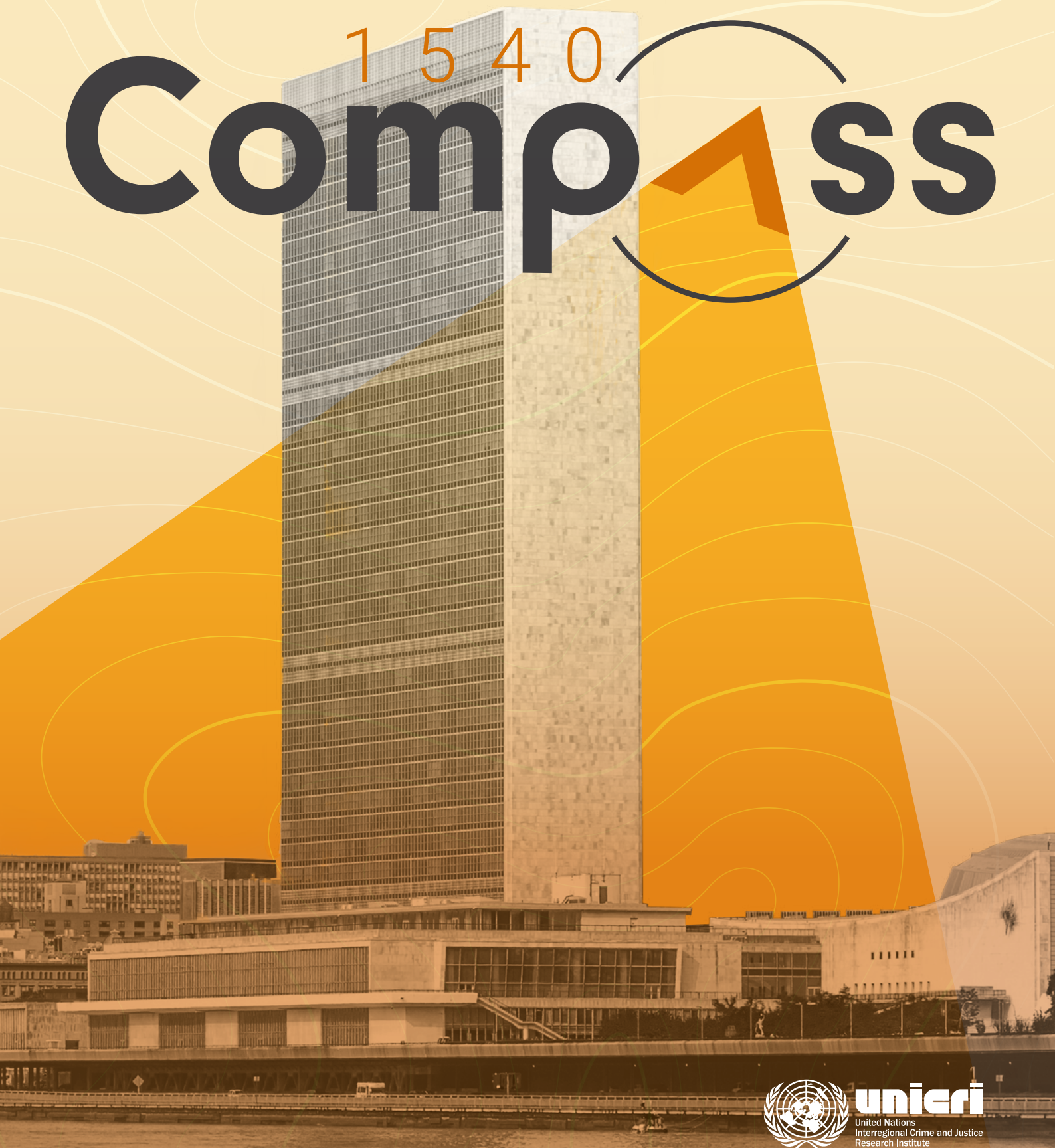


Issue **04**

MAY 2025

THE JOURNAL DEDICATED TO THE OBJECTIVES OF UNITED NATIONS SECURITY COUNCIL RESOLUTION 1540  
for preventing the proliferation of weapons of mass destruction by non-state actors

# 1540 Compass



**unieri**  
United Nations  
Interregional Crime and Justice  
Research Institute



© UNICRI 2024 | May 2025

THE JOURNAL DEDICATED TO THE OBJECTIVES OF UNITED NATIONS SECURITY COUNCIL RESOLUTION 1540  
for preventing the proliferation of weapons of mass destruction by non-state actors



# ACKNOWLEDGEMENTS

## EDITORIAL BOARD

**Francesco Marelli**, Editor-in-Chief | **Carlotta Zenere**, Programme Management Officer |  
**Katy Carroll**, Fellow

## BOARD OF ADVISORS

**Dr Karim Ben Ali**, Director, Technological Watch and Foresight Department, Military Research Centre, Tunisia | **Amanda Cowl**, Regional Coordinator for Asia and the Pacific, UNODA  
**Nicolas Kasprzyk**, European Diplomat, former 1540 Committee Expert | **Marcelo Martínez**, UNSCR 1540 Regional Coordinator, Inter-American Committee against Terrorism, OAS | **Dr Todd Perry**, Special Coordinator for UNSCR 1540, U.S. Department of State | **Dr Kiwako Tanaka**, Associate Professor, Toyo Eiwa University, former 1540 Committee Expert | **Dr Sarah Tzinieris**, Research Fellow, Centre for Science and Security Studies, Department of War Studies, King's College London | **Dr Andrea Viski**, Founder & Director, Strategic Trade Research Institute (STRI)

If you wish to submit a letter to the Editor to be published in a future issue of the journal, or for any other enquiries, please contact: [unicri-1540compass@un.org](mailto:unicri-1540compass@un.org)

You can find resolution 1540 in full [here](#).

If you would like more information about the work of the 1540 Committee, please see: <https://www.un.org/en/sc/1540/>

Volume 2, issue 1, published May 2025



# DISCLAIMER

---

The opinions, findings, conclusions, and recommendations expressed herein are those of the authors and do not necessarily reflect the views and positions of the United Nations and UNICRI, or any other national, regional or international entity involved. Contents of the publication may be quoted or reproduced, provided that the source of information is acknowledged. The designations employed and presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area of its authorities, or concerning the delimitation of its frontiers and boundaries.

In order to ensure the sustainability of the journal, the *1540 Compass* is looking for financial contributions from other Member States and international and regional organizations.

The *1540 Compass* was originally launched in 2012 by the Center for International Trade and Security (CITS) at the University of Georgia in hard copy format. Under the initial direction of Dr Igor Khripunov, and in cooperation with the UN Office for Disarmament Affairs, the *1540 Compass* was designed to provide an accessible forum on the effective implementation of UN Security Council resolution 1540. Back issues of the *1540 Compass* can be found at: <https://spia.uga.edu/departments-centers/center-for-international-trade-and-security-cits/publications/compass/>

# TABLE OF CONTENTS

## Note from the editor

Francesco Marelli

6

## Letters to the Editor

Caner Dereli

8

Jusu M. Ngobeh

10

## Special Features

Emerging technologies and UNSCR 1540

12

Germany's Biosecurity Blueprint: Three Projects  
Making a Difference

14

## INTERVIEWS



David Théard

16



Edith Valles

24

# ARTICLES

---

<b>Cybersecurity Challenges and Opportunities: UNSCR 1540</b> Ali Alkis	32
<b>UNSCR 1540 and Cybersecurity in the Fourth Industrial Revolution</b> Yasmin Hussien	38
<b>Leveraging Technology for UNSCR 1540 Implementation: The BWC National Implementation Measures Database</b> María Garzón Maceda	42
<b>Enhancing CBRN Risk Mitigation through Big Data</b> Louison Mazeaud	48
<b>The Role of Artificial Intelligence in Mitigating Insider Nuclear Security Threats and Strengthening UNSCR 1540</b> Shahneela Tariq	58
<b>Weaponized Intelligence: AI, Non-State Actors, and WMD Proliferation</b> Thomas Reinhold	64
<b>The Erlangen Initiative: Enhancing dialogue with academia to support the implementation of UNSCR 1540 (2004) worldwide</b> Alessa Mondorf	70
<b>Private Companies and Resolution 1540 (2004): A Complementary Pas de Deux</b> Bernard Galéa	76

# EVENTS AND NOTIFICATIONS

---

<b>Events</b>	82
<b>Notifications</b>	84

# NOTE FROM THE EDITOR



EDITOR-IN-CHIEF | 1540 COMPASS  
**Francesco Marelli**

UNICRI Head of Unit | CBRN Risk Mitigation and Security Governance

Dear Readers, Colleagues and Contributors,

Welcome to the first issue of 2025 and the fourth issue since the re-launch of the 1540 Compass in April 2024. Last year, we published three issues on themes central to United Nations Security Council resolution 1540 (UNSCR 1540), such as export controls, border controls, and measures to secure, account for, and physically protect sensitive materials and related items, as well as reflections on 20 years of 1540 implementation. Now, as we step into a new year, we turn our gaze to the future of resolution 1540.

In this issue, we focus on *UNSCR 1540 and Technologies: Challenges and Opportunities*. We examine how emerging technologies intersect with the obligations and aspirations of 1540. How does the resolution address these rapid developments? Turn to page 12 to see a timeline of how 1540 and successor resolutions deal with the evolving threat landscape. Following on from the last issue, which featured a special on the 1540 Group of Experts, our interview section includes conversations with two former experts, David Théard and Edith Valles, offering valuable insights into the evolving role of emerging technologies in 1540 implementation.

We are also pleased to bring you a rich collection of articles that touch upon this theme. In an increasingly digital world, cyberattacks have the potential to cause massive damage, especially when they intersect with the physical security of WMD materials. Yasmin Handy delves deeper into this novel threat dimension on page 38. Dr Thomas Reinhold looks at the risks associated with artificial intelligence (AI) in the context of weapons of mass destruction (WMD). Ali Alkis not only discusses cybersecurity vulnerabilities in the digital age, but also explores solutions presented by “innovative tools, such as AI, blockchain, and advanced encryption protocols.”

Many other authors in this issue focus on the solutions presented by emerging technologies. María Garzón Maceda discusses how technology can be leveraged for UNSCR 1540 implementation, and Louison Mazeaud reflects on how big data can contribute to non-proliferation efforts across the chemical, biological, radiological, and nuclear spectrum. Shahneela Tariq explores how AI can offer a “transformative approach to enhancing nuclear security measures”. Finally, Alessa Mondorf and Bernard Galéa discuss the importance of engaging academia and businesses in meeting 1540 obligations in their respective articles.

We also feature two thought-provoking letters to the Editor, one from Jusu M. Ngobeh, highlighting the influence of technology on WMD, and the other by Caner Dereli, who discusses the threat posed by fentanyl and its derivatives—an urgent and emerging chemical threat landscape.

As we look ahead to 2025, we invite you to join us in exploring how UNSCR 1540 can evolve alongside technological innovation. We encourage you to submit your research, reflections, and ideas for future issues—and we also warmly invite financial contributions to help sustain and grow this platform for critical discussion.

Thank you for your continued engagement and support. We look forward to another year of collaboration, innovation, and shared commitment to a more secure world.

Warm regards,

**Francesco Marelli**



# LETTERS TO THE EDITOR

Please send any letters to the Editor-in-Chief at [UNICRI-1540compass@un.org](mailto:UNICRI-1540compass@un.org)

Letters should not exceed 750 words



CBRN EXPERT, DISASTER AND  
MANAGEMENT AUTHORITY OF TURKEY  
**Caner Dereli**

Caner Dereli is a chemical engineer and CBRN specialist, working for Türkiye's Disaster and Emergency Management Presidency. He is also pursuing his PhD at Ankara University Institute of Forensic Sciences, Department of Criminalistics, on the use of fentanyl and its subgroups as weapons of mass destruction and the measures to be taken.

## **THE USE OF FENTANYL AND FENTANYL DERIVATIVES BY NON-STATE ACTORS: NEXT GENERATION CHEMICAL THREATS**

Dear Editor,

I am writing to address the emerging threat posed by fentanyl and its derivatives from a UNSCR 1540 perspective, and to emphasize the urgent need for stringent controls over these substances. UNSCR 1540 mandates that all States take effective measures to prevent non-State actors from acquiring and misusing materials that could be used as weapons of mass destruction. As a CBRN expert, I believe that fentanyl—widely used in medicine for its potent analgesic properties—presents unique challenges due to its high potency, low production cost, and ease of transport.

Fentanyl is a synthetic opioid, a meperidine congener of the phenylpiperidine series. It is a pure opioid agonist with a high affinity for the  $\mu$  receptor. It is about 75 to 100 times more potent than morphine as an analgesic. Fentanyl is very commonly used in anaesthetic practice owing to its high potency and quick onset and offset of action.

However, if used outside of a therapeutic setting and without medical supervision, fentanyl can be as dangerous as organophosphorus nerve agents. It is possible that terrorist organizations could use fentanyl and its derivatives in chemical terror attacks to achieve maximum damage and casualties.

There are two main scenarios in which fentanyl derivatives could be misused by non-State actors as weapons of mass destruction:

- 1. Aerosol dispersion:** Fentanyl derivatives could be dispersed as an aerosol in closed areas such as subways, airports, shopping malls, especially through central ventilation. Historical examples have demonstrated that fentanyl derivatives can cause mass deaths when sprayed in aerosol form in closed areas, highlighting their potential as weapons of mass destruction.
- 2. Contamination of food and water supplies:** Fentanyl derivatives could also be introduced into food or water supplies. In particular, the warehouses of large food suppliers could be contaminated. Fentanyl entering drinking water or food supply chains would lead to widespread poisoning. Poisoning scenarios could also be created in hotels, restaurants and public events, as with the salmonella attack during the Oregon state elections in the United States.

Although there is no documented case of fentanyl being used in a chemical attack, there are a number of instances demonstrating the misuse of lethal chemicals by non-State actors. The Tokyo subway sarin attack in 1995, for example, shows how chemical agents can be weaponized in urban settings. Equally, between 2015 and 2022, ISIS, a terrorist group, used chemicals such as chlorine and sarin to kill.

International law and regulatory frameworks already provide some level of control over chemical weapons. The Chemical Weapons Convention (CWC) prohibits the use of chemical agents for hostile purposes, but it does not classify fentanyl as a chemical weapon. However, UNSCR 1540 goes further by obliging States to implement robust national measures that secure dual-use materials like fentanyl, ensuring that they do not fall into the hands of terrorist groups or other non-State actors.

In conclusion, the low production cost, portability and lethality of fentanyl and its derivatives make them vulnerable to exploitation by terrorist organizations, organized crime networks and hybrid threat actors. Their use in closed-circuit attacks, assassinations and attacks on key infrastructures poses a significant threat.

In this context, the international legal framework needs to be strengthened, more effective border security measures implemented and drug control mechanisms improved. Technical and legal measures must be developed to prevent hostile actors from using fentanyl and its derivatives as weapons of mass destruction. This is a shared responsibility of security forces, health authorities and the international community. If effective preventative measures are not used, the widespread use of chemicals such as fentanyl will lead to the emergence of a new generation of chemical hazards.

*Caner Dereli*

# LETTERS TO THE EDITOR

Please send any letters to the Editor-in-Chief at [UNICRI-1540compass@un.org](mailto:UNICRI-1540compass@un.org)

Letters should not exceed 750 words



MEMBER OF THE SIERRA LEONE CBRN WORKING GROUP

**Jusu M. Ngobeh**

Jusu Ngobeh is a final year PhD student at the Department of Electrical Engineering at Parul University, India. He works as a Field Engineer with the Electricity and Transmission Company of the Ministry of Energy in Sierra Leone and is also a member of the CBRN working team.

## THE INFLUENCE OF TECHNOLOGY ON WEAPONS OF MASS DESTRUCTION

Dear Editor,

We live in an unprecedented world where technological advancement brings both progress and peril, increasingly challenging global security. We are frequently drawn into debates about whether science has done more harm than good. This noble discipline, while responsible for incredible innovation, is also linked to the development of destructive capabilities that have harmed humans, animals, and the environment—I remember that in my village we used ‘Gamalin 20’ in the river to kill aquatic animals for food. Such practices, alongside bioaccumulation and biomagnification, have led to significant ecological damage and human health risks.

Paradoxically, it is sometimes difficult to make a fair judgment with regard to technological advancement, especially when considering the impact of weapons of mass destruction (WMDs). The definition of WMDs remains contested, but within the UN Security Council framework, it typically refers to chemical, biological, and nuclear weapons—arms capable of causing mass casualties and widespread destruction. Undeniably, the proliferation and non-proliferation of weapons of mass destruction should be under control.

Recently, on a Training Course for National Points of Contact for United Nations Security Council Resolution 1540 (2004) in Africa held from 5 to 7 November 2024 in Addis Ababa, Ethiopia—in which I participated as a member of the CBRN working group of Sierra Leone—we discussed at length the challenges and opportunities related to WMD control. The UN will not be able to fully implement resolution 1540 (2004) if there is no bilateral and regional cooperation on non-proliferation of WMDs.

Technological advancement lies at the heart of modern weapon development. While technologies like AI, the internet, and cyber capabilities offer promise, their misuse—whether through cyber warfare, autonomous weaponry, or mass surveillance—poses serious risks. The UN Security Council must revisit and reinforce resolution 1540 (2004), ensuring stricter measures are in place to minimize both the proliferation and misuse of WMDs. Only through collective accountability, ethical technology governance, and international cooperation can we hope to secure a safer future.

I cannot conclude this letter without mentioning the senseless rebel war in Sierra Leone that has destroyed thousands of lives and property. Where did they buy the weapons and other arms? While preventing the proliferation of WMDs by non-State actors remains a critical global priority, for many countries—particularly in Africa—a more immediate and pressing threat is the widespread circulation of small arms and light weapons. In this context, international resolutions should not only address WMDs but also be strengthened to curb the production and transfer of small arms and light weapons, which continue to fuel regional conflicts and human suffering.

*Sincerely,  
Jusu M. Ngobeh.*

# EMERGING TECHNOLOGIES AND UNSCR 1540

While UNSCR 1540 (2004) itself does not explicitly mention emerging technologies, subsequent resolutions have increasingly acknowledged the evolving technological landscape and its implications for non-proliferation efforts. Most notably, resolutions 2325 (2016) and 2663 (2022) reflect growing international concern with regard to the impact that rapid advances in science and technology may have on non-proliferation.

2022

## UNSCR 2663 (2022)

Reinforces and expands the language introduced in UNSCR 2325. It repeats the concerns about the misuse of rapid advances in science and technology by non-State actors and again urges the Committee and Member States to factor in these developments. It also reflects a more routine inclusion of tech-related risks in the resolution's language, suggesting normalization of these concerns within 1540 implementation.

2022

## Comprehensive Review

This review continues the trajectory set in 2016 and further institutionalizes the routine monitoring of technological advancements. It emphasizes that the Committee should “**keep pace**” with dual-use technologies and innovation, and underscores the need for balance: facilitating peaceful technology use while guarding against proliferation.

FROM 2021

## UNSCR 2572 (2021), UNSCR 2622 (2022)

Procedural in nature and focused on mandate extension due to the COVID-19 pandemic, these resolutions do not discuss emerging technologies or related proliferation risks.







## FROM 2004

### UNSCR 1540 (2004), UNSCR 1673 (2006), UNSCR 1810 (2008)

These foundational resolutions focused on establishing and reinforcing the global legal framework to prevent WMD proliferation by non-State actors. However, they contain no reference to emerging technologies, rapid advances in science, or evolving threats.

2009

### Comprehensive Review

No direct mention of emerging technologies or rapid advances in science.

2011

### UNSCR 1777

This resolution marks the first **indirect acknowledgment** of emerging technological concerns. It calls on States to control “**intangible transfers of technology**” and “sensitive information” that could be used in WMD proliferation, hinting at the growing role of digital and scientific advances in facilitating such threats.

2012

### UNSCR 2055

No direct mention of emerging technologies or rapid advances in science.

2016

### Comprehensive Review

A major turning point. This resolution explicitly recognizes the risks posed by “**rapid advances in science, technology, and international commerce**”. It calls on States and the 1540 Committee to take account of the “**continually evolving nature of the risks of proliferation**” and specifically mentions intangible transfers of technology as a threat vector. This marks the formal integration of emerging technology concerns into the 1540 framework.

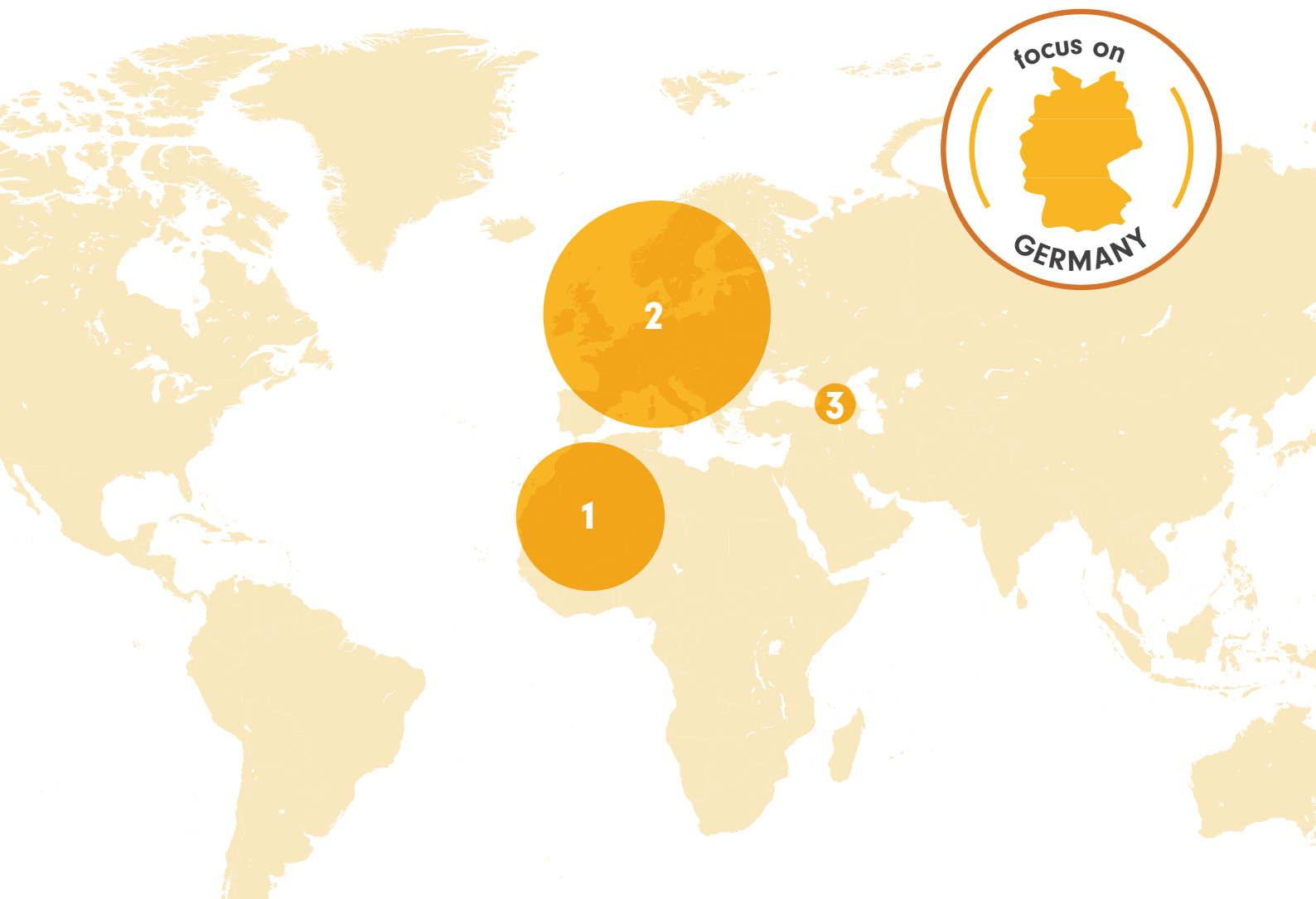


# GERMANY'S BIOSECURITY BLUEPRINT:

## Three Projects Making a Difference

Germany has been providing biosecurity assistance to partner countries around the world for over a decade through its flagship Biosecurity Programme, commissioned by the Foreign Federal Office. Germany provides this assistance through Article X of the Biological Weapons Convention, which promotes the exchange of equipment, materials, and scientific information for peaceful purposes. At the same time, these efforts align with the objectives of resolution 1540, which mandates that all States implement measures to prevent non-State actors from acquiring biological weapons. By enhancing global biosecurity capacities, Germany contributes to the resolution's goal of preventing the proliferation of biological weapons and related materials.

The Bundeswehr Institute of Microbiology (IMB), a military research facility based in Munich, has been part of the Biosecurity Programme since its inception in 2013. As a notable hub for research and knowledge in Germany and home to the annual Medical Biodefense Conference, the IMB is engaged in sharing its expertise through the programme, with hands-on training in both laboratory settings and the field. Read on to learn more about three projects the IMB has implemented in this area.



## 1. Strengthening biosafety & biosecurity capacities in the Sahel

Through the German Biosecurity Programme, the IMB has trained local specialists and equipped Mali, Mauritania, Burkina Faso, Chad, and Niger with mobile labs for safe, rapid response to outbreaks. These labs, designed for low-resource settings, help detect high-threat pathogens while promoting secure handling practices. By strengthening national capacity to manage dangerous biological materials, the project helps reduce the risk of their misuse—contributing to global non-proliferation and biological threat prevention efforts in line with UNSCR 1540.

## 2. Zoonotic disease risk management near the EU's border

Since 2022, this project has focused on rebuilding and expanding Ukraine's biosecurity structures in order to strengthen the response and resilience of Ukrainian security and health institutions to biological threats. This includes expanding the detection and diagnostic capacities of the Ukrainian partner laboratories in order to prevent destabilization of the country through the spread of diseases and epidemics or the potential misuse of highly pathogenic biological agents.

The training modules focus on the independent development and establishment of test systems for the detection of high-consequence pathogens. The test systems can be applied in routine diagnostics, biosurveillance studies and bioforensics. By enabling rapid and accurate identification of dangerous pathogens, these test systems can ensure that biological agents are not being misused by malicious actors.

## 3. Promoting biosafety & biosecurity in the Caucasus

The collaboration with the National Center for Disease Control and Public Health (NCDC) in Tbilisi, Georgia focuses on developing and validating test systems to expand the diagnostics spectrum. The test systems comply with international standards and can be used in routine diagnostics as well as for biosurveillance studies and bioforensics.

Since 2022, the IMB also closely collaborates with the Georgian Ministry of the Interior to strengthen biological reconnaissance and verification capacities in Georgia. The training includes risk assessment, bioforensic sampling, and rapid testing in realistic biological threat scenarios. In 2025, the NCDC will receive a mobile laboratory, developed and customized by the IMB, to investigate the cause and origin of disease outbreaks.

### USEFUL LINKKS

To explore how to request assistance via the 1540 Committee's matchmaking mechanism, visit: <https://www.un.org/en/sc/1540/assistance/general-information.shtml>

For guidance on seeking support under Article X of the Biological Weapons Convention, see: <https://bwc-articlex.unog.ch/>

INTERVIEW WITH:

# David Théard





## A Coordinator's View on 1540

When working to implement resolution 1540 (2004), the 1540 Committee have an ace up their sleeve: they can count on a diverse team of experts appointed to support them. As explored in the previous issue of the *1540 Compass*, the Group of Experts was formally established in 2011 by resolution 1977. Among other duties, they are responsible for sharing their knowledge on the resolution during outreach events, providing expertise to the Committee, preparing the 1540 matrices and contributing to the Comprehensive Reviews.

From the Group, one expert is selected by the Committee to act as the Coordinator, a role that our interviewee, David Théard, recently held. After gaining significant experience at the French Ministry of Defence and the French Atomic Energy Commission, Mr Théard was nominated to join the Group of Experts in 2020, before becoming its Coordinator in 2022. Over the course of his four-year mandate,, Mr Théard worked alongside experts from a wide range of fields, including international law, export controls, and nuclear, chemical, and biological (NCB) weapons, something he saw as “essential for addressing the broad spectrum of non-proliferation issues.”

In this interview, Mr Théard reflects on his time with the Group, providing insight into how implementation of resolution 1540 (2004) can be both a security imperative and a strategic opportunity for States, especially those looking to attract investment through strong regulatory frameworks. He also touches upon the theme of this issue of the *1540 Compass*: emerging technologies. For Mr Théard, while they represent a major challenge, they also offer opportunities to improve implementation of resolution 1540, “particularly in the area of information management aimed at detecting proliferation activities or attempts”.

Looking ahead, Mr Théard underscores the need for sustained commitment to non-proliferation efforts. His reflections serve as a compelling reminder of the critical role experts play in fostering dialogue, building trust, and strengthening the global non-proliferation regime.



**Can you tell us more about your area of expertise and how it complemented the Group of Experts? How are experts selected to support the Committee?**

By resolution 1977 (2011), the Security Council requested the Secretary-General, in consultation with the 1540 Committee, to establish a group of up to eight experts—later expanded to nine—who would act under the Committee’s direction. These experts are selected based on their relevant experience and knowledge to assist the Committee in fulfilling its mandate. The Committee also considers recommendations regarding expertise requirements, geographic representation, and working methods.

As an expert from 2020 to 2024, I worked alongside specialists from diverse backgrounds, including international lawyers focused on arms control, including non-proliferation treaties, export control officers, and technical experts on nuclear, chemical, and biological (NCB) weapons and their delivery systems. My own background is in nuclear and ballistic non-proliferation at the French Ministry of Defence and the French Atomic Energy Commission, with prior experience at the French Ministry of Foreign Affairs in international cooperation for peaceful purposes, such as scientific education, technologies and industry.

I was consistently impressed by the high level of expertise within the group, which was essential for addressing the broad spectrum of non-proliferation issues. The geographic and linguistic diversity of experts also played a crucial role in fostering cultural proximity with Member States, facilitating dialogue, and supporting implementation of resolution 1540 (2004).

**How does the 1540 Committee benefit from the support of the Group of Experts?**

The Group of Experts supports the Committee in two key ways. First, it provides continuous support throughout the Committee’s annual programme of work—the schedule that instructs the Committee’s activities for the year ahead. This support includes providing briefings on Member States’ implementation of resolution 1540 (2004), facilitating assistance requests, engaging with relevant international, regional and sub-regional organizations, conducting outreach, and updating the 1540 Committee matrices. These matrices track implementation progress and are comprehensively reviewed approximately every five years, with the next review scheduled for December 2027 under resolution 2663 (2022). The group also contributes to annual and periodic reports to the Security Council and collaborates with other counterterrorism Committees.

Second, the experts conduct visits to Member States on behalf of the Committee to support implementation efforts. These visits help facilitate dialogue and provide assistance tailored to each country’s needs. Under the Committee’s guidance, experts can assist States to conduct peer reviews and outreach to diverse national stakeholders.

Personally, I believe the expertise of the Group of Experts could be leveraged more actively, particularly through informal initiatives that support Member States’ efforts. While the Committee’s cooperative approach is valuable in maintaining trust and avoiding interference in national affairs, I believe many States would welcome more proactive engagement.

**I was consistently impressed by the high level of expertise within the group.**

**Can you provide an example of a time when the Group of Experts helped a State overcome a challenge?**

Rather than focusing on a single case, I would highlight common challenges many Member States face in implementing resolution 1540 (2004). For many States, resolution 1540 (2004) remains complex, particularly in terms of its relevance for their country if they lack advanced NCB industries. However, I have yet to meet a State for which resolution 1540 (2004) is not relevant: I think every country, at diverse levels, handles nuclear, chemical, and biological related materials in sectors such as agriculture, mining, automotive production, textiles, and cosmetics.

Another challenge is coordination among various national stakeholders, including policymakers, regulators, customs officials, and law enforcement. Additionally, legislative priorities often place other more pressing security concerns, such as small arms proliferation, ahead of weapons of mass destruction (WMD) non-proliferation.

In this context, the Committee offers essential tools to support implementation, particularly through its assistance mechanism. Acting as a matchmaker, it connects States requesting help with relevant providers, including 20 international, regional and subregional organizations and 46 Member States—I encourage States to make use of this tool. The Committee's website provides more information about this mechanism and how to request assistance.

Another tool used by the Committee is outreach aimed at raising awareness among Member States and fostering continuous dialogue. I have sometimes encountered Member States that became aware of the risk that their territory could be used by non-State actors for proliferation-related activities, including through proliferation financing and related services. Imagine the potential impact on a country's international image if its territory is misused in this way.

On the other hand, I have also seen States recognize opportunities in implementing resolution 1540 (2004)—including the potential economic benefits for countries seeking to attract foreign investment. Compliance with international regulatory instruments demonstrates that a country's industry is well-regulated, which can, in turn, draw investors. This is particularly relevant for countries that serve as corridors for international transportation, such as those involved in transit and transshipment.

From the perspective of resolution 1540 (2004), I see these potential benefits as additional incentives—beyond the primary goal of building a safer world in which Member States both contribute to and rely on the implementation efforts of others.

**What has been the overall impact of the 1540 Committee and its Group of Experts on global non-proliferation efforts over the past 20 years?**

Resolution 1540 was adopted unanimously in 2004 in the context of the September 11 attacks of 2001. At that time, the world was terrified that terrorist organizations such as Al-Qaida might use WMDs; remember that anthrax envelopes were subsequently sent to US officials and, a few years before, in 1995, the cult movement Aum Shinrikyo had perpetrated a chemical terrorist attack in the Tokyo subway. The Security Council recognized gaps in the international security framework and acted to prevent non-State actors from acquiring nuclear, chemical and biological weapons and their means of delivery.

Since then, follow-up resolutions have reinforced 1540's provisions, with resolution 2663 (2022) extending the Committee's mandate for another decade. This reflects the Security Council's impressive insight, as they noted in the preamble of resolution 1673 (2006), which recognized that the full implementation of resolution 1540 (2004) by all States—including the adoption of national laws and measures to enforce them—is a long-term undertaking requiring sustained efforts at national, regional, and international levels.

The Security Council's continued efforts have, in my view, produced positive results. Between

2016 and 2022, implementation of resolution 1540 advanced by six percent, reaching 56 percent of all possible measures required under the resolution. This progress is documented in the 2022 Comprehensive Review on the Status of Implementation, publicly available on the 1540 Committee's website. While much work remains for many Member States—often with the Committee's support—I remain optimistic. In my experience during my engagements with Member States, awareness of the resolution's importance continues to grow.

Finally, we should not overlook the value of international cooperation in achieving shared goals. This aligns with operative paragraph 9 of resolution 1540 (2004), in which the Security Council calls on all States to promote dialogue and cooperation on non-proliferation to counter the threat posed by the spread of nuclear, chemical, and biological weapons and their means of delivery.

**Resolution 2663 (2022) highlights “rapid advances in science, technology and international commerce” as threats to non-proliferation. What measures can States take to mitigate these risks?**

Rapid advances in science and technology, combined with the growing complexity of international commerce, represent—in my view—one of the most significant challenges for the future. These developments are not only progressing rapidly but are also becoming increasingly accessible to the public. For example, DNA biotechnology is offering new ways to create novel pathogens; 3D printing is enabling the production of equipment that could be used in weapon manufacturing processes;

and artificial intelligence is opening pathways to alternative methods for producing weapons or components that may not yet be included on current control lists. These are just a few of the emerging challenges in the effort to counter proliferation.

In my opinion, this evolving threat must be addressed by Member States, with support from the 1540 Committee as well as relevant international, regional, and sub-regional organizations. The Committee plays a vital role in raising awareness and sharing experiences and good practices, including through its website. It also promotes dialogue among States—for instance, through voluntary peer reviews, where two or more Member States agree to work together on implementing resolution 1540 (2004), using the Committee's matrices, which are updated nearly every five years, as a basis for assessing implementation.

I believe additional cooperation among Member States is essential, including through intelligence sharing to detect proliferation activities or intentions by non-State actors. Effective national responsibility over border and export controls not only reinforces mutual confidence but also strengthens collective security. Notably, resolution 1540 (2004) emphasizes export controls rather than import controls—an approach that reflects the Security Council's vision of mutual security, where a State's safety is bolstered by the preventive measures taken by others.

**This issue of the 1540 Compass is not only focused on the challenges posed by emerging technologies, but also the opportunities. How can emerging**

**technologies help States implement resolution 1540 more effectively?**

I'm glad you asked me this question, because it gives me the opportunity to clarify that resolution 1540 (2004) should not be viewed as a tool intended to restrict the development of Member States or the growth of international trade in emerging technologies.

To respond to your question, let's consider the issue of terrorism. I am convinced that States will continue to hold a strategic advantage over non-State actors when it comes to leveraging new technologies—particularly in the area of information management aimed at detecting proliferation activities or attempts. States will be able to harness increasing computational power, combined with the development of specialized algorithms, to achieve this objective.

Although emerging technologies are becoming more widely available in the public domain, Member States are likely to employ artificial intelligence with growing levels of anticipation and precision, enabling them to stay ahead of potential threats.

**What key lessons or insights would you share with future coordinators and experts supporting the 1540 Committee?**

I would first like to say that it has been an honour and a pleasure to coordinate the Group of Experts throughout 2023 and 2024, up to the end of my mandate, under the direction of the 1540 Committee. I had previously gained valuable experience as an expert myself, under the coordination of my predecessor.

Referring to paragraph 5(a) of resolution 1977 (2011), the Committee, in its report on recommendations regarding the structure, methods, modalities, expertise, and representation of the Committee and its Group of Experts (S/2011/819, annex), recommended that the Secretary-General, in consultation with and with the prior consent of the Committee, appoint a Coordinator to oversee and coordinate the activities of the other experts.

It is important to emphasize that the Coordinator is not the head of the Group—an approach I fully support, as it ensures that each expert's contribution is respected and valued. It is essential for experts to share not only their technical knowledge and professional experience, but also their regional perspectives and cultural insights. This exchange enhances the Group's ability to support the Committee effectively and to identify the most appropriate strategies and dialogues to assist Member States in implementing resolution 1540 (2004).

The Coordinator also plays a vital role in facilitating interaction between the Group of Experts and the Committee. One of the Coordinator's core responsibilities is to create an environment that encourages constructive dialogue within the Group, to help build consensus on various issues, and to accurately reflect those views to the Committee. Equally important is the need to foster trust between the Group and each Committee member. In this regard, it is crucial to provide the Committee with neutral, technical solutions that can help navigate differing political perspectives, where appropriate.

A strong relationship with the Chair of the Committee is, of course, essential. I would like to express my sincere thanks to the Ecuadorian Chairmanship for the high quality of engagement and collaboration with the Group of Experts during my mandate as Coordinator of the Group. I would also like to express my gratitude to the 1540 teams within the United Nations Office for Disarmament Affairs and the United Nations Department of Political and Peacebuilding Affairs, which are mandated to support the Committee's work. I believe that effective interaction with these entities is highly beneficial to the successful implementation of resolution 1540 (2004).

In closing, I would like to thank my fellow experts with whom I had the privilege to work. The diversity of expertise and the multicultural approach within the Group are, in my view, great assets and key to collective success. I strongly encourage the next generation of experts to uphold and actively nurture this spirit. Experts are a valuable technical resource, and I encourage all United Nations Member States to make full use of their knowledge and dedication.



A large, stylized orange opening quotation mark is positioned at the top left of the text block.

**I am convinced that States will continue to hold a strategic advantage over non-State actors when it comes to leveraging new technologies—particularly in the area of information management aimed at detecting proliferation activities or attempts.**

A large, stylized orange closing quotation mark is positioned at the bottom right of the text block.

INTERVIEW WITH:

# Edith Valles



## From the Laboratory to Global Impact

When it comes to the implementation of resolution 1540 (2004), the importance of regional expertise cannot be overstated. During her time with the Group of Experts, Edith Valles offered a key perspective on what the national implementation of resolution 1540 looked like across Latin America, while also contributing more than two decades of experience in chemical and biological weapons non-proliferation. She also had a strong foundation in outreach, technical assistance, and interagency coordination, having helped shape Argentina's national reporting under the Biological Weapons Convention and resolution 1540.

In this interview, Ms Valles shares reflections on her time with the Group, from conducting outreach in regions new to her professional experience, to revising 1540 matrices during the pandemic. She offers her perspective on the specific non-proliferation challenges faced by Latin American countries—such as under-resourced enforcement, limited technical capacity, and low perceived threat levels—and how these possibly lead to “a reactive rather than proactive approach” to non-proliferation, which make it “difficult to justify investments in regulatory and enforcement mechanisms”. Nevertheless, she also highlights how, in recent years, with the support of the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS), Latin American Member States have been taking meaningful steps to comprehensively implement resolution 1540.

With a focus on the theme of this issue—emerging technologies—Ms Valles discusses the dual-use nature of biotechnology, the importance of biosecurity safeguards, and the role of both regulation and education in mitigating proliferation risks. Her insights reinforce the value of regional leadership, interdisciplinary expertise, and sustained outreach as key pillars of effective resolution 1540 implementation.

### Can you tell us more about your career journey that led you to join the Group of Experts?

I have been working on biological and chemical non-proliferation issues for 20 years. My career began at the Institute of Scientific and Technological Research for Defence, part of Argentina's Ministry of Defence, where I obtained my PhD in Toxicology.

Following the events of 2001—first the attacks on the Twin Towers and later the mailing of *Bacillus anthracis* spores through the US postal system, which deeply impacted the international security community—the Argentine government decided to strengthen its capabilities in the non-proliferation of biological weapons. In response, I joined the institute's section responsible for implementing international non-proliferation agreements.

In this role, I was responsible for drafting technical reports on items subject to export controls under the Australia Group and contributing to the preparation of Argentina's 1540 National Reports and Biological Weapons Convention Confidence-Building Measures.

Additionally, we launched a proactive awareness-raising campaign on the dual use of life sciences, dual-use research, responsible science, and research security, among other key topics. I also collaborated with the National Authority for the Chemical Weapons Convention in designing outreach campaigns for the industrial sector and developing train-the-trainer programmes for academia to enhance awareness of the dual use of chemistry.

I provided technical advice on chemical and biological weapons related matters to both the Ministry of Defence and the Ministry of Foreign Affairs and was part of the Argentine delegation to the Australia Group meetings. I also participated in various national, regional and international forums related to non-proliferation of WMDs and security and co-authored several papers on biological weapons and biosecurity.

As part of my work, I trained enforcement personnel from Argentina and the region in Commodity Identification Training after receiving instruction through the U.S. EXBS Program, and I received training to respond to and investigate the alleged use of chemical and biological weapons.

In addition, before joining the Group of Experts, I was a member of the Advisory Board on Education and Outreach of the OPCW, a position I resumed this year and will hold until 2027.

### Reflecting on your time in the Group of Experts, can you describe an impactful workshop or event that you participated in?

My tenure at the Group of Experts was affected by the pandemic, and we were unable to conduct in-person missions for an extended period due to travel restrictions, which significantly impacted our activities. But, during that time, we were extremely busy revising the matrices assigned to us as part of the Comprehensive Review.

Regarding the most significant experiences for me, I perfectly recall the 1540 Point of Contact trainings we conducted in Russia and China. These were my first opportunities to engage with audiences from Eastern Europe and Asia, offering a unique chance to interact with

diverse perspectives and cultures, refine my communication approach, and gain a deeper understanding of regional security concerns and non-proliferation challenges.

**What unique non-proliferation challenges do you see in Latin America, and how can your region's experiences inform global best practices under UNSCR 1540?**

Latin America faces several challenges in implementing robust non-proliferation measures, despite its commitment to international treaties such as the NPT, CWC, and BWC. Many countries struggle with capacity gaps in enforcing these agreements due to a lack of technical expertise, scarce funding, and competing national priorities. Even when there is interest in strengthening non-proliferation policies, resource constraints hinder the effective implementation of export controls, border security, and dual-use material monitoring. Additionally, bureaucratic hurdles and low political motivation, often driven by the absence of immediate security threats, further weaken enforcement. While some countries have adopted necessary laws, institutional inertia, poor interagency coordination, and competing demands, such as economic development and public security, continue to impede progress.

The low perceived threat level in the region exacerbates these challenges. With no history of nuclear weapons programmes and minimal exposure to chemical, biological, or nuclear terrorism, many Latin American governments do not prioritize WMD proliferation risks. This perception leads to a reactive rather than proactive approach, making it difficult to justify investments in regulatory and enforcement mechanisms. At the same time, illicit trafficking and dual-use concerns remain significant issues

due to porous borders and complex supply chains that could be exploited for smuggling WMD-related materials. The growing use of dual-use technologies in industries and research further raises concerns about their potential misuse.

**Bureaucratic hurdles and low political motivation, often driven by the absence of immediate security threats, further weaken enforcement.**

Another pressing challenge is the weak engagement of industry and academia in non-proliferation efforts. Many scientific, industrial, and academic communities in the region have limited awareness of dual-use research concerns and WMD proliferation risks. Without strong outreach initiatives, private sector actors



and research institutions may unintentionally contribute to proliferation threats. Moreover, transnational criminal organizations operating in Latin America pose additional security risks, as they could potentially engage in trafficking WMD-related materials. Strengthening law enforcement cooperation and export control mechanisms is crucial to mitigating these threats.

Addressing these challenges requires a comprehensive approach that includes capacity-building initiatives, stronger regulatory frameworks, and enhanced collaboration between governments, industries, and the scientific community. By improving enforcement mechanisms, raising awareness, and prioritizing non-proliferation efforts alongside other national security concerns, Latin America can take meaningful steps to reduce the risks associated with WMD proliferation and dual-use technology misuse.

Since 2017, the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS) has hosted the Regional Coordinator for the implementation of United Nations Security Council resolution (UNSCR) 1540 (2004). CICTE supports OAS Member States in strengthening the resolution's implementation at the regional level.

Recent CICTE projects assisting OAS Member States have focused on strategic trade controls and the implementation of biosecurity measures in facilities handling high-consequence pathogens. As part of these initiatives, CICTE encourages Member States to share their experiences both within the region and globally. For example, when assisting States in drafting 1540 National Action Plans, CICTE encourages them to submit their

plans to the 1540 Committee. Likewise, during peer review processes organized among States, participants are urged to share their insights with the 1540 Committee.

“

**Transnational criminal organizations operating in Latin America pose additional security risks, as they could potentially engage in trafficking WMD-related materials.**

”



Additionally, the international community is kept informed about regional achievements through CICTE-organized side events, such as those held in the margins of First Committee meetings and Biological Weapons Convention (BWC) conferences. These engagements help highlight the region's contributions to the global non-proliferation and security framework.

**This issue of the 1540 Compass is focused on emerging technologies. In your view, what steps could States take to balance innovation in fields such as biotechnology with robust safeguards to prevent misuse?**

The dual-use nature of biotechnology and its widespread applications make it particularly challenging to implement robust safeguards. This challenge is further heightened by the fact that many facilities in the region—and, more broadly, around the world—lack effective biosecurity measures, even in environments where high-consequence pathogens are handled. To genuinely safeguard biotechnology from potential misuse, it is essential not only to establish such measures based on international standards, but also to formally regulate them.

Given the characteristics of the life sciences community, education plays a key role in promoting biotechnology safeguards. Raising awareness about the dual-use nature of these technologies is a fundamental step toward fostering a culture of responsibility. Establishing oversight committees at both institutional and national levels can also be an effective approach. These committees can regulate synthetic biology, genome editing, and other cutting-edge technologies, while assessing the risks associated with biological research projects.

Additionally, clear guidelines for dual-use research, including mandatory risk assessments for emerging biotechnologies, can further strengthen biosecurity frameworks. Another important measure is the implementation of national oversight on research funding, ensuring that grants prioritize responsible innovation when supporting dual-use biotechnologies.

Although soft law measures contribute to biosecurity, they may be perceived as insufficient. At the same time, implementing hard law to safeguard emerging biotechnologies presents several challenges. For instance, one major difficulty is that biotechnology evolves at a much faster pace than regulatory frameworks can adapt. New techniques, such as CRISPR gene editing, synthetic biology, and AI-driven biotechnologies, develop at a rate that often surpasses traditional legislative processes. This makes it difficult to establish long-term regulations without inadvertently restricting innovation. Furthermore, regulatory agencies may lack the specialized expertise needed to effectively evaluate the risks and benefits of these interdisciplinary advancements.

Uncertainty surrounding the long-term consequences of technologies like human genome editing and synthetic biology also complicates regulation. Policymakers must strike a delicate balance between precautionary measures and avoiding unnecessary restrictions on beneficial research. Additionally, resistance from industry and the scientific community must be considered, as overly restrictive legislation could hinder scientific progress. Lastly, even when regulations are in place, many countries face significant challenges in enforcement due to limited infrastructure, insufficiently trained

personnel, and inadequate funding. Addressing these gaps is essential for ensuring that safeguards are not only well-designed but also effectively implemented.

**Dual-use research in biotechnology is increasingly relevant due to proliferation concerns. Could you discuss how emerging biotech research might inadvertently contribute to proliferation risks, and what regulatory or technical measures may help to mitigate these risks?**

We know that rapid advances in bioscience and bioengineering, while offering revolutionary advancements in medicine, agriculture, and industry, can inadvertently contribute to proliferation risks in several ways. Considering the emergence of a successful global bioeconomy and the fact that these revolutionary technologies become more accessible—partly due to machine learning advancements that push the boundaries of innovation and make once-specialized knowledge more widely available—their dual-use potential and vulnerability to unforeseen consequences could pose entirely new risks.

Some key concerns may include the advances in synthetic biology and gene editing. For example, techniques able to allow precise genetic modifications, while beneficial for disease treatment, could also be exploited to enhance the virulence or transmissibility of pathogens. Furthermore, the ability to synthesize entire genomes or modify microorganisms raises concerns about the potential recreation of eradicated pathogens or the enhancement of the pathogenicity of existing ones.

In terms of the use of artificial intelligence tools, they are increasingly being used to predict

protein structures, design synthetic molecules, and optimize biological pathways. While these tools, for example, accelerate vaccine discovery, they could also be misused to engineer novel toxins or pathogens. Automated DNA synthesis and lab automation lower the technical barriers, making it possible to conduct sophisticated experiments with potential dual-use implications. However, while these technologies are becoming more widely accessible, tacit knowledge remains essential for their effective use.

Some efforts aimed at reducing the risk of misusing synthetic biology involve screening processes implemented by certain companies that sell benchtop DNA synthesis devices and process DNA orders.

For example, the International Gene Synthesis Consortium (IGSC) is an industry-led group of gene synthesis companies and organizations that has established a common screening protocol. This protocol is designed to examine both the sequences of synthetic gene orders and the customers who place them, helping to prevent unauthorized access to potentially hazardous genetic materials. Similarly, the International Biosecurity and Biosafety Initiative for Science (IBBIS), provides tools to safeguard biotechnology. One of their key initiatives is the International Common Mechanism for DNA synthesis screening, which enables DNA providers to screen synthesis orders for potential security risks.

These types of screening measures play a crucial role in mitigating the global risks associated with DNA synthesis misuse, particularly in the absence of a comprehensive international regulatory framework for DNA synthesis screening. By promoting self-regulation and

industry-wide best practices, these initiatives help strengthen biosecurity and prevent the inadvertent or deliberate proliferation of harmful genetic materials.

**Finally, what do you consider the most significant legacy of resolution 1540, and how should future Committee members build on this foundation to tackle emerging challenges?**

I consider that the most significant legacy of the resolution was to fill gaps that the other non-proliferation instruments did not consider. Thanks to resolution 1540, issues like accountability, security measures, and physical protection for related materials, which are not covered by either the NPT, the CWC, or the BWC, are now controlled in many States worldwide, reducing the risk of misuse. Additionally, matters related to export controls and the financing of nuclear, chemical, and biological weapons proliferation, as well as their means of delivery, are obligations under resolution 1540 that are not addressed by those instruments.

For all these reasons, I consider resolution 1540 a cornerstone of the global non-proliferation architecture, as it extends beyond State-to-State obligations and imposes legally binding responsibilities on all UN Member States to prevent non-State actors from acquiring weapons of mass destruction. By mandating national implementation measures, strengthening international cooperation, and promoting assistance programmes, the resolution has significantly contributed to reducing proliferation risks.

Moving forward, future 1540 Committee members should build on the resolution's

foundation, adapting strategies to address evolving threats and emerging technologies, while strengthening global cooperation and enforcement mechanisms. All these will be crucial in ensuring its effectiveness in an evolving global security landscape. Future 1540 Committee members will face complex challenges, including the rapid advancement of biotechnology, artificial intelligence, and cyber capabilities, which may lower barriers for illicit WMD proliferation. Additionally, ensuring uniform implementation across diverse national systems, addressing gaps in export controls, and strengthening private-sector engagement will require sustained political will and resources. However, with a commitment to innovation, capacity-building, and multilateral collaboration, resolution 1540 will remain a vital instrument in preventing WMD proliferation, reinforcing global security, and adapting to new threats in the years to come.



# CYBERSECURITY CHALLENGES AND OPPORTUNITIES: UNSCR 1540

*Cybersecurity has emerged as a new area of concern; Credit: Adi Goldstein.*

## ABSTRACT

Recent digital transformation has increased cybersecurity challenges by introducing new vulnerabilities. Such vulnerabilities could be exploited to undermine the objectives of UNSCR 1540. This paper examines how cyber threats—ranging from sophisticated hacking and ransomware attacks to weaknesses in digital supply chains and financial systems—pose significant risks to counter-proliferation efforts against weapons of mass destruction by non-State actors. It argues that digital transformation creates various cybersecurity vulnerabilities. However, it, at the same time, offers innovative solutions for enhancing detection, monitoring, and threat mitigation. Consequently, robust international collaboration, strategic policy frameworks, and continuous technological innovation could align cybersecurity measures with UNSCR 1540's counter-proliferation goals. Through an analysis of current trends, this contribution hopes that leveraging advanced technologies could transform cybersecurity challenges into opportunities for reinforcing the objectives of UNSCR 1540 in an increasingly digital world.





THE AUTHOR:

**Ali Alkis**



Ali Alkis is a Junior Associate Fellow at the NATO Defense College and NTI's Emerging Nuclear Security Leader. Currently pursuing a PhD in nuclear security, he rigorously investigates challenges in nuclear non-proliferation, extended deterrence, and nuclear piracy. Through a robust portfolio of articles, book chapters, interviews, and op-eds, Ali consistently delivers innovative insights and policy recommendations that help shape the future of global nuclear security.

## **INTRODUCTION**

Technological innovation has fundamentally reshaped global security architecture recently. It has not only introduced new opportunities, but also complex cybersecurity challenges. Going back to the early 2000s, the United Nations Security Council adopted resolution 1540. It established legally binding obligations on all Member States

to prevent non-State actors from acquiring weapons of mass destruction (WMD) and their means of delivery. Adopted in 2004, it called on Member States to implement comprehensive measures to secure sensitive technologies and materials, so that robust policies are in place to counter proliferation. While the resolution is universally binding, not all Member States are equal in terms of

their relevance to WMD counter-proliferation, and not all of the provisions of the resolution are equally pressing for every Member State to fulfil.<sup>1</sup> Furthermore, while the text of the resolution does not have any words related to “cyberattack”, it is important to highlight the importance of cybersecurity measures within a unified approach driven by State policy, given the complexity and global nature of WMD

1 Peter Crail, “Implementing UN Security Council Resolution 1540,” *The Nonproliferation Review* 13, no. 2 (2006).

threats and the evolving threat of terrorism.<sup>2</sup>

Recent digital transformation has expanded the cybersecurity landscape. On one hand, it has increased vulnerabilities, ranging from sophisticated hacking and ransomware attacks to critical weaknesses in digital supply chains and financial systems. For example, a 2020 investigation into counterfeited Cisco devices revealed that the fraudulent circuits bypassed security functions and authenticity checks.<sup>3</sup> Although no backdoors have been detected, the possibility of a chip evading security checks raises alarm bells: it indicates the potential for adversaries to gain easier access to the network through such chips. Such vulnerabilities could not only undermine the counter-proliferation objectives of UNSCR 1540, but also global security. On the other hand, emerging technologies, in other words, artificial intelligence (AI), blockchain, and machine learning, could be leveraged to present innovative

opportunities to enhance detection, monitoring, and threat mitigation.

### **CYBERSECURITY VULNERABILITIES IN THE DIGITAL AGE**

The rapid pace of digital transformation has increased cybersecurity vulnerabilities. Since 2004, non-State actors have acquired significant resources and capabilities, challenging Member States to secure vast and complex digital infrastructures and global supply chains.<sup>4</sup> This interconnectedness has increased the risk of conventional cyberattacks—those typically driven by financial or disruptive aims rather than political ideology. Such attacks include sophisticated hacking, ransomware incidents, and digital sabotage that, while potentially disruptive, are generally not designed to impact WMD non-proliferation.

In addition to conventional digital threats, the risk landscape is further complicated by a peak in strategic

cyberattacks. Strategic cyber threats have increased considerably in recent years, with a series of damaging attacks making sensational headlines. Of particular concern is the possibility of a malicious cyber-attack targeting nuclear facilities and critical Command and Control systems—a scenario where the uncertainty of immediate consequences could greatly undermine counter-proliferation efforts under UNSCR 1540.<sup>5</sup>

Another pressing concern is the vulnerability within digital supply chains. As industries increasingly adopt just-in-time production models and rely on extensive global networks of suppliers, the integrity of these chains becomes vital to national and international security. A breach at any point in the supply chain could compromise sensitive technologies and critical components, thereby facilitating their unauthorized proliferation. For example, breaches in pharmaceutical or nuclear-related supply chains could

- 2 Muhammed Ali Alkis, "The Role of Industry and Academia in Implementing UNSCR 1540," 1540 Compass, no. 2 (2024), <https://unicri.org/sites/default/files/2024-09/UNSCR1540-Alkis-Industry-Academia.pdf>.
- 3 Christopher Hobbs et al., *Securing the Nuclear Supply Chain: A Handbook of Case Studies on Counterfeit, Fraudulent and Suspect Items* (London: King's College London, 2024), <https://www.kcl.ac.uk/csss/assets/securing-the-nuclear-supply-chain-a-handbook-of-case-studies-on-counterfeit-fraudulent-and-suspect-items.pdf>.
- 4 Wilfred Wan, *UNSCR 1540 Civil Society Forum: A Dialogue with Academia and Civil Societ* (Tokyo: United Nations University, 2016), <https://i.unu.edu/media/cpr.unu.edu/attachment/2187/Meeting-Report-UNSCR-1540-Civil-Society-Forum.pdf>.
- 5 Huma Rehman, and Afsah Qazi, "Significance of UNSCR 1540 and Emerging Challenges to its Effectiveness," *Strategic Studies* 39, no. 2 (2019), <https://www.jstor.org/stable/48544299>.



trigger regulatory review or inspection processes, which—while necessary—may result in delays or disruptions. These interruptions could expose systemic weaknesses, strain compliance mechanisms, and create further opportunities for malicious exploitation by non-State actors

Digital financial systems represent another dimension of vulnerability. The advent of digital financial assets, including cryptocurrencies, has revolutionized transactional and funding mechanisms. However, this evolution has also introduced new avenues for financing illicit activities. Non-State actors may exploit these digital financial instruments to conceal funding sources, facilitating the acquisition or transfer of materials that could contribute to the proliferation of WMD.

While global attention often centres on sophisticated cyber intrusions, similar to how Member States traditionally prioritize catastrophic WMD scenarios, emerging evidence suggests that more localized or low-end attacks—comparable to the use of readily available radio-

logical materials—also pose significant risks. Therefore, the diffusion of technical know-how and equipment could lower the barrier for disruptive, if not spectacular, attacks.<sup>6</sup>

In this regard, industry plays an essential role in converting UNSCR 1540's mandates into operational practice. The industrial sector not only ensures that companies comply with strict security protocols for sensitive materials, but also drives innovation through the development of advanced detection and monitoring systems. These real-world experiences provide policymakers with insights into how technology can secure critical infrastructure and prevent unauthorized access—an imperative in today's digital landscape.<sup>7</sup>

Therefore, the inherent risks posed by digitalization demand a rigorous and integrated approach to cybersecurity. Addressing these vulnerabilities requires not only

State-driven policy measures but also the practical insights and technological capabilities of industry and academia.

## **EMERGING TECHNOLOGIES AS SOLUTIONS**

In response to the growing cybersecurity challenges of the digital age, emerging technologies also offer promising avenues to reinforce defences and mitigate vulnerabilities. Innovative tools, such as artificial intelligence (AI), blockchain, and advanced encryption protocols, are being deployed to detect and neutralize cyber threats, while simultaneously securing the critical infrastructures that underpin UNSCR 1540's counter-proliferation objectives.

AI and machine learning have become pivotal in the proactive monitoring of digital ecosystems. By analysing vast quantities of network data in real-time, AI-driven systems can identify anomalies that may signal potential threats. For instance, predictive analytics enabled by these technologies could flag unusual activities across digital supply chains or financial systems, thereby allowing for rapid responses before they escalate. Such capabilities ensure that sensitive materials remain protected from unauthorized

6 Wan.

7 Alkış.

access, directly supporting the preventive measures mandated by UNSCR 1540.

Blockchain technology further reinforces cybersecurity by introducing decentralized, immutable ledgers that guarantee transparency and traceability throughout digital transactions. In sectors where the integrity of supply chains is paramount, blockchain enables stakeholders to monitor every transaction and alteration, ensuring that any breach or tampering is immediately detectable. This enhanced level of security is particularly crucial in preventing the diversion of sensitive components that could contribute to the proliferation of WMD by non-State actors.

In addition, advanced encryption techniques and robust Internet of Things (IoT) security measures play a critical role in safeguarding digital financial systems. End-to-end encryption ensures that data remains secure even if a breach occurs, while continuous monitoring of interconnected devices helps maintain the confidentiality and integrity of sensitive information. By integrating these emerging technologies into existing cybersecurity

frameworks, Member States can address current vulnerabilities and build adaptive, resilient defence mechanisms that evolve in tandem with emerging threats.

### **POLICY IMPLICATIONS AND STRATEGIC RECOMMENDATIONS**

In light of the rapidly evolving digital threat landscape, it is important that Member States, in partnership with all stakeholders, including industry and academia, adopt robust policy frameworks that can swiftly adapt to emerging technologies while effectively mitigating cybersecurity vulnerabilities. A multi-stakeholder approach is essential—one that actively involves regulatory authorities, policy makers, representatives of international organizations, private sector experts, and academic researchers. This collaborative effort should focus on developing comprehensive policies that facilitate technological innovation while ensuring strict compliance with UNSCR 1540's non-proliferation objectives.

At the international level, enhancing cybersecurity resilience requires coordinated efforts to share intelligence, best practices, and innovative

solutions. Member States should engage in global forums and establish bilateral or multilateral platforms to foster an environment of mutual support and information exchange. For example, initiatives such as the European Union's Cybersecurity Act provide frameworks that could be tailored by other regions to create standardized protocols for data protection, incident response, and cyber forensics.

Individual Member States should also invest in capacity-building initiatives that equip public and private sector professionals with the necessary skills to address emerging cyber risks. Specialized training programmes, joint research projects, and the development of state-of-the-art cyber defence mechanisms are all critical to aligning national policies with the overarching goals of UNSCR 1540. Transparent and continuous dialogue among stakeholders is vital to ensure that these policies are both practical and reflective of real-world operational challenges.

Beyond technological solutions, there is a clear call for enhanced self-regulation within academic and research communities. Scientists

working on dual-use technologies bear a crucial responsibility not only to innovate but also to exercise restraint in disseminating sensitive data—a lesson that is equally applicable to managing cybersecurity risks.<sup>8</sup>

Complementing these perspectives, academic institutions significantly contribute through training and research. By offering specialized courses and conducting interdisciplinary research, academia not only builds the next generation of experts but also advances strategic counter-proliferation solutions. These efforts ensure that both current and future policymakers are well-prepared to address the evolving digital and physical security challenges posed by non-State actors.<sup>9</sup>

Moreover, regulatory policies should be continually reviewed and updated to keep pace with rapid technological advancements. This iterative approach will help bridge the gap between legislative mandates and operational realities, ensuring that the legal frameworks remain robust against evolving cyber threats.

Beyond technological innovation, enhancing UNSCR 1540's effectiveness will require a shift in institutional frameworks. UNSCR 1540 could benefit more from working by consent to ensure sustainability, which requires moving beyond the resolution to other multilateral consensus-based platforms. Such a move would facilitate more inclusive coordination, enabling international, regional, and sub-regional organizations to collaboratively address the counter-proliferation challenges introduced by both physical and cyber vulnerabilities.<sup>10</sup>

By integrating these strategic recommendations, Member States can transform cybersecurity challenges into opportunities, thereby reinforcing global security while upholding the critical mandate of UNSCR 1540.

## **CONCLUSION**

In conclusion, the rapid evolution of digital technologies has not only created cybersecurity vulnerabilities, but has also provided promising

opportunities to enhance our defences against the threat of WMD proliferation. Advanced tools, such as AI, blockchain, and strong encryption protocols, offer innovative solutions to detect, monitor, and mitigate cyber threats. By turning digital challenges into strategic advantages, Member States can effectively align cybersecurity measures with UNSCR 1540's counterproliferation goals, ultimately contributing to a more secure global environment.

Ultimately, the path to reinforcing UNSCR 1540's counter-proliferation objectives involves a comprehensive, integrated approach. Utilizing these technological solutions demands a unified effort among all stakeholders, supported by dynamic State-led policy frameworks and international collaboration. This State-driven collaboration is essential to ensuring that our evolving cybersecurity and counter-proliferation strategies remain both robust and adaptable.<sup>11</sup>

8 Wan.

9 Alkış.

10 Rehman, and Qazi.

11 Alkış.



# UNSCR 1540 AND CYBERSECURITY IN THE FOURTH INDUSTRIAL

*The 4IR is characterized by hyperconnectivity and automation; Credit: Murilo Gomes.*

## ABSTRACT

The adoption of the United Nations Security Council resolution (UNSCR) 1540 in 2004 represented a significant advancement in the efforts to prevent the proliferation of weapons of mass destruction (WMD) by non-State actors. Nonetheless, the emergence of the Fourth Industrial Revolution (4IR) has introduced novel threat dimensions, particularly within the realm of cyberspace. This paper offers a critical examination of the implications of UNSCR 1540, specifically concerning cybersecurity in the context of the 4IR. It elucidates the resolution's efficacy in mitigating the physical transfer of WMD materials, while concurrently identifying its deficiencies in addressing cyber threats. The analysis accentuates the necessity for an expanded framework that incorporates cyber capabilities with impacts akin to those of WMD, delineates State obligations in cyberspace, and promotes enhanced real-time information sharing. By effectively bridging the divide between physical and digital security measures, this paper advocates for a dynamic and adaptive approach to international security, thereby fostering sustainable peace within an increasingly interconnected global landscape





THE AUTHOR:  
**Yasmin Hussien**



Yasmin Hussein is a Peace Scholar at the Boutros-Ghali Chair for Sustainable Peace, a Scholar at the Deraya Center for Research and Sustainability, and a Non-Resident Fellow at the Arms Control Negotiation Academy. Previously, she was a Trainee at the UNODA's Youth for a World without Nuclear Weapons and a Reviewer at the Oxford University COVID-19 Government Response Tracker. She is the Co-Author of the Child-Friendly Text of the UN Palermo Protocol and Paris Agreement and was recognized as UNHCR Young Champion for Refugees and Young Arab Pioneer by the Government of UAE's Arab Youth Center.

Adopted in 2004, UNSCR 1540 holds significant weight in preventing the proliferation of WMD and their means of delivery by non-State actors, including terrorist individuals and entities<sup>1</sup>. However, the landscape of potential threats has expanded drastically in the Fourth Industrial Revolution, with cyberspace emerging as a critical battleground, blurring

the lines between traditional and novel WMD.<sup>2</sup>

This article examines the impact of UNSCR 1540 on cybersecurity in the digital era, exploring its strengths, limitations, and potential adaptations for sustainable peace.

## **ADDRESSING THE CONVENTIONAL THREAT, BUT FALLING SHORT IN THE DIGITAL AGE**

UNSCR 1540 mandates international cooperation to prevent the transfer of WMD materials and related technologies to non-State actors. By establishing legal obligations for States to implement

1 UN Security Council resolution 1540 (2004): <https://disarmament.unoda.org/wmd/sc1540/>.

2 The Fourth Industrial Revolution: <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> (Accessed, February 2024).

control measures and report suspicious activities, the resolution aims to create a global safety net against catastrophic events. While undoubtedly successful in curtailing the physical movement of WMD components, UNSCR 1540 (2004) struggles to address the evolving nature of threats in the digital age.<sup>3</sup>

Firstly, the resolution's focus on tangible materials and delivery systems does not encompass cyber capabilities enabling actors to attack critical infrastructure or manipulate information for mass disruption remotely. These digital "weapons" lack a physical footprint, making them harder to track and control under the existing framework. Secondly, the resolution's emphasis on State-to-State cooperation overlooks the decentralized nature of cyberspace. Non-State actors often operate across borders, exploiting weak cyber defences and leveraging readily available digital tools. This complicates attribution and makes enforcement measures challenging.

Finally, the resolution's reporting mechanisms, while valuable for sharing information

about physical WMD proliferation, are inadequately equipped to capture the dynamic and rapidly evolving threats in cyberspace. The sheer volume and complexity of cyber incidents demand real-time collaboration and information exchange, exceeding the scope of the current framework.

### **THE INTERTWINED WEB: FROM PHYSICAL TO DIGITAL DESTRUCTION**

The Fourth Industrial Revolution, characterized by hyperconnectivity and automation, further intertwines the physical and digital worlds. Critical infrastructure systems, traditionally physical targets, have become increasingly dependent on software and interconnectedness. This convergence creates a vulnerability where cyberattacks can trigger real-world consequences, potentially causing widespread disruption and physical harm.

For example, the 2020 cyberattack on a Florida water treatment plant illustrates how digital manipulation can have physical repercussions. Hackers gained access to the system and attempted to increase the

levels of sodium hydroxide, a dangerous chemical, before being stopped. This incident highlights the potential for cyberattacks to be used as WMD in disguise, bypassing the limitations of UNSCR 1540.

### **ADAPTING THE FRAMEWORK FOR A DIGITAL FUTURE**

Recognizing these limitations, the international community has begun exploring ways to adapt UNSCR 1540 to address cyber threats. Several proposals suggest expanding the resolution's scope to encompass:

- **Cyber capabilities with WMD-like impact:** Defining and regulating the development and use of cyber tools that could cause widespread physical destruction or disruption, similar to traditional WMD.
- **State obligations in cyberspace:** Clarifying States' responsibilities to prevent malicious cyber activities within their borders, including cooperation in investigations and attribution.

<sup>3</sup> UN Office for Disarmament Affairs (UNODA) report on "The Security Council and Non-Proliferation: The Case of Resolution 1540": <https://disarmament.unoda.org/wmd/sc1540/> (Accessed, February 2024).



- **Enhanced information sharing:** Establishing dedicated mechanisms for real-time exchange of cyber threat intelligence and incident reports to facilitate coordinated responses.<sup>4</sup>

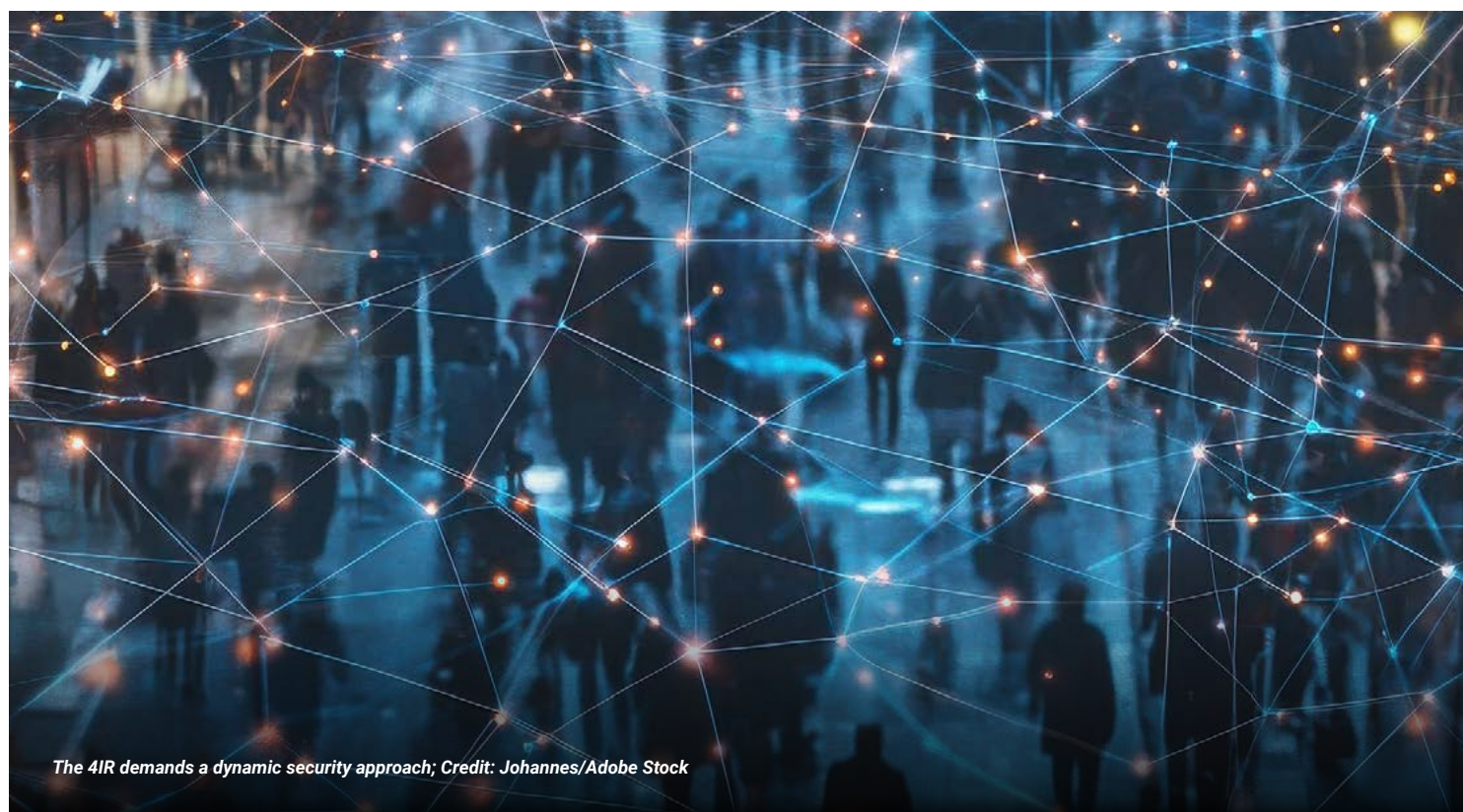
While these proposals hold promise, significant challenges remain. Defining the boundaries of “cyber WMDs” and navigating diverse national cybersecurity policies within a universal framework requires careful consideration and international consensus.

Additionally, balancing information sharing with privacy concerns and potential misuse of data necessitates delicate negotiations.

### **CONCLUSION: TOWARDS A SECURE AND PEACEFUL DIGITAL FUTURE**

The Fourth Industrial Revolution demands a dynamic security approach, adapting frameworks like UNSCR 1540 to accommodate the evolving threat landscape.<sup>5</sup> Addressing the nexus between cybersecurity and WMD

proliferation requires international cooperation, innovative thinking, and a willingness to bridge the gap between the physical and digital worlds. By fostering dialogue, promoting responsible State behaviour in cyberspace, and developing efficient information-sharing mechanisms, the international community can strive towards a future where technology empowers, rather than endangers, sustainable peace and security.



*The 4IR demands a dynamic security approach; Credit: Johannes/Adobe Stock*

- 4 UNODA report on “The Potential Role of UNSCR 1540 in Addressing Cyber Threats”: <https://www.un.org/en/sc/1540/documents/OAS%20Statement.pdf> (Accessed, February 2024).
- 5 United Nations High-Level Meeting on the Rule of Law in the Digital Age report on “Building a Secure and Inclusive Digital Future for All”: <https://www.un.org/development/desa/un-desavoice/sdg-blog/2021/12/2934.html> (Accessed, February 2024).



# LEVERAGING TECHNOLOGY FOR UNSCR 1540 IMPLEMENTATION: THE BWC NATIONAL IMPLEMENTATION MEASURES DATABASE

*The BWC NIM Database consolidates implementation data from over 100 countries; Credit: Markus Krisetya.*

## ABSTRACT

The UNIDIR-VERTIC BWC NIM Database is a digital tool developed through a partnership leveraging technology to support BWC national implementation. By consolidating open-source data on national implementation measures adopted by BWC States Parties, it provides a centralized platform for policymakers, researchers, and assistance providers. Being a collaborative effort between stakeholders, the database counts with input from experts from an international organization research institute and a non-governmental think tank, and it benefits from governmental feedback. Its user-friendly interface and multiple functionalities allow its 1,000 monthly users to access, compare and search legislative and regulatory frameworks. This makes it a key resource to enhance transparency, facilitate research, support cooperation and strengthen biosecurity governance, while also serving stakeholders that work towards wider UNSCR 1540 objectives. This article explores how the BWC NIM Database illustrates the potential and challenges of technology-driven tools to advance disarmament and non-proliferation efforts in an evolving security landscape.





THE AUTHOR:

**María Garzón Maceda**



María Garzón Maceda is Project Coordinator for the WMD Programme at UNIDIR, focusing on the CBW workstream.

Before joining UNIDIR, María was a Policy Fellow at the European University Institute, working on the participation of the Global South in WMD regimes. Previously, she was a civil servant with years of experience at the Argentine Ministry of Foreign Affairs, working on the implementation of the CWC.

## **INTRODUCTION**

Effective implementation of the Biological Weapons Convention (BWC) is critical for global security and directly supports the objectives of UNSCR 1540, particularly in preventing the misuse of dual-use biological materials, technologies, and research for proliferation purposes. Article IV of the Convention mandates States Parties to

adopt national measures prohibiting and preventing the development, production, and acquisition of biological weapons, which includes their misuse by non-State actors. However, translating these commitments into national laws, regulations, and enforcement mechanisms remains a work in progress. Some States have enacted comprehensive legal frameworks, while others are still in the process

of developing the necessary measures.

To address such gaps in national implementation, accessible and innovative technology-driven resources can play an important role. One such initiative is the Biological Weapons Convention National Implementation Measures (BWC NIM) Database,<sup>1</sup> developed by the United Nations Institute for Disar-

1 BWC NIM Database. Available at <https://bwimplementation.org> (accessed 18 February 2025).

mament Research (UNIDIR) in partnership with the Verification Research, Training and Information Centre (VERTIC), with technical support from the United Nations International Computing Centre (UNICC). The database is a publicly accessible resource that consolidates open-source information on BWC national implementation, providing policymakers, researchers, and assistance providers with a centralized platform to access national legislative measures. With more than 1,000 monthly visitors from over 190 countries, this digital tool has become a key resource for enhancing transparency, promoting information-sharing, and supporting discussions on strengthening the BWC regime.

### **A COLLABORATIVE EFFORT AMONG STAKEHOLDERS**

The BWC NIM Database is a digital platform that combines technology and interdisciplinary

collaboration. With initial funding provided by the United States of America, the project is led by UNIDIR and VERTIC, who leveraged their combined expertise in policy and legal issues related to weapons of mass destruction to develop the concept and research methodology.

On the technical side, UNICC, the UN's primary digital services provider, was responsible for UI/UX design, software development, security testing, and hosting. Partnering with UNICC ensured the database is "compliant with the high levels of security and ITC standards required by the funders and the UN".<sup>2</sup>

Moreover, the project benefits from a multi-stakeholder approach. As part of the research process, BWC States Parties are invited to review their country profiles and submit feedback. This engagement not only strengthens data accuracy but also

increases the visibility of the project and builds confidence in the database among States. The database serves as a reference point on what has been done to support national implementation and facilitates information to States Parties (or signatories) seeking to develop or improve their own national frameworks.

### **AN INNOVATIVE DIGITAL TOOL**

The BWC NIM Database builds upon existing tools, such as VERTIC's earlier BWC legislation database, offering an updated and expanded version with multiple functionalities.<sup>3</sup> It features a user-friendly interface, including an interactive map, individual country profiles, a comparative tool, and a text search function.

The illustrative map<sup>4</sup> allows users to apply filters on different national measures and visualize the implementation status worldwide. Each

2 United Nations International Computing Centre (2024). "UNICC Collaborates with UNIDIR and VERTIC to Develop a BWC National Implementation Measures Database." Available at <https://www.unicc.org/news/2024/02/05/unicc-collaborates-with-unidir-and-vertic-to-develop-a-bwc-national-implementation-measures-database> (accessed 18 February 2025).

3 Drobysz, Sonia (2023). "VERTIC and UNIDIR Develop BWC National Implementation Database." Trust & Verify, no. 172, Summer 2023, pp. 11. Available at <https://www.vertic.org/wp-content/uploads/2023/07/TV172-REV2.pdf> (accessed 18 February 2025).

4 The illustrative map was provided by the UN Geospatial Information Section and the boundaries and designations shown do not imply official endorsement by UNIDIR or VERTIC. More information: United Nations Geospatial Information Section. Available at <https://www.un.org/geospatial/> (accessed 18 February 2025).

of the country profiles<sup>5</sup> are structured into key implementation categories, including prohibitions, export and transfer controls, biosafety and biosecurity, oversight of dual-use life sciences research, and governance structures. Additionally, profiles include information on UNSCR 1540 national reports, BWC working papers, Confidence-Building Measures, and Article X assistance and cooperation offers. Each profile provides detailed summaries, direct references to national legislation, and downloadable resources.

The comparative tool allows users to view up to five country profiles side by side, making it easier to analyse different approaches and identify commonalities and variances among them, as well as opportunities for collaboration. The text search function allows users to locate specific policies, laws, or key terms within the text of over 2,300 official documents included in the database. The tool is multilingual, available in all six UN languages, and features a mo-

bile-friendly interface to ensure accessibility worldwide.

Strengthening UNSCR 1540 through the BWC NIM Database

A variety of stakeholders besides States Parties can benefit from using the database and play a role in providing feedback on possible improvements.<sup>6</sup> For example, think tanks can analyse legislative trends; providers of assistance to States may use the database information to develop targeted assistance programmes; and bio or pharma industry actors can consult the database to better understand their obligations under national legislation.

While designed to support these and other stakeholders on BWC national implementation issues, the BWC NIM Database also serves as a valuable resource for those working on UNSCR 1540-related initiatives. By consolidating detailed information on national biosafety, biosecurity, dual-use research, and transfer controls, the database supports with key biological

disarmament and non-proliferation efforts.

**As part of the research process, BWC States Parties are invited to review their country profiles and submit feedback.**

<sup>5</sup> Comoros acceded to the Convention as the 188th State Party on 14 February 2025.

<sup>6</sup> Krasny, Jaroslav (2024). "Strengthening Global Biosecurity and Biosafety Efforts: The Role of the BWC National Implementation Database in Informing and Guiding National Policies." CIL Blog, 7 February 2024. Available at <https://cil.nus.edu.sg/blogs/strengthening-global-biosecurity-and-biosafety-efforts-the-role-of-the-bwc-national-implementation-database-in-informing-and-guiding-national-policies> (accessed 18 February 2025).



Enhancing transparency is a key function of the database. By making national implementation data publicly available, it provides a structured platform to analyse legislative measures that align with obligations under UNSCR 1540 and helps update its reporting.

The database also supports capacity-building and cooperation. Governments and agencies engaged in UNSCR

1540 implementation can use it to assess gaps and develop policy recommendations to strengthen national legal frameworks on BWC issues, which complements broader non-proliferation efforts.

Additionally, stakeholders involved in biological non-proliferation can use it to identify vulnerabilities in biosafety regulations, dual-use research oversight, and export controls,

supporting risk assessment and early warning in the prevention of exploitation by non-State actors.

## CHALLENGES AND FUTURE PROSPECTS

Despite its success, the BWC NIM Database faces challenges typical of such digital tools. Gathering and standardizing national implementation data is complex,



Promoting the BWC NIM Database to Member States at a side event to the 2023 BWC; Credit: UNIDIR.



as legislation differs significantly across jurisdictions and may change over time. UNIDIR and VERTIC mitigate this by conducting open-source research, engaging States Parties for cross-checking, and encouraging ongoing updates and feedback mechanisms.

In this regard, sustaining engagement of all key stakeholders remains a long-term effort. It requires proactive outreach through side events and booths at formal BWC meetings, informal events on this important topic, promotion via regional biosecurity networks, and collaboration with other entities in the UN system and other international organizations to maximize visibility.

Adapting to emerging challenges is another key consideration. The rapid evolution of biotechnology, among other trends, presents new implementation challenges. To ensure the database remains adaptable and responsive to changes, the categories may need to be further expanded in the future. Future developments to the database may also include enhanced filters on the homepage and on the search function, data visualization tools to better illustrate

trends, or even integration with other databases.

Finally, guaranteeing the long-term sustainability of the database will require diversified funding from both governments and non-governmental organizations. Continued investment is essential to maintain and expand the database's functionality, accessibility and relevance, ensuring it remains a valuable resource for strengthening biosecurity governance.

### CONCLUSION

The BWC NIM Database stands as an example of how collaborative partnerships between international organizations, academia, and governments can leverage technology to support BWC implementation and provide valuable insights for those working on UNSCR 1540 objectives. As the international community continues to tackle biological security challenges in a complex international landscape, digital tools like the BWC NIM Database can play an increasingly important role in supporting stakeholders' efforts to strengthen national implementation, foster cooperation, and reinforce broader non-proliferation commitments.

**To ensure the database remains adaptable and responsive to changes, the categories may need to be further expanded in the future.**

# ENHANCING CBRN RISK MITIGATION THROUGH BIG DATA

*Big data has huge potential to contribute to non-proliferation efforts; Credit: Markus Spiske.*

## ABSTRACT

United Nations Security Council resolution 1540 (UNSCR 1540) requires States to implement domestic controls preventing the proliferation of nuclear, chemical, and biological weapons, notably by securing related materials. Effective risk mitigation remains challenging due to several factors, including resource constraints, coordination gaps, and evolving threats from non-State actors. This paper explores how big data and its analysis can support States in fulfilling their UNSCR 1540 obligations by enhancing prevention, detection, analysis and response to CBRN incidents. The paper highlights how big data applications—such as anomaly detection—can strengthen oversight of CBRN materials and contribute to non-proliferation efforts across the CBRN spectrum.



THE AUTHOR:  
**Louison Mazeaud**



Louison Mazeaud is an Associate Researcher in the WMD programme at UNIDIR, where she focuses on the national implementation of the Biological and Toxin Weapons Convention (BTWC). She holds a bachelor's degree from King's College London (War Studies Department) and a master's degree from the Graduate Institute Geneva.

United Nations Security Council resolution 1540 (UNSCR 1540) calls on States to 'take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery, including by establishing appropriate controls over related materials.'<sup>1</sup> Various actions at the different phases

of the chemical, biological, radiological and nuclear (CBRN) risk mitigation cycle contribute to this overarching objective. In particular, implementing robust national frameworks for preventing and detecting CBRN incidents, contributes to States' fulfilment of their obligations under UNSCR 1540.

While significant improve-

ments have been made by States to enhance their capacities in this area, important challenges remain to control and secure CBRN materials. As Dr Bilal Nsouli, Head of Lebanon's CBRN and WMD Commission, stated: 'While we may have commendable legal frameworks in certain aspects of CBRN and WMD risk mitigation, short-

<sup>1</sup> United Nations Security Council Resolution 1540 (2004), S/RES/1540, 28 April 2004, [https://docs.un.org/en/S/RES/1540\(2004\)](https://docs.un.org/en/S/RES/1540(2004)).

comings in implementation at the technical level pose challenges.<sup>2</sup> Innovative solutions can help overcome some of these challenges and prevent non-State actors (NSA) from acquiring CRBN materials. In particular, big data and big data analytics (BDA) offer some applications which could assist States in fulfilling their obligations under UNSCR 1540 and related international treaties like the Biological Weapons Convention (BWC) and the Chemical Weapons Convention (CWC).

This paper explores the concept of 'big data,' along with related methods of analysis and applications. It then offers a concise overview of current challenges in CBRN risk mitigation before examining both existing and prospective big data applications across

various stages of the mitigation cycle, including prevention and detection.

## **BIG DATA AND BIG DATA ANALYTICS**

Big data can be defined as an 'information asset characterized by such a high volume, velocity and variety to require specific technology and analytical methods for its transformation into value.'<sup>3</sup> Raw data takes different forms and can be extracted from various sources. More than the data itself, BDA is critical and relies on various activities performed by algorithms, including anomaly detection, classification and recommendation.<sup>4</sup> Anomaly detection notably involves 'identifying items, events or observations that do not conform to an expected behaviour or pattern.'<sup>5</sup>

Analysing large volumes of information has become increasingly important as a more effective and efficient approach to addressing numerous issues. For example, in defence and security, BDA can be applied to enhance threat analysis and prevention strategies in relation to attacks on critical infrastructure.<sup>6</sup> Big data is also intensively used in cybersecurity where different applications help address critical technical issues. Companies gather data and share information on cyber incidents to better understand threat nature, prevent them, and enhance detection and response.<sup>7</sup> In particular, BDA can be leveraged to have a more nuanced understanding of attack types (hacking, malware, social attacks, human errors or advance persistent threats) relying on past oc-

- 2 Interview with Dr. Bilal Nsouli, 1540 Compass, Issue 01, April 2024, <https://unicri.org/Publication/First-issue-UN-SCR1540-Compass>.
- 3 Andrea De Mauro, Marco Greco and Michele Grimaldi, 'A formal definition of Big Data based on its essential features', Library Review, Vol. 65 No. 3, pp. 122-135, [https://www.emerald.com/insight/content/doi/10.1108/Ir-06-2015-0061/full/html?smclient=33ff0215-1ae3-11e7-bfcb-0cc47a6bceb8&utm\\_source=salesmanago&utm\\_medium=email&utm\\_campaign=default](https://www.emerald.com/insight/content/doi/10.1108/Ir-06-2015-0061/full/html?smclient=33ff0215-1ae3-11e7-bfcb-0cc47a6bceb8&utm_source=salesmanago&utm_medium=email&utm_campaign=default).
- 4 Damien Van Puyvelde, Stephen Coulthart and M. Shahriar Hossain, 'Beyond the buzzword: big data and national security decision-making', International Affairs, 93: 6, pp. 1397-1416, [https://www.chathamhouse.org/sites/default/files/images/ia/INTA93\\_6\\_06\\_VanPuyvelde et al.pdf](https://www.chathamhouse.org/sites/default/files/images/ia/INTA93_6_06_VanPuyvelde%20et%20al.pdf).
- 5 Damien Van Puyvelde, Stephen Coulthart and M. Shahriar Hossain, 'Beyond the buzzword: big data and national security decision-making', International Affairs, 93: 6, pp. 1397-1416, [https://www.chathamhouse.org/sites/default/files/images/ia/INTA93\\_6\\_06\\_VanPuyvelde et al.pdf](https://www.chathamhouse.org/sites/default/files/images/ia/INTA93_6_06_VanPuyvelde%20et%20al.pdf).
- 6 Paul B. Stephan, 'Big Data as a National Security Issue', The University of Chicago Legal Forum, 2024, <https://legal-forum.uchicago.edu/print-archive/big-data-national-security-issue>.
- 7 Danda B. Rawat, Ronald Doku and Moses Garuba, 'Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security', IEEE, Volume 14, Issue 6, 25 March 2019, <https://par.nsf.gov/servlets/purl/10094358>.

currences or attempts.<sup>8</sup> While recognizing risks inherent to this technique, big data could also be leveraged in similar ways to assist non-proliferation efforts and responses to CBRN incidents.

## **CHALLENGES IN CBRN RISK MITIGATION**

CBRN designates 'chemical, biological, radiological and nuclear materials and agents

that could potentially harm society through their accidental or deliberate release, dissemination, or impact.'<sup>9</sup> Some of these materials and agents are classified as 'dual-use' meaning they can be used both for peaceful purposes—such as enabling critical advancements in human and animal health or agriculture—as well as for malicious purposes, by facilitating the development of weapons capable of causing

mass casualties and/or socio-economic upheaval.

Historical accounts of the use of CBRN weapons by non-State actors remain imperfect and, at points, patchy. Nonetheless, there are documented and credible cases of terrorists pursuing CBRN weapons. For example, in the 1990s, the Japanese cult Aum Shinrikyo used various chemical weapons, including sarin, to



*In the 1990s, Aum Shinrikyo used chemical weapons, including sarin, to attack the public; Credit: Zalfa Imani.*

- 8 Danda B. Rawat, Ronald Doku and Moses Garuba, 'Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security', IEEE, Volume 14, Issue 6, 25 March 2019, <https://par.nsf.gov/servlets/purl/10094358>.
- 9 EU CBRN Risk Mitigation, European Union, accessed 3 March 2025, [https://cbrn-risk-mitigation.network.europa.eu/index\\_en](https://cbrn-risk-mitigation.network.europa.eu/index_en).



perpetrate mass murder in Tokyo's subway. The subway attack using Sarin in 1995 killed 12 and injured more than 1,000 people.<sup>10</sup> In 2001, letters containing *Bacillus anthracis* (the bacteria causing Anthrax) spores were sent to various locations including media facilities and Senators' offices in the United States.<sup>11</sup>

Twenty-two people fell ill and 5 died from pulmonary infection.<sup>12</sup> More recently, in 2017, the Islamic State of Iraq and the Levant (ISIL) was found, by the Organisation for Prohibition of Chemical Weapons (OPCW), to have used sulphur mustard against civilians in Syria.<sup>13</sup> With regard to nuclear weapons, there are no confirmed cases of terrorist groups successfully accessing

and using fissile material to build a nuclear bomb, but different groups, including Al-Qaeda, have attempted to do so.<sup>14</sup>

The consequences for mis-handling or weaponization of CBRN materials can be devastating. Yet the number of entities and individuals handling CBRN materials worldwide is growing. Developments in the biological domain illustrate this broader trend well. For instance, the number of facilities across the world handling dangerous pathogens and toxins is increasing concomitantly with the growth of the bioeconomy.<sup>15</sup> This is augmented by the "democratization" of synthetic biology and other technologies that ease access to and manipulation of agents by various communities. While potentially introducing great benefits, such trends could also facilitate terror groups' access to CBRN materials.

**The number of facilities across the world handling dangerous pathogens and toxins is increasing concomitantly with the growth of the bioeconomy.**

10 Monterey Institute of International Studies, WMD Terrorism Database, December 2001, [https://www.nonproliferation.org/wp-content/uploads/2016/06/aum\\_chrn.pdf](https://www.nonproliferation.org/wp-content/uploads/2016/06/aum_chrn.pdf).

11 Anthrax in America: A Chronology and Analysis of the Fall 2001 Attacks, Center for Counterproliferation Research, November 2002, <https://wmdcenter.ndu.edu/Portals/97/Documents/Publications/Articles/Anthrax-in-America.pdf>.

12 Anthrax in America: A Chronology and Analysis of the Fall 2001 Attacks, Center for Counterproliferation Research, November 2002, <https://wmdcenter.ndu.edu/Portals/97/Documents/Publications/Articles/Anthrax-in-America.pdf>.

13 United Nations, 'Government, 'Islamic State' Known to Have Used Gas in Syria, Organisation for Prohibition of Chemical Weapons Head Tells Security Council', 7 November 2017, <https://press.un.org/en/2017/sc13060.doc.htm>.

14 [https://npolicy.org/article\\_file/1602-The\\_Nuclear\\_Terrorism\\_Threat.pdf](https://npolicy.org/article_file/1602-The_Nuclear_Terrorism_Threat.pdf).

15 Global BioLabs Report, King's College London and George Mason University, 2023, p. 5, [https://static1.squarespace.com/static/62fa334a3a6fe8320f5dcf7e/t/6412d3120ee69a4f4efbec1f/1678955285754/KCL0680\\_BioLabs+Report\\_Digital.pdf](https://static1.squarespace.com/static/62fa334a3a6fe8320f5dcf7e/t/6412d3120ee69a4f4efbec1f/1678955285754/KCL0680_BioLabs+Report_Digital.pdf).

Controlling and securing CBRN materials remains a challenge for many States and international organizations, both of which are often inadequately resourced to cover all aspects of CBRN risk mitigation. Among the key challenges are political prioritization, legislative development and effective coordination between different State entities. In addition, more specific tasks, such as monitoring access to CBRN materials also constitute challenges in various countries. Finding efficient technological solutions to challenges at various stages of the mitigation cycle can support States in their efforts to counter CBRN proliferation and fulfil their 1540 obligations.

### **BIG DATA AND CBRN RISK MITIGATION**

Big data and BDA, notably through open-source intelligence (OSINT) have been explored to enhance the verifications of key international treaties.<sup>16</sup> They can also complement States and international organizations at different stages of the CBRN risk mitigation cycle from prevention to response. The



Figure 1 CBRN Risk Mitigation Cycle

prevention and detection phases are particularly relevant to fulfilling UNSCR 1540 obligations. Indeed, this is when implementation measures undertaken by States to control CBRN materials and prevent non-State actors from acquiring them come under stress. Big data could be mobilized to help authorities, particularly by augmenting technical solutions to prevent and detect non-State actor CBRN weapons programmes. Whilst this is not a substitute for traditional methods of policing dual-use materials,

it can augment and aid such methods under certain conditions.

During the prevention phase, the goal should be to establish a clear understanding of baselines which would allow an easier detection of anomalies by algorithms. Big data can be leveraged to gather information on activities involving CBRN materials, facilities and individuals handling agents, trade and transfer, but also waste water and hospital activity. With regard to collecting information on facilities, big

16 James Revill and María Garzón Maceda, *The Role of Open-Source Data and Methods in Verifying Compliance with Weapons of Mass Destruction Agreements* in Henrietta Wilson and Dan Plesch (eds.), *Open Source Investigations in the Age of Google* (World Scientific, June 2024).

data could be used to observe staff and visitors' movements in and around sensitive sites. The control of access to dual-use items could also be enhanced by various applications relying on big data. A UNIDIR essay notably explored the use of open-source trade data to follow trade in aspects of dual-use biotechnology.<sup>17</sup> International databases like the United Nations Comtrade Database allow for gathering information on import of dual-use items using Harmonized System (HS) codes.<sup>18</sup>

At the detection phase, the goal should be to identify anomalies altering trends identified during the prevention stage. This may include unauthorized access to facilities, unusual trade of dual-use items or undeclared activities in sensitive locations. As an example, the International Atomic Energy Agency

(IAEA) uses the International Radiation Monitoring System (IRMIS) to collect data on radiological situations in over 6,000 locations around the globe.<sup>19</sup> This information can help detect abnormal levels of radiation in an emergency and inform authorities in a timely manner.<sup>20</sup> States could implement similar systems of data gathering and anomaly detection to monitor laboratory activities, waste water contamination and orient inspections by law enforcement agencies. The possibility of using nano-technology based biosensors for laboratory monitoring has notably been evoked during an expert presentation at the Third Session of the Working Group on the Strengthening of the BWC in 2023.<sup>21</sup> Machine learning tools relying on big datasets for training could be used to automate these processes and enhance irregularity detection.

Additionally, big data can help inform process of response and analysis. Measures to effectively analyse and respond to events can mitigate some of the effects of CBRN weapons in certain cases through gap analysis and the threat of credible attribution and justice can serve as a strong deterrence against the pursuit of such weapons by non-State actors.

During analysis, the goal should be to determine the impact and origins of the CRBN incident. Big data applications could support information gathering and identification origins. The analysis of the latter is also critical to enhance domestic controls implemented by authorities, notably through gaps identification. The World Health Organization's Early Warning Alert and Response System (EWARS) supports practitioners during outbreaks

17 Borrett, V., Hanham, M., Jeremias, G., Forman, J., Revill, J., Borrie, J., Åstot, C., Baulig, A., Curty, C., Dorner, B.G., Fraga, C., Gonzalez, D., Mikulak, R., Noort, D., Raza, S.K., Tang, C., Timperley, C., van Straten, F.M., van Zalen, E., Vanninen, P. and Waqar, F. 2020. "Science and Technology for WMD Compliance Monitoring and Investigations, WMD Compliance and Enforcement Series no. 11, Geneva, Switzerland: UNIDIR, <https://doi.org/10.37559/WMD/20/WMDCE11>.

18 Borrett, V., Hanham, M., Jeremias, G., Forman, J., Revill, J., Borrie, J., Åstot, C., Baulig, A., Curty, C., Dorner, B.G., Fraga, C., Gonzalez, D., Mikulak, R., Noort, D., Raza, S.K., Tang, C., Timperley, C., van Straten, F.M., van Zalen, E., Vanninen, P. and Waqar, F. 2020. "Science and Technology for WMD Compliance Monitoring and Investigations, WMD Compliance and Enforcement Series no. 11, Geneva, Switzerland: UNIDIR <https://doi.org/10.37559/WMD/20/WMDCE11>.

19 IAEA, 'Five Countries Join IAEA's Radiation Monitoring System', 23 May 2023, <https://www.iaea.org/newscenter/news/five-countries-join-iaeas-radiation-monitoring-system>.

20 IAEA, 'Five Countries Join IAEA's Radiation Monitoring System', 23 May 2023, <https://www.iaea.org/newscenter/news/five-countries-join-iaeas-radiation-monitoring-system>

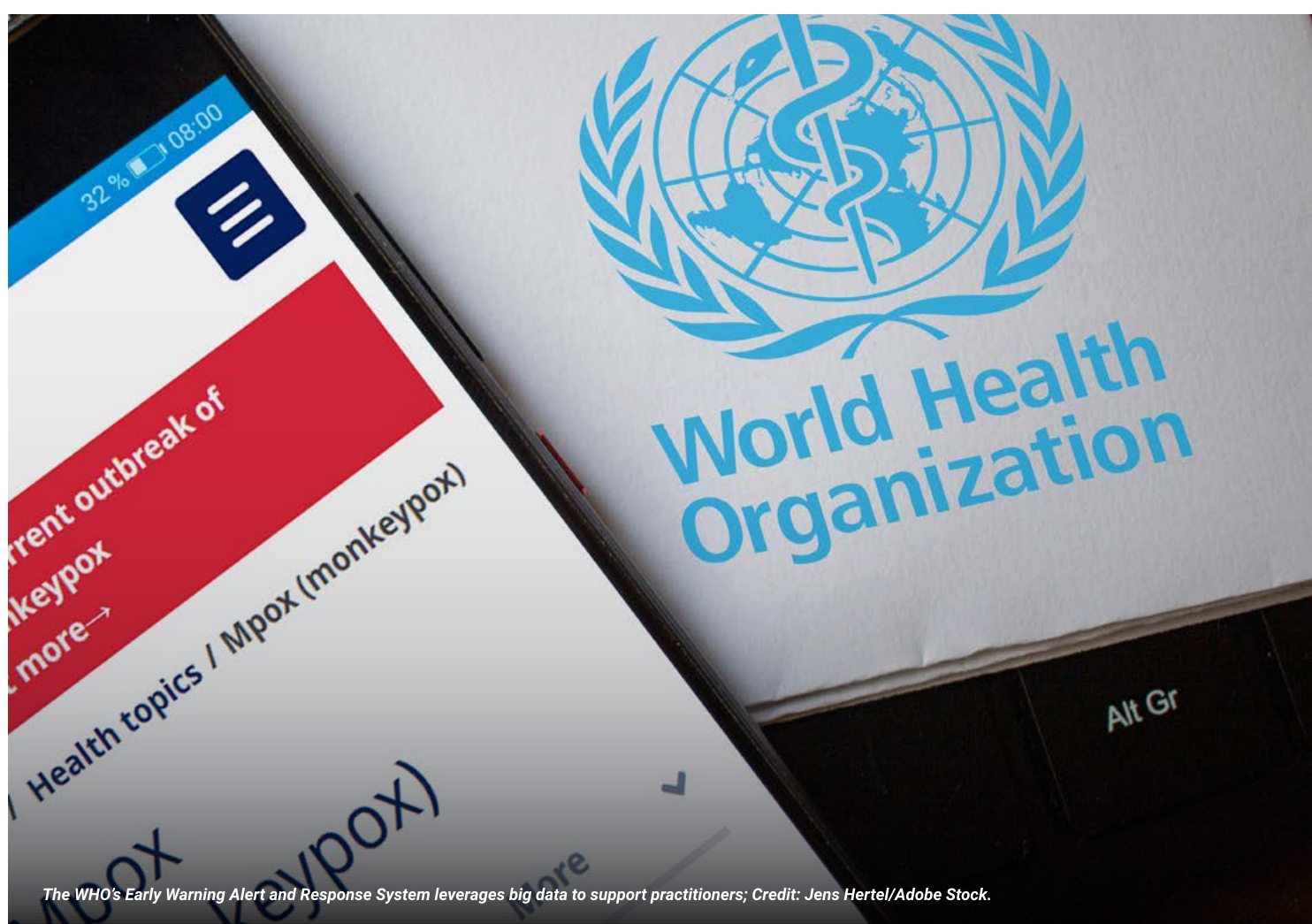
21 Ryan Teo, Developments in Science and Technology related to Verification (presentation), 12 July 2023, [https://docs-library.unoda.org/Biological\\_Weapons\\_Convention\\_Working\\_Group\\_on\\_the\\_strengthening\\_of\\_the\\_ConventionThird\\_session\\_\(2023\)/2023-12-07\\_BWC\\_WG3\\_Verification\\_finalv2\\_0.pdf](https://docs-library.unoda.org/Biological_Weapons_Convention_Working_Group_on_the_strengthening_of_the_ConventionThird_session_(2023)/2023-12-07_BWC_WG3_Verification_finalv2_0.pdf).

with real-time reporting from treatment centres and hospitals, as well as advanced data analysis and visualization including maps.<sup>22</sup> Similar tools to monitor casualties, impact on critical infrastructures or natural resources could be useful for national authorities facing CBRN incidents. Big

data applications could also be leveraged for forensics purposes. As an example, the OPCW Scientific Advisory Board Temporary Working Group explored datasets and analytics methods which might be leveraged to investigate incidents involving chemical agents.<sup>23</sup> These tools could

facilitate 'cross-referencing, validating and linking together information' during investigations and help identify perpetrators.<sup>24</sup>

During the response phase, where authorities try to mitigate the impacts of the incidents and track perpetra-



The WHO's Early Warning Alert and Response System leverages big data to support practitioners; Credit: Jens Hertel/Adobe Stock.

22 World Health Organization, EWARS in a box (presentation), accessed 4 March 2025, [https://cdn.who.int/media/docs/default-source/documents/emergencies/ewars-presentation.pdf?sfvrsn=9bf14b42\\_4](https://cdn.who.int/media/docs/default-source/documents/emergencies/ewars-presentation.pdf?sfvrsn=9bf14b42_4).

23 OPCW, Report of the SAB Temporary Working Group, December 2019, [https://www.opcw.org/sites/default/files/documents/2020/11/TWG%20Investigative%20Science%20Final%20Report%20-%20January%202020%20\(1\).pdf](https://www.opcw.org/sites/default/files/documents/2020/11/TWG%20Investigative%20Science%20Final%20Report%20-%20January%202020%20(1).pdf).

24 OPCW, Report of the SAB Temporary Working Group, December 2019, [https://www.opcw.org/sites/default/files/documents/2020/11/TWG%20Investigative%20Science%20Final%20Report%20-%20January%202020%20\(1\).pdf](https://www.opcw.org/sites/default/files/documents/2020/11/TWG%20Investigative%20Science%20Final%20Report%20-%20January%202020%20(1).pdf).



tors, big data applications could also support different tasks from strengthening efforts to localize suspects to enhancing assistance delivery and improving coordination between State services. As an example, big data applications have been explored to support relief efforts during natural catastrophes like hurricanes through past population movement patterns.<sup>25</sup> An efficient response to a CBRN incident is critical to sustaining UNSCR 1540 and domestic controls of CBRN materials. Indeed, such a response would reduce the effects of CBRN weapons and, in turn, possibly deter actors from pursuing these means. More attention has notably been given to the ways in which non-State actors could engage in disinformation campaigns to affect responses to a CBRN incident. In this area, big data analysis of social media activity and Natural Language Processing (NLP) could flag fake news articles and posts circulating on social media platforms.<sup>26</sup>

This could assist authorities in detecting and responding to hostile campaigns affecting public health responses during a CBRN incident and ultimately reduce the incentive for NSAs to engage in these activities.

### **WAY FORWARD**

Big data and BDA could assist States during the various phases of the CBRN risk mitigation cycle. In particular, big data could be leveraged to gather more information on facilities and individuals handling CBRN materials. Enhanced prevention and detection of CBRN incidents would effectively support States' fulfilment of their obligations under UNSCR 1540 and reinforce related international treaties. Similarly, effective analysis and response to incidents could deter non-State actors from attempting to access and use CBRN materials. Sensitizing authorities on the existence of these applications as well as understanding their needs will

appear critical in the development of innovative solutions for the control of CBRN materials.

A reflection on financial and physical resources required to implement these solutions should however be concomitantly conducted. Costs associated with technologies required for big data exploitation could be particularly high and deter States from adopting these methods, particularly States from low- and middle-income countries that may lack the resources and expertise to effectively use big data. Uneven access can in turn create issues related to trust in and legitimacy of the use of big data and related tools. Information management is also a challenge and needs to be backed by reliable hardware and standard operating procedures. Beyond these practical aspects, States would need to agree on methods and data used, as well as the relative advantage of any of these tools over existing methods.<sup>27</sup> Similarly,

25 Alyson Chapman, 'Leveraging big data and AI for disaster resilience and recovery', Texas A&M University College of Engineering, 5 June 2023, [https://engineering.tamu.edu/news/2023/06/leveraging-big-data-and-ai-for-disaster-resilience-and-recovery.html?\\_gl=1\\*pilunr\\*\\_ga\\*MzcwMTQ0NjI5LjE3NDEzNTg3MjQ.\\*\\_ga\\_3LYM4WJM04\\*MTc0MTM1ODcyMy4x-LjEuMTc0MTM1OTE1NC42MC4wLjA.\\*\\_gcl\\_au\\*MTAzMTEwMDE4NS4xNzQxMzU4NzI0\\*\\_ga\\_SJ5GMN0ZQL\\*MTc0MTM1ODcyNC4xLjAuMTc0MTM1ODcyNC42MC4wLjA](https://engineering.tamu.edu/news/2023/06/leveraging-big-data-and-ai-for-disaster-resilience-and-recovery.html?_gl=1*pilunr*_ga*MzcwMTQ0NjI5LjE3NDEzNTg3MjQ.*_ga_3LYM4WJM04*MTc0MTM1ODcyMy4x-LjEuMTc0MTM1OTE1NC42MC4wLjA.*_gcl_au*MTAzMTEwMDE4NS4xNzQxMzU4NzI0*_ga_SJ5GMN0ZQL*MTc0MTM1ODcyNC4xLjAuMTc0MTM1ODcyNC42MC4wLjA).

26 Fatemeh Torabi Asr and Maite Taboada, 'Big Data and quality data for fake news and misinformation detection', Big Data and Society, January-June 2019, pp. 1-14, <https://journals.sagepub.com/doi/pdf/10.1177/2053951719843310>.

27 James Revill and María Garzón Maceda, The Role of Open Source Data and Methods in Verifying Compliance with Weapons of Mass Destruction Agreements in Henrietta Wilson and Dan Plesch (eds.), Open Source Investigations in the Age of Google (World Scientific, June 2024).



PREVENTION (establish baselines through big data gathering)	DETECTION (identify anomalies through BDA)	ANALYSIS (determine impact/incident origins through BDA)	RESPONSE (mitigate impact/track perpetrators through BDA)
<ul style="list-style-type: none"> <li>• Staff and visitors movements in/ around facilities</li> <li>• Financial flows</li> <li>• Trade of dual-use items</li> <li>• Hospitals activity</li> <li>• Waste water levels</li> <li>• Publications or patents</li> </ul>	<ul style="list-style-type: none"> <li>• Unusual trade flows</li> <li>• Unusal social media activity</li> <li>• Unauthorized access to facilities</li> <li>• Undeclared activities in sensitive locations</li> <li>• Irregularities in financial flows</li> </ul>	<ul style="list-style-type: none"> <li>• Real time reporting of impacts on hospitals and other critical infrastructures</li> <li>• Real time reporting of impacts on environment and natural ressources</li> <li>• Investigation support through linking and cross-referencing information</li> </ul>	<ul style="list-style-type: none"> <li>• Enhanced deployment coordination</li> <li>• Targeted ressources mobilization</li> <li>• Enhanced disinformation mitigation</li> <li>• Strengthened geospatial/ financial tracking capabilities</li> </ul>


*Figure 2 Big Data and CBRN Risk Mitigation Cycle (Examples Summary)*

security risks impacting data confidentiality and integrity, should also be considered.

Finally, partnerships need to be fostered between international organizations and States to raise awareness of existing applications of big data and enhance their features to better respond to States' needs. Fostering information sharing and interoperability between databases and algorithms

at the international level will also appear critical. Dialogue with private entities notably companies developing technological solutions relying on big data is also essential to design realistic means which are safe, cost efficient and effective at enhancing CBRN risk mitigation globally. Whilst there are therefore challenges to the use of big data to enhance CBRN mitigation, it would also be remiss to

ignore the growing potential of big data and related tools in efforts to take and enforce effective measures to establish domestic controls to prevent NSA from acquiring and using WMD in the future.

A photograph of a nuclear power plant at night. The image shows several large, white, conical cooling towers illuminated from within, with bright lights at their bases. In the background, there are several large, dark, dome-shaped containment domes. The foreground is dark, with some lights reflecting on the ground. The overall scene is industrial and somewhat mysterious due to the night setting.

# THE ROLE OF ARTIFICIAL INTELLIGENCE IN MITIGATING INSIDER NUCLEAR SECURITY THREATS AND STRENGTHENING UNSCR 1540

*Insider threats are one of the most pressing risk for nuclear security; Credit: Nicolas Hippert.*

## ABSTRACT

This paper argues that one of the most pressing challenges of nuclear security today is the insider threat. Artificial intelligence (AI) offers a transformative approach to enhancing nuclear security measures to mitigate insider threats, a critical concern for United Nations Security Council resolution (UNSCR) 1540 implementation. This article explores the multifaceted role artificial intelligence can play in strengthening nuclear facilities' physical and cyber security, preventing weapons of mass destruction (WMD) proliferation through advanced user behaviour analysis, and improving operational efficiency. AI-powered nuclear security systems can also enhance States' commitment to UNSCR 1540 and facilitate international cooperation through the sharing of best practices. Despite the challenges associated with AI technologies, leveraging AI can reinforce UNSCR 1540 objectives and bolster the global nuclear security architecture.



THE AUTHOR:  
**Shahneela Tariq**



Shahneela Tariq has an M.A. in Nonproliferation and Terrorism Studies from the Middlebury Institute of International Studies (MIIS), Monterey, California. Her research interest lies in the intersection of nuclear security and artificial intelligence to mitigate insider threats at nuclear power plants. Shahneela is passionate about workforce development and attracting new talent to the nuclear security field. She initiated the Women in Nuclear Security Podcast while at MIIS with a grant from the MIIS Provost's office.

Insider threats pose a significant and persistent risk to nuclear infrastructure and to nuclear security culture. Arguably, the overemphasis on external threats has led to the overlooking of insider threats, particularly those stemming from marginalized groups.<sup>1</sup> The major component that is missing in many long-term

nuclear terrorism strategies is the reduction of risk from insider threats.

UNSCR 1540, adopted in 2004, mandates all States to take and enforce effective measures to prevent non-State actors from acquiring WMD. The resolution emphasizes physical protection and developing

robust domestic control over sensitive materials. However, insider threats at nuclear power plants undermine these controls and create a potential route for nuclear materials to fall into the wrong hands.

Individuals with access, knowledge and authority over sensitive locations

<sup>1</sup> Nair, Sneha, Christina McAllister, and Annie Trentham. 2023. "Bias in Nuclear Security Implementation: Solutions to Identify Threats and Strengthen Security Culture in the United States." The Henry L. Stimson Center. <https://www.stimson.org/wp-content/uploads/2023/11/Bias-in-Nuclear-Security-Implementation.pdf>.

and materials at a facility could potentially abuse their privileges, causing irreversible harm to national security. For example, they could help terrorists access the facility and acquire critical materials and knowledge. Insiders can bypass security checks and can steal small amounts of radioactive materials without being noticed for a long period. Historically, it is evident that several nuclear security incidents—in other words, theft and sabotage—frequently had insiders involved, either as direct perpetrators or as crucial enablers and facilitators.<sup>2</sup>

While nuclear and non-nuclear high-security industries have employed several methods to prevent and detect insider threats, these methods—including screening, ongoing monitoring, regular training, and post-employment measures—remain insufficient to mitigate insider threats in the rapidly evolving security landscape. Therefore, it is vital to adopt innovative and effective ways

to deal with these threats in the age of technological advancement. Among the most promising developments is AI, a rapidly evolving field that is reshaping global security strategies.<sup>3</sup> This article will explore the critical role AI can play in countering nuclear terrorism and reinforcing the objectives of UNSCR 1540. In particular, the article will discuss how AI can enhance nuclear security measures, by addressing the challenges posed by insiders.

AI is a dual-use transformative technology that employs computational methods to perform tasks that typically require human intelligence, such as pattern identification and signals, behavioural anomaly detection, and image recognition.<sup>4,5</sup> Many key domains, including finance, healthcare, retail, and government, are already utilizing the benefits of AI technologies.

In the realm of security, AI-powered solutions are significantly enhancing detection,

prevention and response capabilities and strategies with their ability to analyse vast amounts of data in real-time.<sup>6</sup> AI technologies such as machine learning (ML), data science, deep learning, natural language processing (NLP) and computer vision are making a tangible impact, including by supporting the safety and security of organizations. Even industries such as casinos and gambling are increasingly turning to AI to strengthen their security frameworks.

Examples of the ways in which AI technologies are revolutionizing both physical and cyber security domains are discussed in the following table:

In the context of insider threats, the link between AI-driven nuclear security measures and UNSCR 1540 is multifaceted. Firstly, by strengthening nuclear facilities' physical and cyber security, AI technologies can directly prevent the proliferation of sensitive materials. AI technologies

2 Bunn, Matthew., and Scott D. Sagan, eds. 2017. Insider threats. Cornell University Press.

3 Horowitz, Michael C., et. al. 2018. Artificial intelligence and international security. Report by Center for a New American Security. [https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/CNAS-AI-and-International-Security-July-2018\\_Final.pdf](https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/CNAS-AI-and-International-Security-July-2018_Final.pdf).

4 Konar, Amit. 2018. Artificial intelligence and soft computing: behavioral and cognitive modeling of the human brain. CRC press.

5 Patcha, Animesh, and Jung-Min Park. 2007. "An overview of anomaly detection techniques: Existing solutions and latest technological trends." Computer Networks 51, no. 12: 3448-3470.

6 Cadet, Emmanuel. 2024. "AI-powered Threat Detection in Surveillance Systems: A real-time Data processing framework." Open Access Research Journal of Engineering and Technology, 07(02).



PHYSICAL SECURITY	CYBERSECURITY
<p><b>Anomaly Detection:</b> ML can enhance surveillance systems by predicting potential threats and suspicious behaviours in real time. It includes cameras, sensors and access control systems.</p>	<p><b>Anomaly Detection:</b> ML algorithms can help in identifying unusual patterns in computer systems and flag unusual behaviours in network traffic, and system logs i.e., intrusions and data breaches.</p>
<p><b>Risk Assessment:</b> AI can analyse historical data to identify patterns and predict potential security threats to inform organizations and governments to take proactive measures.</p>	<p><b>Malware Detection:</b> ML models are advancing in analysing and detecting malware codes and malicious patterns and can help create effective antivirus systems to mitigate these threats.</p>
<p><b>Biometric Authentication:</b> This application heavily relies on machine learning and can enhance control access systems to physical locations, which includes fingerprint scanners on doors and facial recognition at certain entry points in a building.</p>	<p><b>Phishing Detection:</b> AI is getting better at detecting phishing emails. It can analyse emails, URLs and other online communication channels to identify and block any malicious actor in a timely manner.</p>
<p><b>Behavioural Analytics:</b> ML can identify user behaviour and prevent unauthorized access. It can identify patterns, trends and anomalies in a person's behaviour and provide meaningful insights and recommendations.</p>	<p><b>Intrusion Detection Systems (IDS):</b> ML-powered IDS can detect a malicious act early as it can constantly monitor network trafficking and system activities.</p>
<p><b>Predictive Policing:</b> Data science algorithms can analyse historical criminal data and predict areas with a higher likelihood of crimes to deploy resources as preventive measures.</p>	<p><b>Fraud Detection:</b> Deep learning can enhance fraud detection in financial transactions, i.e. insurance claims and credit cards.</p>
<p><b>Object Detection &amp; Tracking:</b> AI can identify and track objects and people with a specific computer vision area in real-time, i.e. unattended bags and loitering. It can also allow security personnel to focus on real threats by reducing alarms and alerts.</p>	<p><b>Threat Intelligence Analysis:</b> Natural Language Processing (NLP) can analyse intelligence reports and dark web forums to extract insightful data for security analysts. It can also analyse emails, texts and website content to identify unusual inconsistencies.</p>



can help prevent insiders diverting nuclear materials or sabotaging a critical system by providing timely analysis of user behaviour and, in some cases, intentions, reinforcing the resolution's core objective of preventing WMD proliferation.

benefits of an AI-enabled insider threat mitigation system.<sup>7</sup> AI can analyse massive amounts of data quickly at nuclear power plants, something which humans cannot do. This demonstrates an extremely effective way to provide preventive measures on the front line through the application of predictive AI.<sup>8</sup>

enabling swift response to emerging threats.

Finally, UNSCR 1540 also implies the need to protect sensitive materials from cyber threats. The increasing globalization of the nuclear industry and the rise of cyber threats have further complicated the nuclear security landscape. The complex infrastructure of nuclear facilities, including control systems and communication networks, is susceptible to cyberattacks which could compromise safety and security protocols. However, as discussed above, AI-driven cybersecurity tools can identify and mitigate cyber threats that could compromise nuclear facilities.

Artificial intelligence is not a new technology, but its application in different security fields is more widely accepted now than before. Nevertheless, it has some significant challenges, such as the licensing of AI technology, data protection, and high chances of biases and discrimination against employees, which could lead to false alarms and

Secondly, AI-driven security systems can offer significant operational benefits in the nuclear security domain. Sandia National Laboratories and the Nuclear Engineering Teaching Laboratory (NETL) of University of Texas at Austin (UT) identified anomaly detection as one of the major

Furthermore, AI-enabled systems can provide robust and efficient insider threat detection and mitigation capability in security operations, which can potentially help to reallocate security resources elsewhere. It can also improve threat response by providing real-time alarms,

**Artificial intelligence is not a new technology, but its application in different security fields is more widely accepted now than before.**

7 Williams, Adam D., Shannon N. Abbott, Nathan Shoman, and William S. Charlton. "Results from invoking artificial neural networks to measure insider threat detection & mitigation." Digital Threats: Research and Practice (DTRAP) 3, no. 1 (2021): 1-20.

8 Frank, Malcolm, Paul Roehrig, and Ben Pring. 2017. What to do when machines do everything: How to get ahead in a world of ai, algorithms, bots, and big data. John Wiley & Sons.

unfair security assessments at nuclear power plants if applied without humans in the loop. National regulators and the international community are not yet sufficiently convinced to apply these tools to sensitive areas like nuclear power plants. However, continued research by reputable organizations, universities and national laboratories is crucial to demonstrate the positive utility of AI in nuclear security, to build the

foundation of trust that can enhance the implementation of States' obligations under UNSCR 1540.

AI offers powerful and promising tools for mitigating insider nuclear security threats and strengthening the implementation of UNSCR 1540.

Nevertheless, concerns regarding the application of AI at nuclear power plants are

valid, as it is crucial to address the challenges associated with AI-powered security systems, such as bias, the need for human oversight, and data privacy. By doing so, States can harness the full potential of AI to protect these critical facilities and prevent the proliferation of WMDs, ultimately contributing to a safer and more secure world.



*AI offers powerful and promising tools for mitigating insider nuclear security threats and strengthening the implementation of UNSCR 1540; Credit: Adobe Stock.*



# WEAPONIZED INTELLIGENCE: AI, NON-STATE ACTORS, AND WMD PROLIFERATION

*AI is becoming ever more prevalent, but it comes with risks; Credit: Maxime Valcarce.*

## ABSTRACT

Artificial intelligence (AI) is rapidly transforming both civilian and military domains, offering unprecedented capabilities but also introducing serious risks—especially in the context of weapons of mass destruction (WMD). This article explores the intersection of AI, security, and international regulation, with a focus on the implementation of United Nations Security Council resolution 1540 (UNSCR 1540). While AI’s military applications are increasingly embraced by State actors, the lack of clear regulation, transparency, and enforceable oversight creates ambiguities and leaves dangerous opportunities for the proliferation of this dual-use technology, including through the empowerment of non-State actors in new and alarming ways. From autonomous weaponization of small, commercially available, unmanned vehicles to AI-assisted chemical design and smuggling logistics, the barriers to entry for illicit WMD development are shrinking. Existing international frameworks must be adapted to address this evolving threat landscape. The piece concludes with concrete policy recommendations, including strict regulation of AI in high-risk domains, enhanced transparency, and the urgent need to incorporate AI-related risks into national implementation plans under UNSCR 1540.



THE AUTHOR:  
**Thomas Reinhold**



Dr Thomas Reinhold is a Researcher at the Cluster for Natural and Technical Science Arms Control Research (CNTR). CNTR is an interdisciplinary research initiative that examines emerging military-relevant technologies and developments in the natural sciences to assess their impact on international security and provide recommendations for strengthening arms control. This project received start-up funding from 2023 to 2026 from the German Federal Foreign Office and continues to receive partial funding. Thomas Reinhold conducts research on the militarization of cyberspace, AI and possibilities for arms control and disarmament of these technologies.

AI is increasingly regarded as the solution to a vast array of challenges across industry, IT, governance, and security. Its ability to process immense amounts of data, automate decision-making, and optimize operations makes it an appealing tool in virtually every sector, all whilst making human interaction with the knowledge of the world easier than ever. The promise of AI is so compelling that there is an undeniable trend toward its widespread integration—often

without fully considering the consequences.

This rapid expansion is driven by an intensely competitive commercial race, where speed and innovation outpace regulatory frameworks. AI development today is largely controlled by private corporations, many of which operate under the ethos of “move fast and break things” or “it’s easier to ask for forgiveness than to get permission.” This culture fosters a kind of digital

recklessness that prioritizes short-term gains over long-term stability. Vast sums of money are poured into AI projects, with investments driven by the expectation of high returns rather than a cautious evaluation of risks. Compounding this issue is the lack of effective regulation. While initiatives like the EU AI Act have been set in place, they are not yet fully enforced, and existing institutional oversight remains insufficient to control the pace and scope of AI deployment.



“

**Even when humans retain final authority, AI systems often make micro-decisions—such as filtering data or narrowing action options—that shape outcomes in subtle ways.**

”

### **THE SPILL-OVER OF MILITARY AI DEVELOPMENTS**

This unchecked approach to AI development is not confined to the commercial sector. Military forces and defence contractors are actively integrating AI into their systems, motivated by the need to keep up with the increasing speed of modern warfare. AI is seen as indispensable in military applications because it allows armed forces to process vast amounts of sensor and intelligence data, enhancing situational awareness and operational coordination. It increases the autonomy of military equipment, such as drones and robotic systems, making them

robust against jamming and electronic countermeasures (while rendering the question of meaningful human control more relevant than ever). While these capabilities might offer strategic advantages, the question remains: at what cost? The increasing use of AI in security-sensitive and military applications presents serious risks to global security that need to be taken into account with regard to UNSCR 1540.

One of the most pressing concerns is the lack of clear regulatory limits. The use of AI in situations involving military force demands defined red lines, yet few legally binding restrictions exist. Phrases like

“keeping a human in the loop” or “meaningful human control” are often cited but lack clear technical or operational definitions. Does this commitment mean that autonomous drones won’t operate beyond communication range? Does it allow a human to override a lethal decision? If such commitments are to be more than symbolic gestures, they must be anchored in specific technical requirements and regulations that have to be adapted by current and next-generation military-grade weaponizable systems. At the same time, this would also help to shape regulatory frameworks for commercially available, consumer-ready, autonomous vehicles, like, for example, a

restriction from using AI that exceeds a specific security-sensitive threshold, which would allow its impact to be mitigated if used harmfully by non-State actors.

A similar limiting effect can have technical guardrails for AI in automated data processing and when used as decision-making support. AI may enhance the quantity and speed of these processes but can also increase the risk of unintended escalation. Human judgment often serves as a buffer during crises, allowing time for de-escalation. AI systems, in contrast, prioritize speed over context and may misinterpret ambiguous data. The risk of rapid, automated, harmful responses based on flawed or incomplete information is non-negligible. Even when humans retain final authority, AI systems often make micro-decisions—such as filtering data or narrowing action options—that shape outcomes in subtle ways. These systems often function as “black boxes,” lacking transparency or explainability. While Explainable AI (XAI) offers approximations of reasoning processes, it does not provide meaningful insight into the system’s step-by-step logic, especially in time-sen-

sitive contexts. Moreover, the presence of **bias in training data**—which is frequently proprietary and opaque—can lead to flawed, unreliable and thus unwanted decisions, regardless of whether they are used by State or non-State actors.

The current rush towards AI and its integration into security-relevant IT systems can also introduce critical vulnerabilities that can be exploited by non-State actors. Adversarial techniques such as **data poisoning, model manipulation, and evasion attacks** allow attackers to subtly alter or deceive AI models, compromising threat detection and decision-making. These risks are particularly acute in systems that manage or monitor sensitive WMD-related activities. For example, **AI-enhanced Nuclear Command, Control, and Communications (NC3) systems** may improve response times and threat assessment, but also create opaque, complex decision layers vulnerable to cyber intrusion or spoofing. A compromised AI subsystem in NC3 could lead to false alarms, misattribution, or even unauthorized escalation. Such kinds of “data-driven” attacks on AI systems are especially difficult

to detect because they often exploit statistical weaknesses rather than system-level faults. Mitigation is further complicated by the black-box nature of many AI models, making it hard to trace, audit, or even anticipate manipulated behaviour.

### **THE PROLIFERATION OF AI AND NON-STATE ACTORS**

In the context of United Nations Security Council resolution 1540, the rapid advancement and democratization of AI technologies demand urgent attention as AI significantly lowers the barriers to developing or deploying WMD-related capabilities. What once required deep institutional knowledge and access to specialized infrastructure can now, in some cases, be approximated or simulated using publicly available AI models. For instance, open-source platforms powered by large language models or machine learning algorithms may assist in designing chemical precursors, optimizing the dispersal of radiological materials, or even engineering biological agents. This transformation not only expands the range of possible actors involved in proliferation, but

also obscures the detection and prevention of such activities.

Many of the most powerful AI tools—especially those developed for research, logistics, or scientific innovation—carry inherent dual-use potential. Language models trained on scientific publications or industrial data can be exploited to identify WMD-relevant materials, understand the mechanisms of chemical synthesis, or suggest routes to bypass regulatory oversight. These tools, often created for entirely legitimate purposes, can be misused with minimal adaptation, highlighting the urgent need for tighter controls and broader awareness of how dual-use risks manifest in the digital age. AI also enhances the operational capabilities of illicit proliferation networks. Smuggling routes, procurement chains, and covert financial operations may all be optimized using AI-driven logistics planning, pattern recognition, or synthetic identity generation. These technologies enable non-State actors to improve coordination and avoid detection, making traditional enforcement mechanisms less effective.

Moreover, the already mentioned weaponization of commercially available autonomous systems—capabilities that are made possible by AI—introduces new threats. Non-State actors have already demonstrated the ability to adapt consumer drones for tactical attacks. With AI, such platforms can operate independently or in coordinated swarms, allowing for more precise targeting or complex delivery methods. The possibility of AI-guided systems being used to disperse chemical or radiological agents, once the realm of speculation, is becoming technically feasible—and dangerously affordable.

Equally concerning is the diffusion of AI knowledge itself. The global open-source AI ecosystem encourages the sharing of code, datasets, and models across borders and disciplines. While this openness has driven innovation, it also makes it possible for individuals with no formal training or institutional backing to access tools and methodologies relevant to WMD development. The line between scientific progress and proliferation risk is becoming increasingly difficult to define.

## **POLICY RECOMMENDATIONS: WHAT SHOULD—AND SHOULD NOT—BE DONE**

UNSCR 1540 was crafted in an era before the current AI revolution, and its interpretation must evolve to reflect this new landscape. States must consider AI not only as a strategic asset, but also as a potential vector for proliferation. National implementation strategies should incorporate risk assessments related to AI tools, especially those with dual-use potential. Export controls must be modernized to include certain types of AI software and platforms, and clearer frameworks should be developed for managing access to sensitive datasets and training resources. Furthermore, States should promote transparency in AI development and deployment—particularly in research institutions and private companies involved in scientific and security-adjacent innovation.

In this emerging reality, where WMD-relevant capabilities can be amplified or even initiated by AI in the hands of non-State actors, the international community must act with foresight. Preventing

the misuse of AI is not solely a matter of regulation—it is a matter of global security, requiring a shared understanding that innovation without safeguards can have consequences far beyond its creators' intentions. In addition, to mitigate risks stemming from attacks on AI-enabled critical systems and infrastructures themselves, AI should be strictly prohibited or highly regulated in such domains. Whenever the margin for error

is zero or where automated processes and accidental triggering of effects can lead to devastating results, the leading question for decision makers should be if the seduction of AI is worth these risks.

### **CONCLUSION**

Raising awareness of these emerging risks must be a priority—not just among policymakers and militaries, but also among **developers**,

**academic institutions, and the private sector**, who may unknowingly contribute to proliferation through dual-use AI tools. As AI becomes more powerful and accessible, our global regulatory frameworks—including UNSCR 1540—must evolve in parallel. We must not let the allure of AI's potential blind us to its risks. Caution, regulation, and restraint are not hindrances to innovation; they are safeguards for global security.

“

**Non-State actors have already demonstrated the ability to adapt consumer drones for tactical attacks. With AI, such platforms can operate independently or in coordinated swarms, allowing for more precise targeting or complex delivery methods.**

”





# THE ERLANGEN INITIATIVE: ENHANCING DIALOGUE WITH ACADEMIA TO SUPPORT THE IMPLEMENTATION OF UNSCR 1540 (2004) WORLDWIDE

*The Erlangen Initiative focuses on outreach to academia; Credit: Good Free Photos.*

## ABSTRACT

Universities and research centres are an important target audience for export controls as they handle potentially critical goods and sensitive technological expertise. They play an instrumental role in the counter-proliferation of WMDs, especially given their predisposition to intangible transfers of technology (ITT) within international academic exchange. It is therefore vital to raise awareness among authorities for the need to reach out to academia, and to make researchers aware of their compliance obligations, especially when engaged in cross-border collaboration of a dual-use nature. Researchers must be equipped with means to detect, prevent and report attempts by illicit end-users to acquire and proliferate goods or technology applicable for WMDs. An improved understanding of resolution 1540 (2004) and its obligations will foster compliance and improve voluntary self-regulation within academic institutions.



---

THE AUTHOR:  
**Alessa Mondorf**



Alessa Mondorf serves as a project manager in the outreach division of the German Federal Office for Economic Affairs and Export Control, also known as BAFA. There, she is involved in a number of international outreach projects such as the Erlangen Initiative outlined above. She holds a bachelor's degree in International Business Management with a specialization on China and a master's degree in International Governance and Diplomacy from Sciences Po and Peking University. The opinions, findings, conclusions, and recommendations expressed in the article are those of the author.

**Considering this, the German Federal Government and UNODA in 2023 launched the “Erlangen Initiative”, establishing an international forum dedicated to dialogue about outreach to academia, the role of academia in fulfilling the non-proliferation obligations stipulated in UNSCR 1540 (2004), and national regulations. The initiative continued in 2024 with a regional conference in Southeast Asia and a global conference, delivering insights into effective academia outreach and the selection of outreach content for this target group.**



Preventing the misuse of research results for proliferation purposes is a key concern for regulators worldwide. Due to rapid advances in science and technology and the associated risks, as well as growing global interdependence in scientific research, academic and other R&D institutions have come to play an increasingly important part in non-proliferation efforts over the past years. As a result, both regulatory authorities and scientific institutions themselves are affording increasing attention to the role of academia in export controls. Scientists across different dis-

ciplines, ranging from biotech to aerospace, often work on research projects and with materials that have potential dual-use applications; but, in some cases, recent developments are not yet captured in existing international control lists. Even when scientific research is undertaken with a civilian purpose in mind, there could be a risk of misuse by illicit actors.

This potential threat adds complexity to understanding the scope and implications of export control requirements in academia, including where their boundaries begin

and end. In order to better reflect the academic perspective in export controls, and to advance the implementation of export control related obligations stemming from UNSCR 1540 (2004) and more direct national laws, frequent exchange and a trustful collaboration between regulators and academia is paramount. Such dialogue can raise awareness for the cause and ensure that individuals and institutions are equipped with the right skills to detect, prevent and report attempts by illicit end-users to acquire and proliferate WMD technology.

“

**In many respects, academia operates in a starkly different environment compared to industry: there is no catalogue of standardized products in university departments and research institutes; hierarchies are often less stringent compared to businesses, requiring more persuasive communication on an individual level; and both financial and personnel resources are sometimes scarce.**

”

To facilitate dialogue between regulatory authorities and academia beyond national borders, and to promote the implementation of UNSCR 1540 (2004) concerning export controls, the Erlangen Initiative (named after the German city Erlangen) was launched in May 2023. The German Federal Foreign Office spearheads the initiative with the support of the United Nations Office for Disarmament Affairs (UNODA), the German Federal Office for Economic Affairs and Export Control (BAFA), and the Fraunhofer Society. It offers a platform for open exchange between all stakeholders, on the one hand enhancing the understanding of export control requirements among academia, and on the other hand sharing the challenges of the research community and its particularities with regulators. Regular conferences both in an international, as well as in a regional context bring together State and academia representatives to discuss among peers and with their respective counterparts. The enhanced understanding of the challenges academia faces when dealing with export control regulations can thereby be translated into helpful guidelines and targeted outreach activities that facilitate the implemen-

tation of UNSCR 1540 (2004) with the help of academia.

### **ACADEMIA COMES WITH ITS OWN PARTICULARITIES**

In many respects, academia operates in a starkly different environment compared to industry: there is no catalogue of standardized products in university departments and research institutes; hierarchies are often less stringent compared to businesses, requiring more persuasive communication on an individual level; and both financial and personnel resources are sometimes scarce. Often, at the outset of the research cycle, it is not yet clear what the results will be, and even less to what extent they may be security-relevant. It is also an inherent pursuit of academic research to share knowledge and make it public to advance science, rather than to withhold it from others. In addition, the fundamental freedom of scientific research, as granted in many constitutions worldwide, needs to coexist and function with stringent export control measures required to prevent the proliferation of WMDs and their means of production and delivery. These unique circumstances lead to challenges

when regulators approach academia and when academia sets out to develop best practices for export controls.

Exchange within the Erlangen Initiative has highlighted two crucial themes to consider when engaging academia in export controls: First is how to raise and consolidate awareness among scientists, both of the risks as well as the obligations that are incumbent upon them when engaging in cross-border academic exchange. Of course, as in any field, the existing level of awareness differs between institutions and individuals, and some might already be highly sensitized to their responsibilities in preventing the proliferation of WMDs and their means of production and delivery. Yet, in most cases, export control and its implementation are neither part of degree programmes, nor of onboarding procedures, meaning that scientists might have never previously encountered the topic. Regulators, on the other hand, face the challenge of understanding the academic landscape in their respective countries and reaching a large number of institutions and individuals in a structured manner.



The second point to consider is a substantial communication barrier between authorities and academia. Representatives from universities and research institutions repeatedly pointed this out during the two central and one regional Erlangen Conferences in 2023 and 2024. “Scientists are not lawyers” was a recurrent statement, highlighting the overabundance of legal jargon that regulators tend to use when writing guidelines or conducting outreach to academia. The aim should be to deliver concise messages using language that resonates with the target audience. Open, collaborative dialogue between regulators and academia can only take place when the right language is used.

Researchers, whose main task is advancing the scientific research projects they are involved in, require practical, straightforward information. Key terms used frequently in export controls such as ITT, catch-all, fundamental research, and applied research should be explained or contextualized to clarify their importance and relevance to the academic field. Ideally, real-world examples or good/best practices underline the application and implementation

of legal provisions to illustrate them for a non-legal audience. At the same time, it seems desirable that the academic world is not only confronted with rules, but also actively develops tools for self-training in export control. In case of doubt, the regulator will likely be a step behind the cutting edge of technological development, necessitating the active involvement of academia.

### **WHAT REGULATORS SHOULD KEEP IN MIND**

The idiosyncrasies outlined above mean that outreach to academia differs significantly from outreach to industry, even if some legal instruments of export control are identical. As a result, for some regulators, this represents a relatively new area of focus requiring a novel approach, simply because the outreach mechanisms that have been developed and practised for years with industry do not translate well when applied to academia. Clearly, the road ahead is a learning process for both sides, and regulators need to apply careful consideration when designing outreach-to-academia strategies to ensure their effectiveness.

How to develop suitable strategies for outreach to academia was a topic of discussion at the second Erlangen Conference in November 2024. Participants discussed with panellists and cast their votes in an online opinion poll to identify what regulators must keep in mind when approaching academia to promote export controls stemming from UNSCR 1540 (2004). Foremost, academia highlighted the need to consider the underlying principle of scientific freedom. The foundation of science lies in the unfettered access to—and the open exchange of—research findings, which can appear to conflict with regulators’ focus on controlling the flow of information. As a result, outreach efforts must address these concerns thoughtfully and effectively while introducing the legal framework, definitions, and procedures that apply to academia.

Another distinctive challenge in engaging academia is its decentralized structure and the diversity of disciplines that regulators must address. These disciplines often vary significantly in their needs and practices. In some, researchers might be accustomed to

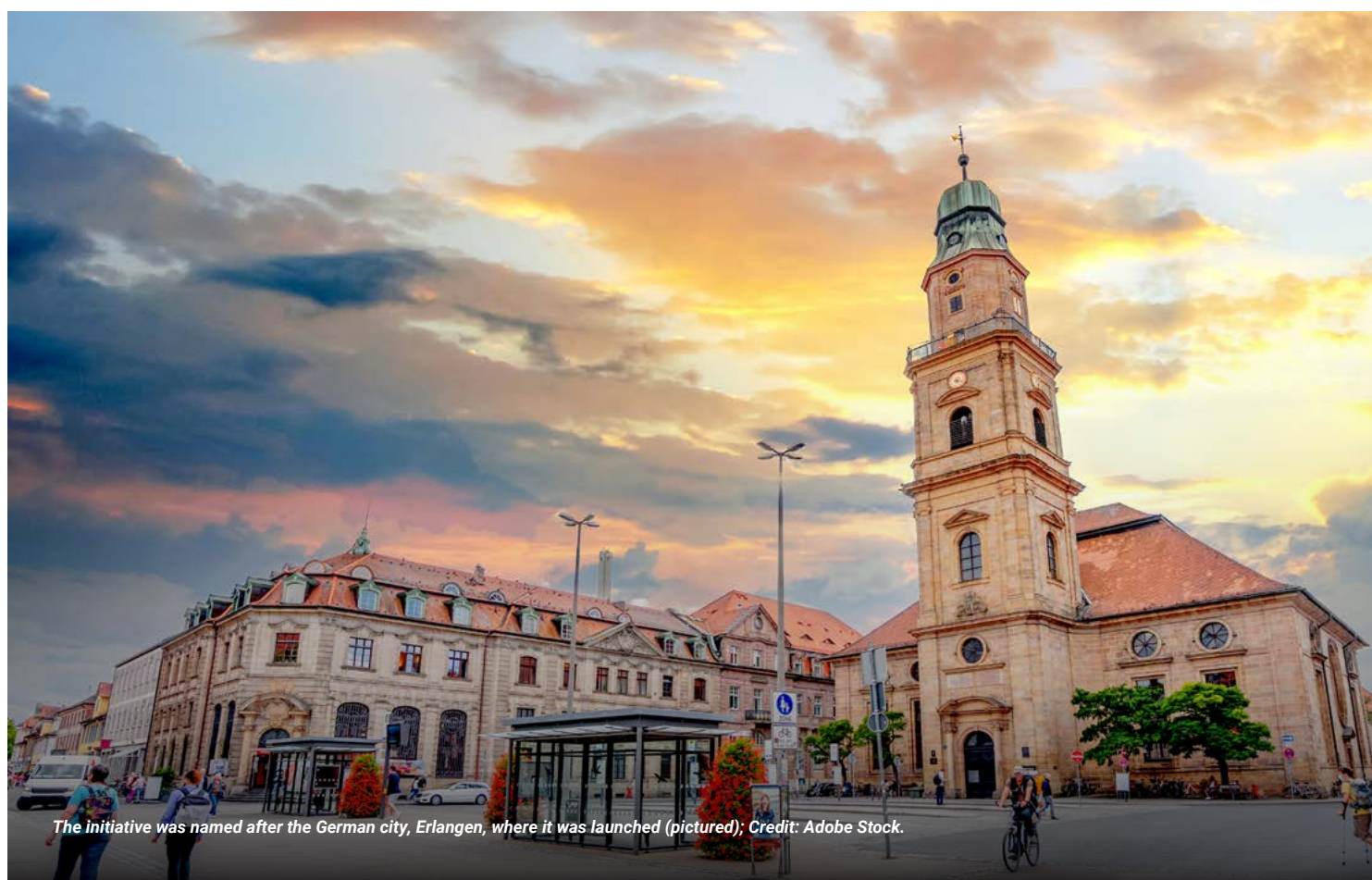
the application of national laws and/or ethical codes of conduct and thus be familiar with having to adhere to sets of rules when conducting research, while in other disciplines, researchers may have worked free from such considerations so far. In addition, to what extent research results are security-relevant, how interconnected research projects are on an international level, and to what extent ITT vs. physical exports play a role may differ between disciplines. After commencing awareness-raising programmes, it could then be helpful for regulators to consider additionally approaching scientists of same academic disciplines directly and tailoring outreach

formats to field-specific subgroups. Scientists expressed their hope that the introduction of internationally unified recommendations or even legally binding definitions could enhance their understanding of the aims and the scope of controls in place.

## **CONCLUSION**

The involvement of and cooperation with academia is increasingly important to advance general compliance with export controls and the implementation of UNSCR 1540 (2004) on a global scale. Exchange between regulators and academia in the framework of the Erlangen Initiative revealed the need to shape a specific-

ly designed outreach for this target group, reflecting their unique circumstances and challenges when conveying export control compliance needs. In any case, there is the shared understanding that responsibility for export control lies with both the regulator and academia, and that it is imperative for regulators worldwide to continue establishing and maintaining open channels of communication with this important target group. BAFA as the organizer of the Erlangen Conferences will collect the conference proposals on effective methods and key elements of outreach to academia in a good practice paper to refer to for all interested stakeholders.



*The initiative was named after the German city, Erlangen, where it was launched (pictured). Credit: Adobe Stock.*





# PRIVATE COMPANIES AND RESOLUTION 1540 (2004): A COMPLEMENTARY PAS DE DEUX

*Fermenters are an example of the dual-use dilemma that many businesses face; Credit: Jennifer Yung.*

## ABSTRACT

This article explores the evolving role of private companies—especially those involved with dual-use goods—in supporting national implementation measures of United Nations Security Council resolution 1540 (2004), such as export controls and border security. It highlights the challenges posed by technological innovation, including 3D printing and AI, and emphasizes the need for greater industry awareness and engagement. Looking ahead to the 2027 open consultations, the article calls on private sector actors to actively participate in shaping a balanced regulatory framework that safeguards global security without unduly burdening legitimate trade.



THE AUTHOR:  
**Bernard Galéa**



Bernard Galéa is the Founding President of AUMA Partners, a boutique firm built around three main pillars, both in France and internationally: strategic consulting for C-Suite, operational support, assistance to organizations (legal, public affairs, or security/risks departments). He is also Senior Advisor for ESL & Rivington, a European firm leader in Strategic Business Intelligence & Diplomacy and Advisor for French Foreign Trade. He is an Officer of the French Legion of Honour.

Dual-use technologies and materials—in other words, technologies and materials that can have both civilian and military applications—pose particular regulatory and security challenges for States, as well as non-State actors, such as private companies. While governments bear the formal responsibility of implementation and oversight, private companies increasingly find

themselves on the frontlines of non-proliferation efforts. Within this evolving dynamic, United Nations Security Council resolution 1540 (2004) underscores a quiet yet essential choreography between States and non-State actors, including industry.

The 1540 Committee, a subsidiary body of the Security Council established under

Article 29 of the UN Charter, is tasked with implementing Security Council resolution 1540 of 28 April 2004. However, unlike other committees established by the Security Council, the 1540 Committee is not a sanctions—nor a verification or investigative—committee. The 1540 Committee takes a preventative approach, emphasizing national capacity-building to deter the proliferation



of nuclear, biological, and chemical (NBC) weapons.

Unlike traditional treaties, which apply only to States, resolution 1540 broke new ground by targeting a legal blind spot: non-State actors. The resolution focuses on the connections that may exist between non-State actors and the proliferation of NBC weapons, as well as their means of delivery and related materials, which are considered a threat to international peace and security. Non-State actors include not only terrorist groups, but also commercial entities—manufacturers, suppliers, shippers, and financiers—whose products or services might be repurposed for hostile ends.

### **RESOLUTION 1540 AND THE 1540 COMMITTEE: A UNIQUE APPROACH IN THE INTERNATIONAL FIGHT AGAINST THE DIVERSION OF NBC WEAPONS BY NON-STATE ACTORS**

The resolution imposes binding obligations on States to take domestic measures to prevent the proliferation of these weapons by non-State actors. This represents a significant legal innovation—it

addresses a gap in international law, which does not recognize non-State actors as subjects of international law and who therefore cannot be included in non-proliferation treaties for NBC weapons. Resolution 1540 thus supplements the non-proliferation regime that applies to States through conventional texts by including non-State actors.

To operationalize these obligations, States are required to establish domestic implementation measures, notably export controls, customs checks at borders, and more generally, law enforcement controls. These practical mechanisms are intended to address the absence of a universal international export control regime. These obligations have very practical consequences for Member States. The text covers most aspects of non-proliferation and calls on all public services and national administrations to act, whether in foreign affairs, defence, intelligence services, customs, police, criminal courts, financial intelligence units, or trade and industry.

Importantly, resolution 1540 does not focus solely on armed terrorist groups; it applies to all types of non-State actors.

As threats evolve and proliferation channels diversify, the risk that materials listed in resolution 1540 could fall into the hands of non-State actors remains high, according to the Permanent Mission of France to the UN.

One illustrative example is the threat of bioterrorism. Although biological attacks are rare, their consequences can be severe. The 2001 anthrax attacks in the United States, along with more recent foiled attempts involving ricin in Europe, demonstrate the continuing relevance of this threat. While terrorist non-State actors mostly use conventional weapons, the Global Terrorism Database has recorded 37 cases of biological terrorism since 1970 (Ricin, Anthrax, Salmonella, Botulinum, HIV infected razor blades).

Though resolution 1540 does not provide a clearly defined list of private companies that may fall under its scope, this information can be inferred from the provisions of operative paragraphs 3 (a) and (b)—“control,” in other words, “securing” dual-use goods related to NBC materials and means of delivery. Similarly, the following operative paragraphs, (c) and (d)—“border and export

“

**In the agri-food industry, pharmaceuticals, cosmetics, biotechnology in general, chemicals, mining, mechanical engineering, and of course, the nuclear industry, all may engage with materials or equipment that could be repurposed for illicit ends.**

”

control,” including transport, maritime transshipment, and prevention of proliferation financing activities—also apply. This summary of the main points is not exhaustive. Dual-use goods, under the meaning of 1540, are defined as materials, equipment, and technologies that could contribute to proliferation.

As a result, a wide range of industrial sectors are implicated. For example, in the agri-food industry, pharmaceuticals, cosmetics,

biotechnology in general, chemicals (especially those using substances listed in the Chemical Weapons Convention that entered into force on 29 April 1997), mining, mechanical engineering, and of course, the nuclear industry, all may engage with materials or equipment that could be repurposed for illicit ends. Yet, awareness of the resolution among these industries remains uneven. Outside of the defence sector, relatively few companies are familiar with its scope and implications.

Adding further complexity is the rapid pace of technological advancement. Resolution 1540 also calls on States, though without specifying a clear scope, to take emerging technologies into account. Therefore, certain scientific and technological advances constitute new challenges that resolution 1540 must consider, such as 3D printing, the use of the dark web, the development of cyber capabilities, AI, drones... as well as cryptocurrencies for financing purposes or innovative materials like

nanotechnologies or advanced composites. The resolution calls on States to consider new developments such as those mentioned yet stops short of outlining a formal framework. The result is a regulatory landscape that struggles to keep pace with innovation.

The issue of means of delivery remains central to the effective implementation of resolution 1540. Despite the growing complexity of supply chains, relatively few countries have implemented specific controls over means of delivery. This is concerning given that certain standard industrial equipment, depending on its specifications, could serve dual-use purposes. For instance, the pharmaceutical and agri-food industries use pumps, steel, fermenters, and centrifuges; depending on their specifications, these types of equipment may constitute dual-use goods. Although the use of an agri-food centrifuge in the nuclear field is generally inappropriate due to fundamental differences in technical requirements, this does not prevent malicious non-State actors from being tempted to divert such items to support weapons programmes.

Fermenters are another relevant example of this

dual-use dilemma. Fermenters (batch, fed-batch, continuous fermentation) play a crucial role in various industries by enabling the efficient and controlled production of biological substances. Their ability to maintain optimal conditions for microorganism growth makes them an indispensable tool in modern biotechnology. While their civilian applications are well known in the agri-food industry (for the production of dairy items, such as yogurt and cheese) and in the pharmaceutical industry (for drug production, such as antibiotics, vaccines, biopharmaceuticals, enzymes, and recombinant proteins), they could also be diverted for military applications to manufacture pathogenic agents for biological warfare.

Thus, dual-use fermenters and technologies represent a complex challenge for international security and underscore the critical role that private companies must play. While dual-use goods offer significant benefits for civilian applications, their potential misuse for malicious purposes necessitates constant vigilance and international cooperation to ensure their responsible and secure use. Companies must comply with strict national reg-

ulations regarding the handling and trade (that is to say the purchase, transport, sale...) of these sensitive materials and items that may constitute dual-use goods. A violation of obligations under resolution 1540 can severely damage a company's reputation. Yet, only a few companies, apart from those in the defence industry, are familiar with resolution 1540.

### **EFFECTIVE PARTNERSHIPS WITH CIVIL SOCIETY: THE OPPORTUNITY PRESENTED BY THE 2027 OPEN CONSULTATIONS**

Resolution 1540 does not just impose constraints, it also opens the door for constructive engagement. The Office for Disarmament Affairs (UNODA) actively encourages partnerships with civil society, the private sector, and industry to support national and international efforts to achieve the resolution's objectives. In 2012, the Office for Disarmament Affairs, in cooperation with Germany, convened the first conference of international, regional, and sub-regional industry associations on resolution 1540 (2004), attended by professional associations and private companies from the nuclear, chemical,

“

**The private sector, knowingly or not, holds many of the levers that determine whether dual-use technologies are safeguarded or subverted. Recognizing their role, equipping them with the tools to comply, and inviting them to the policy table are not optional steps**

”

biological, financial, land, air, and maritime transport, and aerospace sectors.

Approximately every five years, open consultations are organized by UNODA, offering qualified civil society members within the resolution’s scope (private companies, trade associations...) a unique opportunity to speak out and propose the establishment of rules that limit trade impacts while meeting the requirements of resolution 1540 (2004). This means that, before December 2027, as stipulated in resolution 2663 (2022), a full review of 1540

is expected to take place and will offer an excellent platform for companies to demonstrate their commitment to the issue, enhancing their reputation and customer trust.

Consultations with civil society are expected to occur prior to this review, probably around May or June 2027. This represents an opportunity for companies to engage more actively with the subject, participate in Security Council discussions on challenges and operational complexities, and make suggestions for effectively implementing controls

while minimizing the impact on their supply chain.

Ultimately, resolution 1540 reflects a broader truth: that securing global peace requires more than government action alone. The private sector, knowingly or not, holds many of the levers that determine whether dual-use technologies are safeguarded or subverted. Recognizing their role, equipping them with the tools to comply, and inviting them to the policy table are not optional steps—they are essential movements in the shared dance of global security.



# UPCOMING EVENTS

## April 2025

Sihanoukville, Cambodia (Asia)

23/  
25

### **UNSCR 1540 National Action Plan Workshop for Cambodia and the Updating of its UNSCR 1540 National Report**

Organizer: UNODA

A national workshop with the aim of making progress on Cambodia's 1540 national implementation action plan and updating its national report.

## May 2025

Bangkok, Thailand (Asia)

06/  
08

### **Joint Regional Outreach Workshop (BWC, UNSCR 1540 and UNSGM)**

Organizer: UNODA

An outreach workshop looking at raising awareness of the synergies between the three instruments.

Jakarta, Indonesia (Asia)

20

### **Senior Officials Dialogue on STM in Indonesia**

This one-day workshop provides senior officials with the opportunity to discuss the role of strategic trade management in Indonesia.

## June 2025

Colombo, Sri Lanka

10/  
12

**Promoting implementation of UN Security Council Resolution 1540 and Dual-Use Goods' Strategic Trade Management Workshop for High-Level Officials**

Organizer: UNODA

A workshop for high-level officials from Bangladesh, Maldives and Sri Lanka to promote the implementation of UNSCR 1540 in the context of dual-use goods.

## October 2025

Tashkent, Uzbekistan (Asia)

TBD

**Sub-regional BWC Point of Contact Workshop for Central Asian States and Mongolia**

Organizer: BWC ISU

A sub-regional workshop to enhance implementation of the BWC and strengthen the network of POCs.



# NOTIFICATIONS

## Sparking dialogue in Geneva: resolution 1540 and export control regimes

Both resolution 1540 and export control regimes play a vital role in global non-proliferation efforts, yet these complex and, at times, overlapping mechanisms are often not fully understood. In order to bridge this knowledge gap and foster dialogue on the issue, the Geneva Centre for Security Policy (GCSP) hosted a workshop on 4 February 2025 that brought together over 50 diplomats and professionals from international organizations and export control regimes. This gathering provided an invaluable opportunity for both participating and non-participating States to engage with experts and discuss ways to improve dialogue and transparency in non-proliferation efforts.

### LOCATION



**GENEVA,  
Switzerland**

### PARTICIPATION



**Over  
50  
diplomats  
and  
international  
professionals  
participated**

### PRESENTATION



**4  
export control  
regimes presented  
+ resolution 1540**

## Three key takeaways from the event

1. The Geneva disarmament community recognise that export controls need to be discussed in the context of non-proliferation and disarmament efforts.
2. Non-participating States are interested in engaging with the export control regimes to better understand their decision-making.
3. The GCSP provides a less polarised atmosphere to reflect on the peaceful uses of technology.





