Artificial Intelligence

Report of the Scientific Advisory Board's Temporary Working Group

SAB/REP/1/26
March 2026

Page left intentionally blank

ACKNOWLEDGEMENTS

The members of the TWG on AI wish to express their sincere appreciation to all who contributed to this report.

Most notably, TWG members extend their deepest thanks to the external speakers, who took the time out of their busy schedules to share their experience and expertise. The rich diversity of their technical, scientific, and policy perspectives were the driving forces behind the TWG's discussions and the primary foundation for the recommendations presented here.

The TWG on AI is also grateful to the Director-General of the OPCW for his leadership and for prioritising engagement on emerging technologies in support of the Convention. The TWG's work was further made possible by the Technical Secretariat—its staff and interns—whose expert input and logistical coordination were essential throughout the Group's mandate.

Finally, the TWG thanks the European Union and the United States of America for the financial support that enabled the Group's activities, and China for hosting the second meeting in Shanghai.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Abbreviation	Definition
AI	Artificial intelligence
API	Application programming interface
AR	Augmented reality
ASMR	Autonomous sensory meridian response
CBRN	Chemical, biological, radiological, and nuclear
ChemTech Centre	Centre for Chemistry and Technology
Cloud lab	Cloud laboratory
Convention	Chemical Weapons Convention
CWA	Chemical warfare agent
DPIA	Data protection impact assessment
EU	European Union
EU-SENSE	European Sensor System for CBRN Applications
FTIR	Fourier-transform infrared (spectroscopy)
GC-MS	Gas chromatography-mass spectrometry
Global Conference	Global Conference on the Role of Artificial Intelligence in Advancing the Implementation of the Chemical Weapons Convention
GNN	Graph neural network
HRIA	Human rights impact assessment
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
INTERPOL	International Criminal Police Organization
IR	Infrared (spectroscopy)
ISO	International Organization for Standardization
IT	Information technology
ITU	International Telecommunication Union

ITU-T	International Telecommunication Union Telecommunication Standardization Sector
IUPAC	International Union of Pure and Applied Chemistry
LC_{50}	Lethal concentration 50%
LD_{50}	Lethal dose 50%
LLM	Large language model
ML	Machine learning
MR	Mixed reality
MS	Mass spectrometry
MS/MS	Tandem mass spectrometry
NAS	National Academies of Sciences, Engineering, and Medicine of the United States of America
NMR	Nuclear magnetic resonance (spectroscopy)
OPCW	Organisation for the Prohibition of Chemical Weapons
PPE	Personal protective equipment
RACI	Responsible, accountable, consulted, informed
REAIM	Responsible Artificial Intelligence in the Military Domain
SAB	Scientific Advisory Board
SDL	Self-driving laboratory
Secretariat	Technical Secretariat
SIPRI	Stockholm International Peace Research Institute
TOR	Terms of Reference
TWG	Temporary Working Group
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNICRI	United Nations Interregional Crime and Justice Research Institute
VR	Virtual reality
XR	Extended reality

PLAIN-LANGUAGE SUMMARY

1. Artificial intelligence (AI) is developing rapidly and increasingly affecting chemistry, scientific research, and international verification activities. Recognising its potential, the OPCW established a Temporary Working Group (TWG) to examine how AI is already shaping chemical science, how it may evolve in the near future, and how the Organisation can use AI responsibly while managing potential risks.

2. AI tools can help scientists and inspectors work more efficiently. For example, AI can analyse complex chemical data, assist with planning inspections, support training through simulations, and help identify patterns or anomalies in large datasets such as declarations. These capabilities could strengthen the Organisation's ability to understand emerging chemical threats and improve operational effectiveness.

3. At the same time, AI introduces new challenges. Some tools that accelerate legitimate research could also be misused to design harmful chemicals more quickly or with less specialised expertise. Increased automation and remote access to scientific capabilities may also change how chemical activities are conducted, requiring updated approaches to monitoring and oversight.

4. The TWG concludes that AI should be seen as a cross-cutting issue that will increasingly shape chemical science and international security. It provides recommendations (see Table 1) for the OPCW in five key areas: monitoring AI; outreach and engagement; verification; organisational readiness and training; and capacity building.

5. Overall, AI presents both opportunities and risks. With careful governance and proactive engagement, it has the potential to strengthen implementation of the Convention while supporting safer and more effective chemical activities worldwide.

EXECUTIVE SUMMARY

6. The rapid acceleration of AI across scientific, industrial, and governmental domains presents both significant opportunities and novel challenges for the implementation of the Chemical Weapons Convention (the Convention). In recognition of the transformative potential of these technologies, and of their increasing relevance to chemistry, verification, and organisational effectiveness, the Director-General of the OPCW established a TWG of the Scientific Advisory Board to review the current and near-term implications of AI for the OPCW. An overview of the TWG is provided in Figure 1. The mandate of this Group was to provide a structured, forward-looking assessment of how AI is influencing chemical science and related disciplines, how it may further evolve over the coming years, and how the Organisation can responsibly harness its benefits while remaining alert to associated risks.

7. AI, as considered in this report, encompasses a broad set of computational techniques that enable systems to perform tasks traditionally requiring human intelligence, including pattern recognition, prediction, optimisation, language processing, and autonomous decision support. Recent advances, driven by increased data availability, computing power, and the emergence of large and multimodal models, have significantly lowered barriers to adoption and expanded the range of feasible applications. These developments are occurring not only within highly specialised research environments, but increasingly through commercially available platforms and open-source tools accessible to a wide user base. The TWG therefore examined AI not as a single technology, but as an evolving ecosystem with implications that cut across chemistry, verification practices, training, capacity building, and governance.

8. The work of the TWG was informed by a broad range of expertise, including TWG members, SAB members, OPCW Technical Secretariat (the Secretariat) staff, and invited experts. Its deliberations were shaped by engagement with Secretariat staff involved in verification, inspection, and training activities, ensuring that the assessment was grounded in operational experience and practical constraints. Throughout, the TWG focused on AI developments of direct relevance to the Organisation's mandate and to States Parties, rather than on speculative or long-term technological possibilities.

9. One of the TWG's core findings is that AI is already reshaping core areas of chemical science that are directly relevant to the Convention. In chemical research and development, AI-enabled modelling, retrosynthesis planning, and exploration of chemical space are accelerating the identification of viable synthetic routes, optimising reaction conditions, and enabling the prediction of physicochemical and

toxicological properties. When responsibly applied, these tools offer opportunities to enhance the Organisation’s ability to anticipate and understand novel chemicals of concern, including potential future threats that may not be explicitly captured by existing schedules. At the same time, the same tools could be misused to lower the expertise and time required to design or modify toxic chemicals, underscoring the importance of situational awareness and proactive engagement.

10. The TWG notes particular relevance in the emerging integration of AI with automated laboratories. While such systems remain most prevalent in advanced research settings, their increasing modularity, commercial availability, and remote operation capabilities suggest a trajectory towards wider dissemination and commercial adoption. Reduced dependence on tacit human expertise, coupled with digital access models, could alter traditional indicators of chemical weapons-relevant activity. The Organisation will therefore need to monitor these developments systematically and build internal capability to evaluate both their legitimate applications and their potential misuse.

11. AI also offers clear opportunities to augment verification activities. In its findings, the TWG highlights the potential value of AI-supported processing of declarations. This could include the digitisation of historical and current submissions, automated extraction and structuring of relevant data, and secure, searchable storage that preserves traceability and auditability. Properly designed human-in-the-loop systems could enhance efficiency, consistency, and institutional memory, while retaining expert judgement and accountability. In parallel, AI techniques can support the identification of patterns, inconsistencies, or anomalies within large and complex datasets, complementing existing verification methodologies rather than replacing them.

12. Beyond declarations, AI-enabled analysis of open-source information, including satellite imagery and other publicly available data, was identified as a means to improve mission preparation and situational awareness. Such applications can contribute to inspector safety and operational effectiveness by informing logistical planning and risk assessment. The TWG emphasised that these tools should be integrated thoughtfully into established processes, with clear governance and validation, to ensure reliability and appropriate use.

13. Training and capacity development emerged as another area where AI could deliver substantial benefits. AI-enhanced extended reality and simulation tools offer new possibilities for inspector training, particularly for complex or non-routine scenarios that are difficult to replicate safely in the physical world. Dynamic, adaptive simulations can strengthen technical preparedness, decision-making, and communication skills. Similarly, AI-based simulation of chemical facilities and

incident scenarios can support inspector training, and may in future contribute to the development of embodied intelligence, including the use of autonomous systems.

14. In analytical chemistry, AI is increasingly used to support chemical detection and identification, particularly through the analysis of complex spectral data and the fusion of information from multiple sensors. The TWG finds that bespoke AI models, developed and validated for specific analytical contexts, could enhance sensitivity, speed, and robustness, including in remote monitoring systems. Engagement with OPCW Designated Laboratories and other expert communities will be essential to understand the maturity and limitations of these approaches and to ensure that performance claims are independently verified.

15. At the organisational level, this report underscores that effective use of AI will depend not only on technology acquisition, but also on infrastructure, staffing, governance, and culture. The Secretariat will need access to expertise in data science, software engineering, and AI governance to act as an informed user and evaluator of these tools. Secure computing environments, data governance frameworks, and clear policies on acceptable use are prerequisites for responsible deployment. The TWG also recognises the potential value of secure, custom-built AI assistants to support operational and analytical tasks, as well as administrative functions, provided they operate within controlled environments and are accompanied by appropriate training.

16. In its in-depth review, the TWG paid particular attention to emerging risks associated with AI. Large language models, open-source synthesis tools, and automated platforms can be used intentionally or unintentionally in ways that undermine the Convention. Misuse may arise not only from malicious intent, but also from lack of awareness, insufficient expertise, or over-reliance on automated outputs. The development of indicators to help recognise potential AI misuse, and the sharing of such indicators with States Parties, was therefore identified as an important preventive measure.

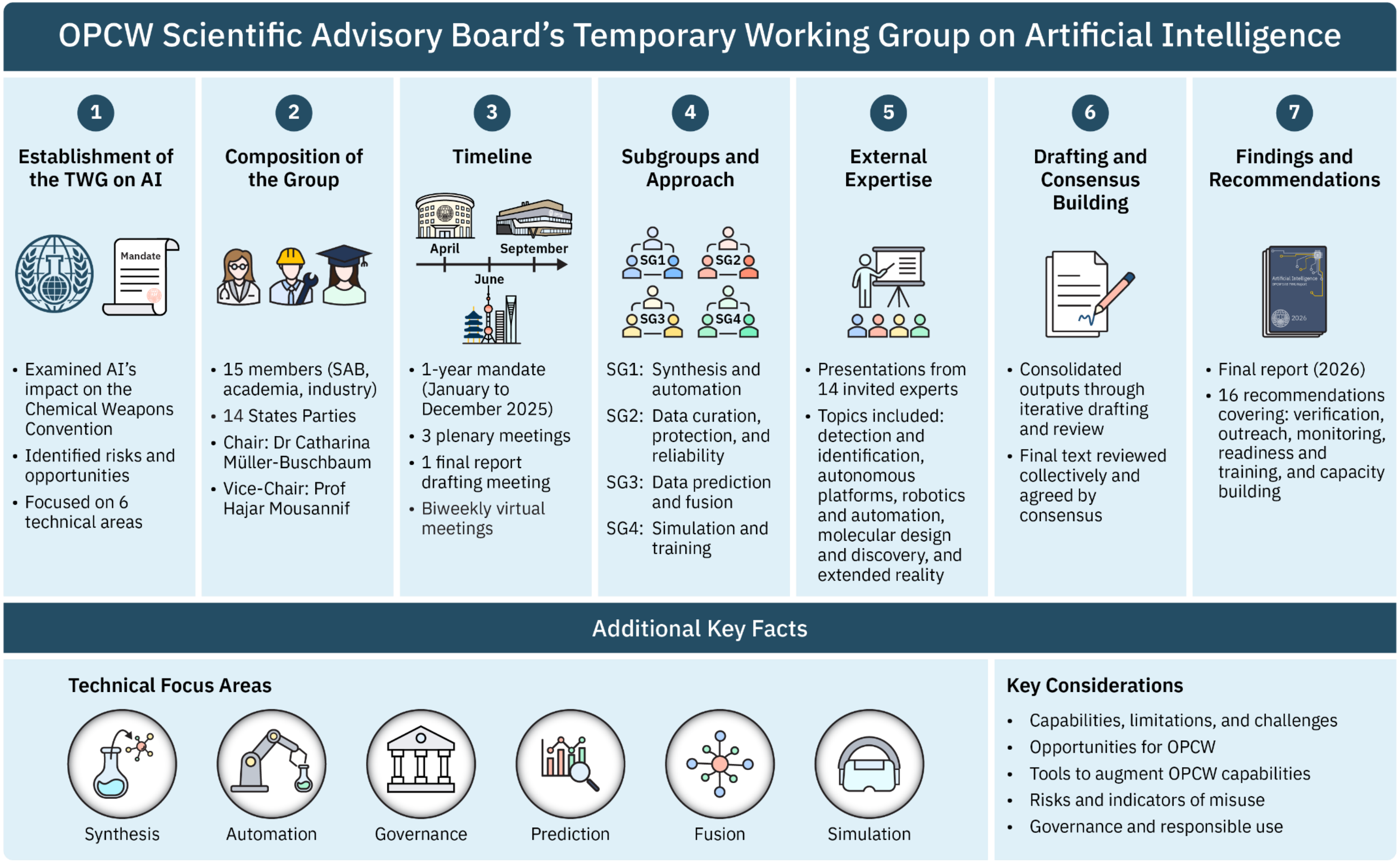
17. Given the pace of change, the Group concludes that no single, time-limited assessment can remain sufficient. Continued monitoring of scientific and technological developments, including industry trends, will be essential. This may involve periodic internal assessments, engagement with external experts, and targeted exercises to explore real-world use cases. Active participation in international dialogues on AI ethics, safety, and governance will further support the Organisation's ability to remain informed and relevant.

18. The implications for States Parties are significant. AI will increasingly shape chemical research, industrial practice, and regulatory oversight. There is therefore a shared interest in building awareness of both opportunities and risks, strengthening data

governance and management capabilities, and promoting safe and responsible use of AI in chemistry. Capacity-building initiatives can enhance chemical safety and emergency response, with AI-based simulations of chemical facilities, processes, and incident scenarios offering particular potential to augment training capabilities in the chemical industry. Collaborative approaches, such as twinning initiatives between States Parties with differing levels of AI maturity, can facilitate knowledge exchange and foster a common understanding of responsible AI use within the context of the Convention.

19. In light of these findings, the TWG has identified a set of recommended actions that the OPCW should undertake. These actions support core areas including continued monitoring, outreach and engagement, verification activities, organisational readiness and training, and capacity building, and are summarised in Table 1.

20. Taken together, these findings and recommended actions underscore that AI is neither a peripheral nor a purely technical issue for the OPCW. It is a cross-cutting development that, if approached strategically and responsibly, can strengthen implementation of the Convention, enhance verification and preparedness, and support States Parties in addressing shared challenges, while preserving the core principles of transparency, accountability, and international cooperation.



OPCW Scientific Advisory Board's Temporary Working Group on Artificial Intelligence

1 Establishment of the TWG on AI

- Examined AI's impact on the Chemical Weapons Convention
- Identified risks and opportunities
- Focused on 6 technical areas

2 Composition of the Group

- 15 members (SAB, academia, industry)
- 14 States Parties
- Chair: Dr Catharina Müller-Buschbaum
- Vice-Chair: Prof Hajar Mousannif

3 Timeline

- 1-year mandate (January to December 2025)
- 3 plenary meetings
- 1 final report drafting meeting
- Biweekly virtual meetings

4 Subgroups and Approach

SG1: Synthesis and automation

SG2: Data curation, protection, and reliability

SG3: Data prediction and fusion

SG4: Simulation and training

5 External Expertise

- Presentations from 14 invited experts
- Topics included: detection and identification, autonomous platforms, robotics and automation, molecular design and discovery, and extended reality

6 Drafting and Consensus Building

- Consolidated outputs through iterative drafting and review
- Final text reviewed collectively and agreed by consensus

7 Findings and Recommendations

- Final report (2026)
- 16 recommendations covering: verification, outreach, monitoring, readiness and training, and capacity building

Additional Key Facts

Technical Focus Areas

Synthesis

Automation

Governance

Prediction

Fusion

Simulation

Key Considerations

- Capabilities, limitations, and challenges
- Opportunities for OPCW
- Tools to augment OPCW capabilities
- Risks and indicators of misuse
- Governance and responsible use

Figure 1: TWG on AI in summary

RECOMMENDATIONS

Table 1: Summary of recommendations

Continued monitoring	
1	Given the continued rapid development of AI and its growing integration into scientific activities, and considering the time-limited mandate of this TWG, the OPCW should continue to actively monitor AI developments and their potential impacts on its work. This could include periodic assessments conducted by Secretariat staff, convening meetings of experts, or establishing specific focus groups of the SAB, or a combination of these approaches. Such monitoring would cover both general advances and industry trends, with attention to opportunities for, and risks to, the effective implementation of the Convention.
2	While automated laboratories are currently most widely deployed in advanced research environments, the field is rapidly professionalising. Commercial platforms, modular synthesis hardware, and AI-enabled orchestration tools are lowering operational barriers and enabling increasingly remote and automated workflows. To remain proactive, the TWG recommends that the OPCW formally monitor these developments and build internal capability to evaluate both opportunities and emerging risks. This should include systematic engagement with leading academic and industrial developers, periodic technical assessments, and targeted exercises to explore real-world use cases. Particular attention should be given to understanding how reduced reliance on human expertise, remote execution, and digital access models may evolve, as well as to identifying governance mechanisms that support responsible innovation while safeguarding against misuse.
Outreach and engagement	
3	The Secretariat should continue to strengthen relationships with external organisations and stakeholders whose work aligns with the OPCW's mandate. This may include AI ethics and safety frameworks, as well as relevant United Nations bodies, multilateral organisations, States Parties, and non-governmental organisations. Ongoing engagement in these international dialogues will help the OPCW remain informed about developments in AI and identify areas warranting further attention.
4	The Secretariat should maintain an up-to-date list of vendors offering AI-enabled synthesis and retrosynthesis platforms and related computational

chemistry solutions, with special attention given to open-source and proprietary platforms that are accessible to the public with no verification process. The OPCW should attempt to raise awareness of Convention-related risks with these companies and promote active governance approaches.

5 The OPCW should build strategic partnerships with relevant AI and chemistry communities, as well as with leading publishers and academic journals that highlight the latest research in these fields, to facilitate dialogue between AI developers, chemists, and arms control experts. These partnerships would afford an opportunity to provide AI developers with a greater awareness of the Convention, the potential risks of AI in this context, and the work of the OPCW.

6 The OPCW should develop a list of indicators to identify AI misuse, which would enable authorities in States Parties to recognise such instances. Misuse of AI may be intentional, by a nefarious actor, or unintentional, arising from inadvertent mistakes, a lack of awareness, or insufficient expertise. Potential indicators may include:

a. acquisition or synthesis of scheduled or toxic chemicals, or novel derivatives/analogues, without legitimate context;

b. unusual query patterns on synthesis platforms;

c. use of anonymised application programming interfaces for sensitive queries; and/or

d. rapid prototyping of novel precursors or intermediates.

The Secretariat may consider holding a series of workshops with experts from States Parties to develop this list.

OPCW verification activities

7 The Secretariat should design, develop (or otherwise acquire and adapt), and implement a human-in-the-loop AI system to support the processing of declarations. This system should include the following core capabilities:

a. digitisation of declarations (historical and current): ability to convert all submissions into machine-readable format, to translate declarations (from multiple languages) following text conversion, and to preserve original submission fidelity;

b. data extraction and structuring: ability to extract relevant data fields from digitised declarations, to structure data in a format suitable for downstream analysis and reporting, and to enable an expert review process for all records that allows editing and approval for completion; and

c. secure storage and accessibility: ability to store digitised and structured data in a secure, queryable database (semantic search/retrieval enabled) and ensure traceability and auditability of all transformations and validations.

Ongoing and future software procurement, as well as information technology infrastructure modernisation, should consider compatibility with AI systems as part of the evaluation criteria.

8 The Secretariat should review OPCW verification practices to identify specific areas that could be enhanced by AI technologies. Possible applications include pattern recognition tasks—such as the detection of inconsistencies or anomalies in declarations—alongside remote sensing, risk assessment generation, and the analysis of open-source data through data mining.

9 The Secretariat should evaluate existing—and, where necessary, develop—AI models to augment chemical detection and identification capabilities. These bespoke models should support the analysis of spectral data, evaluate the utility of multi-sensor fusion for chemical identification, and validate the performance of AI-driven pattern recognition in remote monitoring systems (such as sensors deployed on uncrewed platforms). Outcomes from the OPCW AI Research Challenge may provide useful inputs in this regard. Workshops with OPCW Designated Laboratories could further help identify promising AI models suitable for integration into analytical chemistry workstreams.

Organisational readiness and training

10 The Secretariat should seek to hire staff with expertise in AI, including data scientists and software engineers. Expertise in this area is critical for the OPCW to fully leverage advances in AI in its work.

11 AI-supported extended reality tools should be developed and deployed to train operational Secretariat staff, including inspectors and staff in the Office of Special Missions. Development should be based upon a detailed scenario and user-needs analysis and supported by a clear concept of operations. Key requirements for extended reality training tools should include:

a. realistic, dynamic training scenarios, including contingency operations, with AI-generated injects;

b. integration with real equipment, such as detectors and personal protective equipment;

c. user-defined scenario creation;

d. instructor oversight, including real-time intervention and performance evaluation tools;

e. AI-driven evaluation and feedback;

f. secure, controlled operation, including offline capability and robust data protection; and

g. advanced realism and future readiness, including non-player characters, digital twins for chemical facilities, and future sensory enhancements.

12 The Secretariat should use AI to simulate chemical facilities, production process equipment, and incident scenarios for training relevant staff, including inspectors. Multimodal foundation models should be leveraged to support training for embodied intelligence—including robots, drones, and other uncrewed or autonomous vehicles—enabling realistic and context-aware interactions across multiple data modalities.

13 The Secretariat should design, develop (or otherwise acquire and adapt), and implement a custom, secure chatbot or agent for general-use cases. The system should operate within an air-gapped, secure environment. It should be capable of both assisting with general administrative tasks—such as document translation and summarisation, drafting reports and emails, and question and answer capabilities from input documents—as well as with more specific, programmatic uses, such as:

a. providing inspectors with quick access to technical information, which may include device operation, chemical process knowledge, and relevant information on chemical production and destruction facilities; and

b. assisting in the potential procurement of equipment and technology within the OPCW Technology and Training Hub framework.

Ongoing and future software procurement, as well as information technology infrastructure modernisation, should consider compatibility with AI systems as part of the evaluation criteria. It is also essential that training on the use of the chatbot and AI best practices is provided to OPCW staff.

14 To enhance preparedness for future chemical weapons threats, the Secretariat should explore the utility of complementary AI-supported tools to systematically understand and map the chemical space surrounding known chemical warfare agents. Such tools could include AI-driven retrosynthesis and synthesis-planning approaches to identify potential novel routes to chemical warfare agents and their precursors, particularly those relying on uncontrolled or non-scheduled chemicals. They could also encompass predictive models for spectral information and other key properties relevant to risk assessment and detection, including toxicity, vapour pressure, stability, and detectability.

Capacity building

15 The Secretariat should design, develop, and implement a capacity-building programme for States Parties that:

a. provides information on the latest AI capabilities;
b. enables the recognition of AI misuse, both malicious and accidental;
c. develops data governance capabilities (including data modelling, curation, and structuring, data stewardship and ownership, and identifying access controls);
d. develops data management capabilities (data reliability and protection, enforcing access controls);
e. promotes the use of AI-supported simulation and communication tools, particularly to enhance chemical safety and emergency response capabilities; and
f. shares guidance and best practices for the safe and responsible use of AI in chemical production and research.

16 States Parties and the Secretariat should develop and establish a twinning initiative for the responsible and effective integration of AI technologies to support the implementation of the Convention. The Secretariat would facilitate partnerships enabling States Parties with advanced AI capabilities to “twin” with States Parties with emerging AI capabilities. These partnerships would support capacity-building measures, including training and technical assistance, exchange of best practices and knowledge, and the promotion of a shared understanding of responsible AI use and its potential risks within the context of the Convention.

INTRODUCTION

Background

21. Artificial intelligence (AI) refers to a broad spectrum of technologies that enable machines to perform tasks that typically require human intelligence, such as learning, reasoning, problem-solving, and decision-making. Recent advances in data availability, computational power, and algorithmic innovation have accelerated AI's capabilities, making it one of the most transformative technologies in recent decades. Its applications now span healthcare, finance, education, governance, and many other sectors, creating both unprecedented opportunities and complex challenges.

22. The rapid progress of AI is reshaping the scientific and industrial landscape, including the field of chemistry. In this domain, AI is being applied to streamline chemical synthesis, enhance toxicity prediction and risk assessment, and accelerate the digital transformation of the chemical industry. In the context of the Chemical Weapons Convention (the Convention), it is opening new possibilities for verification, supporting adaptive approaches to detecting and deterring chemical weapons proliferation. These developments present significant opportunities to further the objectives of the Convention, while simultaneously introducing new security considerations such as the development of novel toxic substances, cyber threats to chemical facilities, and the malicious use of automated weapon systems. Key technical terms used in this report are defined in the Glossary (Annex 1).

23. The development of AI as an enabling technology has been monitored by the OPCW via the Scientific Advisory Board (SAB) for more than a decade, with key events shown in the timeline in Figure 2. In its 2012 report on developments in science and technology to the Third Review Conference,[1] the SAB noted the increasing availability and global sharing of data and growing databases of chemicals, particularly biologically active chemicals.[2] In 2017, the SAB held a workshop on "Innovative Technologies for Chemical Security" in Brazil,[3] which explored the potential of new

[1] Review Conference = Special Session of the Conference of the States Parties to Review the Operation of the Chemical Weapons Convention.

[2] Report of the Scientific Advisory Board on Developments in Science and Technology for the Third Special Session of the Conference of the States Parties to Review the Operation of the Chemical Weapons Convention (RC-3/DG.1, dated 29 October 2012).

[3] This workshop was held in cooperation with the International Union of Pure and Applied Chemistry (IUPAC), the National Academies of Science, Engineering and Medicine of the United States of America (NAS), the Brazilian Academy of Sciences (ABC), and the Brazilian Chemical Society (SBQ).

technologies to enhance capabilities necessary for implementation of the Convention.[4] During this workshop, applications of AI were discussed.

24. The following year, the SAB submitted its report on developments in science and technology to the Fourth Review Conference and this report contained an entire section dedicated to big data, informatics, and AI.[5] The Board recommended that "the SAB and Secretariat should continue to assess developments in technical fields of increasing relevance to the Convention, such as computational chemistry, Big Data, informatics and artificial intelligence". Implementing this recommendation, the SAB held a two-day workshop in June 2022, which explored a variety of applications of AI in chemistry, including drug discovery, automation, and chemical synthesis planning and optimisation. This enabled the Board members to increase their understanding of the capabilities of the technology and evaluate potential opportunities and risks.

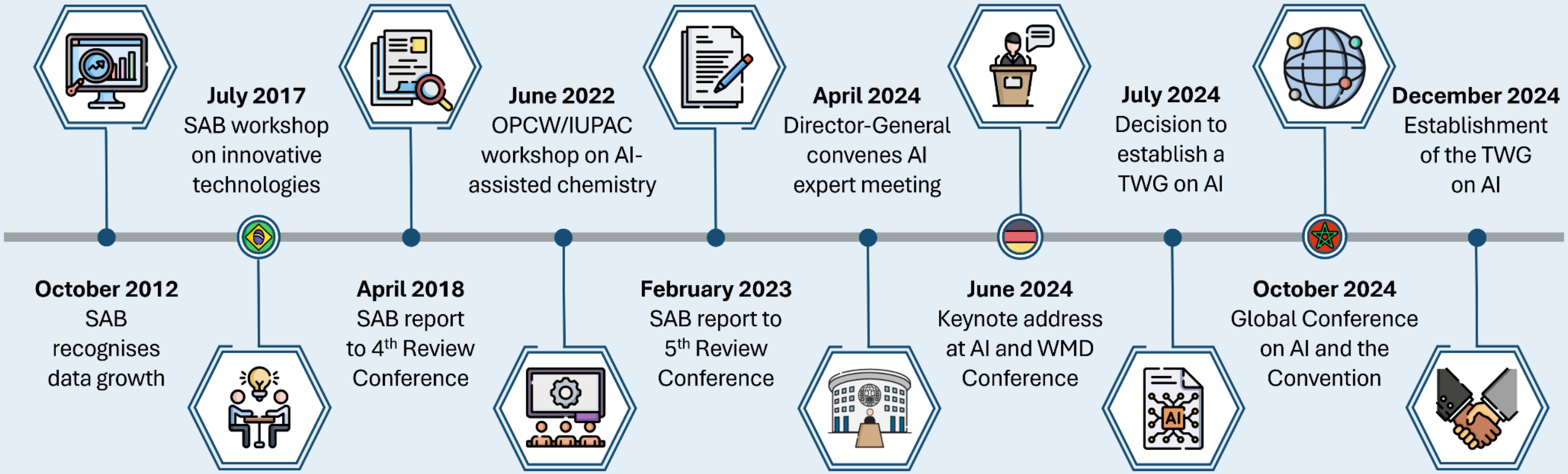
25. In paragraph 8 of its report to the Fifth Review Conference, the SAB recognised that within the context of a volatile social and political landscape, the convergence of different fields of science "presents an ever-changing set of challenges to and opportunities for the implementation of the Convention".[6] The SAB identified significant progress across various scientific and technological domains, with a particular emphasis on the notable advances in AI, additive manufacturing, and biotechnology. Moreover, in paragraph 12 of his response to that report of the SAB, the Director-General noted that the proliferation of AI has been particularly striking.[7] The SAB recommended that "the OPCW should closely monitor the rapid development in AI-assisted chemistry and machine learning and consider not just the potential risks that it poses, but also the opportunities it presents".

[4] Report of the Scientific Advisory Board's Workshop on Emerging Technologies (SAB-26/WP.1, dated 21 July 2017).

[5] Report of the Scientific Advisory Board on Developments in Science and Technology for the Fourth Special Session of the Conference of the States Parties to Review the Operation of the Chemical Weapons Convention (RC-4/DG.1, dated 30 April 2018).

[6] Report of the Scientific Advisory Board on Developments in Science and Technology to the Fifth Special Session of the Conference of the States Parties to Review the Operation of the Chemical Weapons Convention (RC-5/DG.1, dated 22 February 2023).

[7] Response to the Report of the Scientific Advisory Board on Developments in Science and Technology to the Fifth Special Session of the Conference of the States Parties to Review the Operation of the Chemical Weapons Convention (RC-5/DG.2, dated 22 February 2023).



October 2012
SAB
recognises
data growth

July 2017
SAB workshop
on innovative
technologies

April 2018
SAB report
to 4th Review
Conference

June 2022
OPCW/IUPAC
workshop on AI-assisted chemistry

February 2023
SAB report to
5th Review
Conference

April 2024
Director-General
convenes AI
expert meeting

June 2024
Keynote address
at AI and WMD
Conference

July 2024
Decision to
establish a
TWG on AI

October 2024
Global Conference
on AI and the
Convention

December 2024
Establishment
of the TWG
on AI

Figure 2: Timeline of key events, activities, and outputs related to AI at the OPCW leading up to the establishment of the TWG on AI

26. Analysing and assessing the impact of developments in science and technology, and in AI in particular, has been an ongoing priority for the Secretariat. In parallel to the SAB's review, the Secretariat has placed an increasing emphasis on AI to better understand its potential implications for the work of the Organisation, as well as to identify opportunities for its integration into OPCW workflows. A number of activities have been undertaken—and continue to be pursued—in support of this effort.

27. On 22 and 23 April 2024, the Director-General convened a meeting of AI experts at the OPCW Main Building and the Centre for Chemistry and Technology (ChemTech Centre).[8] Its aim was to elicit insights from scientific experts regarding the capabilities of the current AI technological landscape and its forthcoming prospects. The meeting was attended by 10 external experts (including two members of the SAB) with extensive knowledge and experience in several different and complementary areas of AI and its use in chemistry. It provided a basis for the Secretariat to deepen its understanding of AI, the opportunities it offers, and the potential risks it poses.

28. On 28 June 2024, the Director-General delivered the keynote address at the "Artificial Intelligence and Weapons of Mass Destruction" conference in Berlin, Germany, organised by the German Federal Foreign Office. In his address, the Director-General called for an ongoing, continuous discussion to ensure that AI enhances rather than undermines international arms control.

29. As a result of various meetings and discussions, and in recognition of the unprecedented pace of developments in AI and the OPCW's need to continue monitoring them, the Director-General announced his decision to establish a temporary working group (TWG) focused on AI at the 106th Session of the Executive Council in July 2024.[9]

30. Continuing this momentum, from 22 to 24 October 2024, Morocco and the OPCW co-hosted the "Global Conference on the Role of Artificial Intelligence in Advancing the Implementation of the Chemical Weapons Convention" (the Global Conference) in Rabat, Morocco.[10] This pioneering Global Conference explored the implications of AI technology within the framework of the Convention. A broad range of topics of relevance to AI, chemistry, and the Convention were discussed. The Global Conference was attended by 190 participants, from governments, international and

[8] Artificial Intelligence and the OPCW: A Meeting with Experts (S/2289/2024, dated 23 May 2024).

[9] Opening Statement by the Director-General to the 106th Session of the Executive Council (EC-106/DG.21, dated 9 July 2024).

[10] "Global Conference on AI in CWC Implementation." Organisation for the Prohibition of Chemical Weapons, accessed November 12, 2025.

non-governmental organisations, academia, and the chemical industry, representing 46 States Parties across all five OPCW regional groups. The diverse mix of participants, spanning a broad spectrum of expertise, contributed to rich and insightful discussions that met the conference objectives in full.[11]

Establishment of the TWG on AI

31. The objective of the TWG on AI was to understand the impact of the technology on the object and purpose of the Convention and identify the risks to and opportunities for its implementation. In the Terms of Reference (TOR)—found in Annex 2—the TWG was requested to address a series of questions, while considering the current state of the art, and expected near-term progress to be made, in six technical areas:

   a. synthesis and retrosynthesis prediction;

   b. automated and remote synthesis and production of chemicals;

   c. data curation, protection, and reliability;

   d. property, spectral, and data prediction and generation;

   e. data/sensor fusion for augmented detection and analysis; and

   f. simulation and training.

32. The TWG on AI comprised 15 members, drawn from the SAB, academia, and the technology and chemical industries, representing 14 States Parties. Dr Catharina Müller-Buschbaum of the SAB was appointed as the Chairperson of the TWG on AI and was supported by Prof. Hajar Mousannif as the Vice-Chairperson. A list of the TWG members is provided in Annex 3.

33. Following an introductory virtual meeting, the full TWG convened three times during its one-year mandate, which ran from 1 January to 31 December 2025. Two meetings (April and September) were held at the OPCW Headquarters in The Hague, the Netherlands, and the third meeting (June) was held at the operational base of the China-BRICS[12] Artificial Intelligence Development and Cooperation Center, in Shanghai, China. Summaries of these meetings will be reported to the SAB at its Fortieth Session.[13] The timeline of the TWG's mandate is shown in Figure 3.

[11] Global Conference on the Role of Artificial Intelligence in Advancing the Implementation of the Chemical Weapons Convention: a Path Forward (S/2360/2025, dated 29 January 2025).

[12] BRICS is a grouping of countries with emerging economies that includes Brazil, Russia, India, China, South Africa, and other members.

[13] (a) Summary of the First Meeting of the Scientific Advisory Board's Temporary Working Group on Artificial Intelligence (SAB-40/WP.1, dated 11 April 2025); (b) Summary of the Second Meeting of the Scientific Advisory Board's Temporary Working Group on Artificial Intelligence

34. In addition, a series of biweekly virtual meetings were held from March to November to enable the Group to share key developments in this fast-moving field and to maintain momentum during the short mandate of the TWG. A drafting meeting was held in December, which was attended by key representatives of the TWG, specifically to prepare this end-of-mandate report.

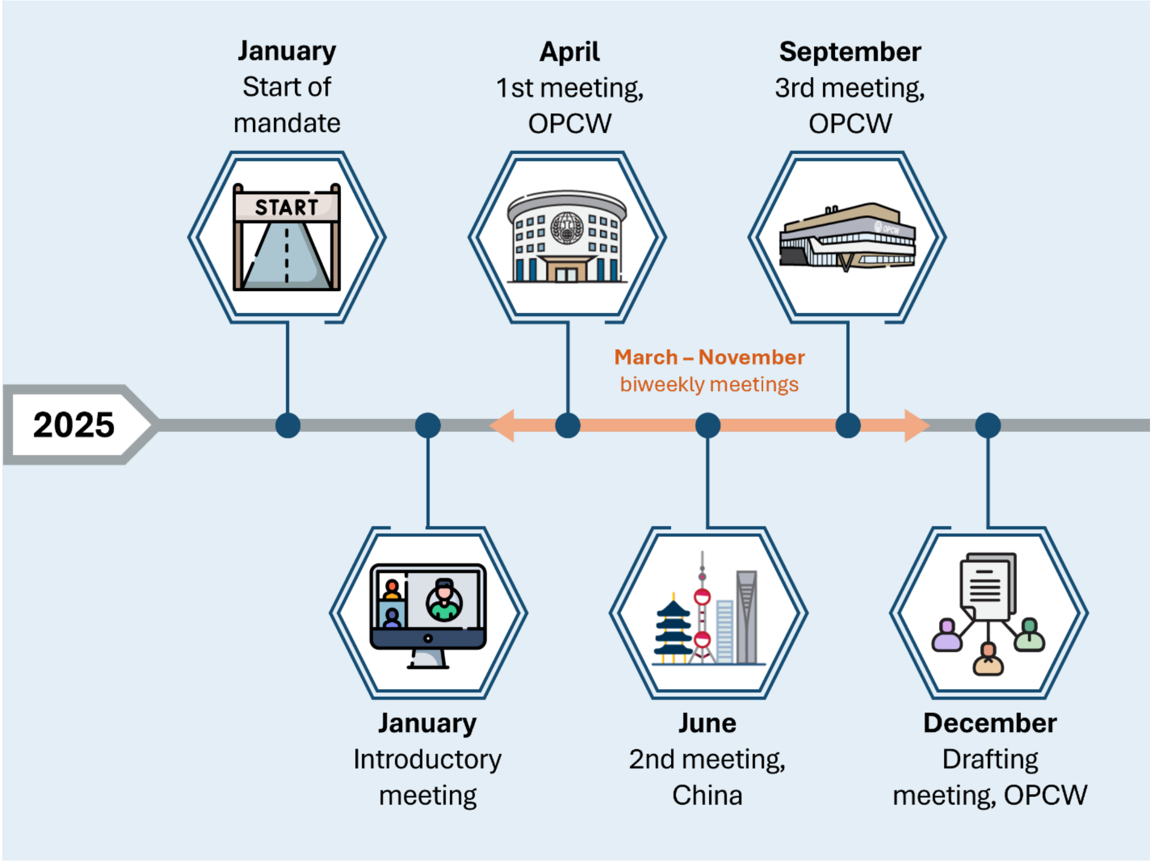


Figure 3: Timeline of the TWG's mandate

35. The work of the TWG was structured to address the TOR. First, to inform its discussions, the TWG received a total of 26 presentations: three from Secretariat staff, 10 from TWG members, and 13 from invited experts. The list of invited speakers is available in Annex 4. The presentations from Secretariat staff (Verification and Inspectorate Divisions) provided the TWG with additional context and understanding relating to the needs of the OPCW and its operational constraints. The technical presentations by TWG members and invited experts covered a broad range of topics, including detection and identification, autonomous platforms, robotics and automation, molecular design and discovery, and extended reality (XR).

(SAB-40/WP.3, dated 24 September 2025); (c) Summary of the Third Meeting of the Scientific Advisory Board's Temporary Working Group on Artificial Intelligence (SAB-40/WP.4, dated 2 December 2025).

36. The TWG also formed four subgroups—aligning with the expertise of its members—to address the six technical areas set out in the TOR in the most efficient and effective manner (see Table 2). While reviewing their respective technical areas, the TWG addressed the following questions from paragraph 7 of the TOR:

a. What new capabilities are being enabled, that is, what can be done now that was not possible before? Consider both opportunities and risks.

b. What are the current limitations and challenges to further progress, and which obstacles are likely to remain difficult or impossible to overcome?

c. What external, non-technical factors exist that may accelerate or enable progress and/or technology adoption or slow it down?

Table 2: TWG subgroups and their technical focus areas

Subgroup	Technical focus areas
1	Synthesis and retrosynthesis prediction Automated and remote synthesis and production of chemicals
2	Data curation, protection, and reliability
3	Property, spectral, and data prediction and generation Data/sensor fusion for augmented detection and analysis
4	Simulation and training

37. The TWG also explored how advances in AI will impact the implementation of the Convention and the work of the OPCW by considering the following questions from paragraph 8 of the TOR:

a. What red flags or anomalies could help in identifying the potential misuse of AI systems?

b. Which specific AI applications are sufficiently mature for the OPCW to utilise in augmenting its capabilities?

c. What changes will be seen in industry in the coming years as AI becomes increasingly integrated into chemical production processes?

d. How might AI impact verification efforts, either by increasing risks or by presenting opportunities?

e. What existing guardrails and governance frameworks in the AI domain could be used, or further developed, to prevent the misuse of AI within the context of the Convention?

f. How can the OPCW promote the responsible use of AI in relation to the Convention?

38. While each subgroup focused on its assigned technical areas, topics were also discussed in plenary sessions. This approach ensured that the findings and recommendations, originating from individual subgroups, were agreed by consensus across the entire TWG. Recommendations appear throughout the text: some relate directly to a specific subgroup's findings, while others reflect cross-cutting issues arising from multiple subgroups and are presented in the most appropriate section, and therefore may not appear in ascending numerical order. The findings and recommendations of the TWG on AI will be instrumental in strengthening and augmenting the Secretariat's capability in this field.

39. During the execution of its mandate, the TWG leveraged AI as a collaborative partner to support and accelerate its work. A summary of the tools and approach used is presented in Annex 5.

FINDINGS OF THE TWG ON AI

INTRODUCTION

40. The integration of AI into almost all sectors of society is provoking a wide range of responses. Some are actively embracing its transformative potential, others remain cautious or sceptical, and many are simply striving to keep up with developments and understand how they impact their work and daily lives. What is widely agreed, however, is that the pace of AI development and its integration into existing scientific workstreams, activities, and technologies is remarkably fast.

41. While important advances in AI are occurring within the chemical sciences themselves,[14] many of the significant breakthroughs originate outside the chemical domain. For an organisation such as the OPCW—whose core expertise revolves around chemistry and its application to chemical weapons, their properties, detection, and destruction—this presents a particular challenge. Identifying which AI developments are most likely to impact the implementation of the Convention, and assessing their potential implications, requires sustained attention beyond traditional disciplinary boundaries. The Director-General has already taken important and timely steps in this regard, including co-hosting the Global Conference on AI in Morocco and establishing this TWG, to examine the potential impacts of AI on the Convention and the work of the Organisation. Given the relentless pace of AI development, however, continued monitoring and assessment will remain critical for the foreseeable future.

Recommendation 1

Given the continued rapid development of AI and its growing integration into scientific activities, and considering the time-limited mandate of this TWG, the OPCW should continue to actively monitor AI developments and their potential impacts on its work. This could include periodic assessments conducted by Secretariat staff, convening meetings of experts, or establishing specific focus groups of the SAB, or a combination of these approaches. Such monitoring would cover both general advances and industry trends, with attention to opportunities for, and risks to, the effective implementation of the Convention.

[14] Ananikov, Valentine P. "Top 20 Influential AI-Based Technologies in Chemistry." *Artificial Intelligence Chemistry* 2, no. 2 (December 2024): 100075. https://doi.org/10.1016/j.aichem.2024.100075.

42. The rapid pace of AI advancement has prompted international efforts to establish overarching governance frameworks for AI. Within the United Nations system, several initiatives have been launched, including the establishment of the Secretary-General's High-level Advisory Body on Artificial Intelligence[15] and the adoption of the United Nations Educational, Scientific and Cultural Organization (UNESCO) 'Recommendation on the Ethics of Artificial Intelligence'.[16] Adopted unanimously by all 193 UNESCO Member States in 2021, this recommendation represents the Organization's first-ever global standard on AI ethics.

43. In parallel, recent international initiatives have focused on the safety of frontier AI. Two complementary efforts stand out. The first is the series of AI Safety Summits, which began in the United Kingdom of Great Britain and Northen Ireland in 2023 with the Bletchley Declaration,[17] calling for international cooperation on AI safety. Subsequent summits in Seoul (2024) and Paris (2025) further highlighted the need for human-centric AI and led to the establishment of international networks dedicated to AI safety science.

44. The second initiative, Responsible Artificial Intelligence in the Military Domain (REAIM), is focused on the responsible development, deployment, and use of AI in defence. Its inaugural summit was hosted in the Netherlands in 2023, and it subsequently established a Global Commission on AI to support policy coherence, raise awareness, and promote responsible AI practices within the military.[18,19]

45. Additionally, national and private initiatives are addressing security aspects of AI. For example, the United Kingdom of Great Britain and Northen Ireland's AI Security Institute conducts research to improve understanding of AI-related security risks and to equip governments with the scientific insight needed to manage advanced AI safely.[20] In 2023, Singapore established the AI Verify Foundation, which leverages the collective expertise of the global open-source community to develop tools for testing and ensuring responsible AI.[21]

[15] "Final Report – Governing AI for Humanity." United Nations, accessed February 18, 2026.

[16] *Recommendation on the Ethics of Artificial Intelligence* (SHS/BIO/REC-AIETHICS/2021). United Nations Educational, Scientific and Cultural Organization, 2021.

[17] "The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023." GOV.UK, February 13, 2025.

[18] "Call to Action on Responsible Use of AI in the Military Domain." Ministerie van Buitenlandse Zaken, and Ministerie van Defensie, February 16, 2023.

[19] "Global Commission on Responsible Artificial Intelligence in the Military Domain (GC REAIM)." HCSS, accessed February 18, 2026.

[20] "The AI Security Institute (AISI)." AI Security Institute, accessed February 6, 2026.

[21] "Building Trustworthy AI." AI Verify Foundation, accessed January 23, 2026.

46. Industry is also prioritising AI security. The Frontier Model Forum brings together leading AI companies—including Amazon, Anthropic, Google, Meta, Microsoft, and OpenAI— to discuss the development of their AI systems with the aim of promoting safety and security.[22] The Forum's three core mandates are to identify best practices and support standards development, advance science, and facilitate information sharing among a diverse range of stakeholders. It also addresses a spectrum of risks, including chemical, biological, radiological, and nuclear (CBRN) threats, with a central concern being that increasingly capable general-purpose AI models may lower the barrier for chemical weapons design.

47. While the OPCW does not have a mandate to provide governance for the misuse of AI, effective oversight in the context of the Convention requires more than passive observation. The Organisation is uniquely positioned to help bridge governance gaps, for example by contributing to certification standards aimed at preventing the misuse of AI in the chemical domain. The OPCW should therefore participate in ongoing AI governance and regulation dialogue—particularly where CBRN issues are involved—and seek to align its policies with existing international standards where possible, reducing duplication of effort. While it is not expected to have a seat at every table, the OPCW should proactively communicate its interest, mandate, and approach to AI, fostering collaboration and strategic harmonisation where feasible.

Recommendation 3

The Secretariat should continue to strengthen relationships with external organisations and stakeholders whose work aligns with the OPCW's mandate. This may include AI ethics and safety frameworks, as well as relevant United Nations bodies, multilateral organisations, States Parties, and non-governmental organisations. Ongoing engagement in these international dialogues will help the OPCW remain informed about developments in AI and identify areas warranting further attention.

[22] "Frontier Model Forum: Advancing Frontier AI Safety and Security." Frontier Model Forum, October 1, 2023.

SUBGROUP 1: SYNTHESIS AND AUTOMATION

48. Subgroup 1 primarily focused on reviewing the current state of the art in AI-supported synthesis planning tools and AI-driven automated and remote chemical synthesis. In relation to these two key areas, and guided by the questions set out in paragraphs 7 and 8 of the TOR, the subgroup examined a range of considerations, including current capabilities, limitations, and potential impacts on implementation of the Convention.

AI-supported synthesis and retrosynthesis tools

49. AI-enabled tools are increasingly being integrated into chemical design, optimisation, and synthesis planning workflows across research and industry. Recent reviews describe how machine learning (ML) and other AI methods are now used for molecular design (identifying and proposing new molecules with desired properties), synthetic route planning (determining the steps needed to make a target molecule), reaction prediction (forecasting whether a proposed reaction will succeed under certain conditions), and automated synthesis (using robotics and software to carry out chemical reactions with limited human intervention), supported by large reaction datasets and high-performance computing.[23] Computer-aided synthesis planning and AI-driven retrosynthesis[24] tools can automatically learn reaction rules from experimental data and propose multi-step synthetic routes.[25] Figure 4 compares traditional and AI-assisted approaches to retrosynthesis and synthesis planning.

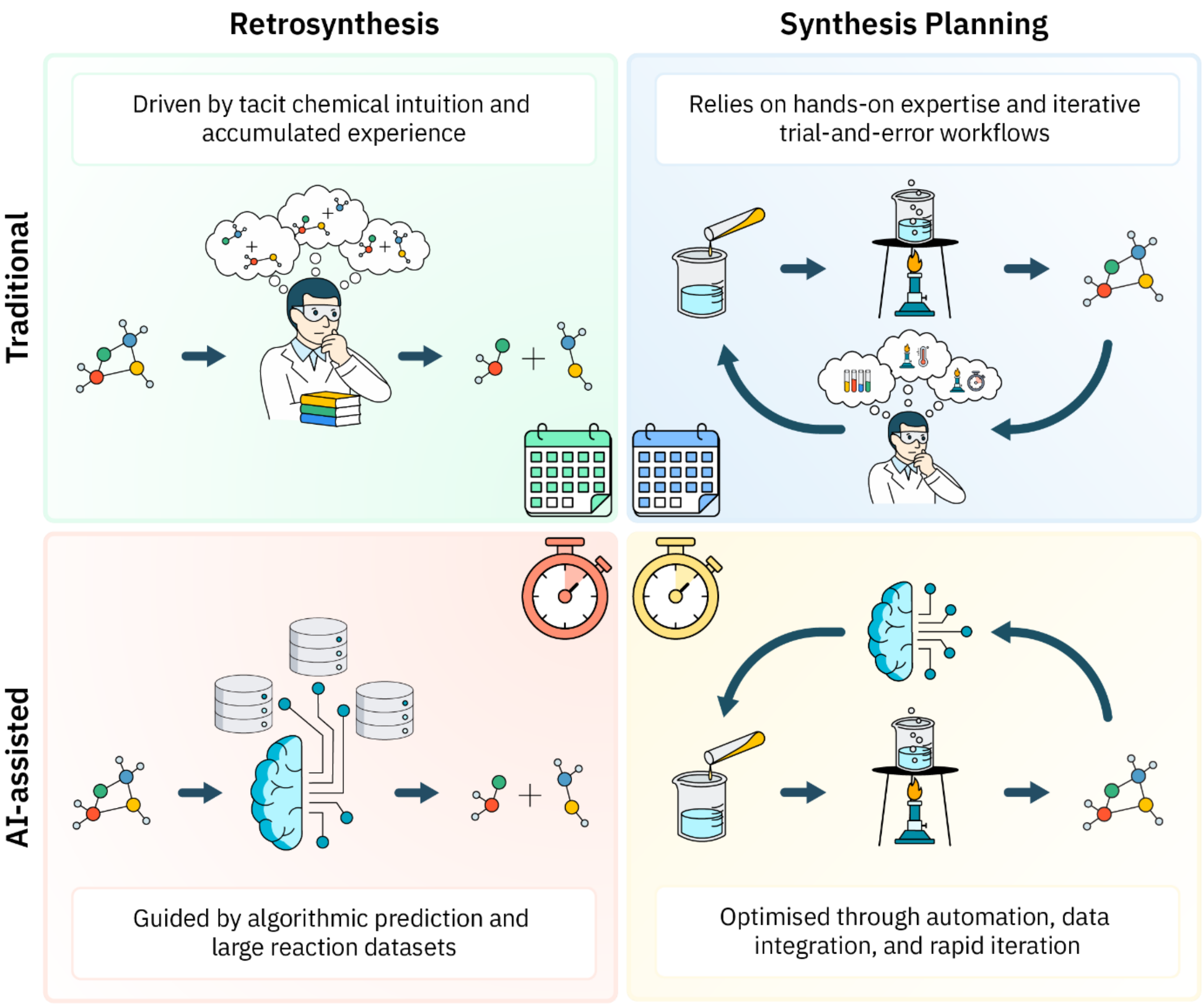
50. Historically, the feasibility of illicit synthesis of highly toxic chemicals, such as chemical warfare agents (CWAs), has been constrained by the need for extensive tacit knowledge—accumulated through experience in troubleshooting, optimisation, and scale-up—alongside barriers related to precursor access, specialised equipment, and supply chains. AI-driven retrosynthesis and synthesis planning tools can now assist with tasks such as route discovery, reagent selection, and condition optimisation,

[23] He, Chasheng, Chengwei Zhang, Tengfei Bian, Kaixuan Jiao, Weike Su, Ke-Jun Wu, and An Su. “A Review on Artificial Intelligence Enabled Design, Synthesis, and Process Optimization of Chemical Products for Industry 4.0.” *Processes* 11, no. 2 (January 19, 2023): 330. https://doi.org/10.3390/pr11020330.

[24] Retrosynthesis involves working backwards from a target molecule to identify simpler precursors and feasible reaction pathways.

[25] Jiang, Yinjie, Yemin Yu, Ming Kong, Yu Mei, Luotian Yuan, Zhengxing Huang, Kun Kuang, et al. “Artificial Intelligence for Retrosynthesis Prediction.” *Engineering* 25 (June 2023): 32–50. https://doi.org/10.1016/j.eng.2022.04.021.

drawing on large reaction databases and learned models.[26] These tools can therefore lower technical barriers to synthesis planning and reduce time required to identify viable routes.



Retrosynthesis
Synthesis Planning
Traditional
AI-assisted
Driven by tacit chemical intuition and accumulated experience
Relies on hands-on expertise and iterative trial-and-error workflows
Guided by algorithmic prediction and large reaction datasets
Optimised through automation, data integration, and rapid iteration

Figure 4: Comparison of retrosynthesis and synthesis planning

51. At the same time, AI-supported design tools are increasingly being used to propose new molecules with specified properties. Reviews of chemical engineering and industrial chemistry highlight a rapid growth in the adoption of AI-enabled tools, with increasing integration into "Industry 4.0" environments.[23]

52. AI-enabled synthesis and retrosynthesis capabilities are provided by a heterogeneous set of vendors and some are offered with limited or no user

[26] Irwin, Ross, Spyridon Dimitriadis, Jiazhen He, and Esben Jannik Bjerrum. "Chemformer: A Pre-Trained Transformer for Computational Chemistry." *Machine Learning: Science and Technology* 3, no. 1 (January 31, 2022). https://doi.org/10.1088/2632-2153/ac3ffb.

verification. These capabilities are now available through a diverse ecosystem of commercial and open-source services, including:

a. commercial platforms that offer cloud-based synthesis planning or molecular design services, sometimes via subscription or application programming interface (API) access;

b. enterprise software or on-premises solutions integrated into industrial workflows;

c. open-source tools and models that can be installed and run locally; and

d. tools embedded within broader laboratory automation or "self-driving" laboratory systems.

Automated and remote laboratories

53. Cloud laboratories (cloud labs) and self-driving laboratories (SDLs) represent two distinct classes of automated laboratory systems and are compared in Figure 5. These classes are differentiated primarily by their access models and degree of AI-driven experimental autonomy. They were considered in turn, beginning with cloud labs, which are already commercially deployed and accessible to a broad range of users.

Cloud laboratories

54. In reviewing remote laboratories—defined here as laboratory capabilities where experiments can be designed, controlled, or executed from a distance—it was highlighted that the growth of cloud labs is further decoupling digital design activities from physical chemical handling. Cloud labs provide software-mediated access to highly automated laboratory infrastructure—often encompassing a wide range of wet-laboratory and analytical processes—enabling users to submit digital instructions that are executed at dedicated facilities operated by the cloud lab provider.[27,28] In these models, experimental design, job submission, and data analysis may occur at the user's location, while all physical handling of materials and equipment takes

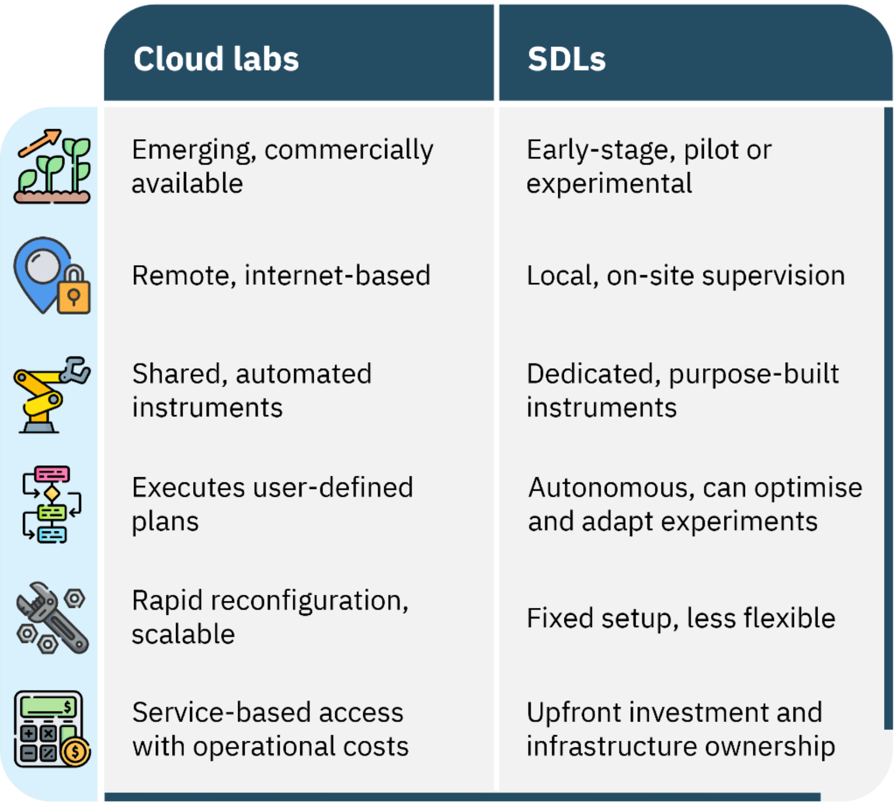
[27] Lee, Jeffrey, Bria Persaud, Barbara Del Castello, Allison Berke, and Gustavs Zilgalvis. Rep. *Documenting Cloud Labs and Examining How Remotely Operated Automated Laboratories Could Enable Bad Actors*. Santa Monica, CA: RAND Corporation, (April 24, 2025). https://doi.org/10.7249/PEA3851-1.

[28] Brockmann, Kolja, Lauriane Héau, and Giovanna Maletta. "Cloud Labs and Other New Actors in the Biotechnology Ecosystem: Export Control Challenges and Good Practices in Outreach." Stockholm International Peace Research Institute, May 2025.

place at the provider's facility. Accessible from anywhere in the world via a web interface, cloud labs operate 24 hours a day, seven days a week, supporting continuous experimentation.

55. Cloud labs integrate robotics, automated sample handling, and instrument control to execute protocols with minimal human intervention. Cloud lab services can be accessed via subscription, institutional agreements, or pay-per-use models, and are commonly used in sectors such as biotechnology, pharmaceuticals, materials science, and chemical research where high-throughput experimentation, reproducibility, and access to specialised equipment are priorities. While publicly available information on the current number and types of clouds labs remains limited, a recent RAND expert insights paper has identified 15 cloud lab organisations and their capabilities.[27]

56. Cloud labs can enable rapid iteration of experiments and expand access to chemical experimentation by providing advanced laboratory capabilities to users who lack local facilities. By integrating AI-driven design tools with automated execution, these services can support closed-loop experimentation, where results are fed back into models to refine subsequent experimental plans. This convergence can significantly accelerate discovery and optimisation cycles in chemistry and materials research, potentially reducing time and cost barriers for legitimate scientific work.



Cloud labs	SDLs
Emerging, commercially available	Early-stage, pilot or experimental
Remote, internet-based	Local, on-site supervision
Shared, automated instruments	Dedicated, purpose-built instruments
Executes user-defined plans	Autonomous, can optimise and adapt experiments
Rapid reconfiguration, scalable	Fixed setup, less flexible
Service-based access with operational costs	Upfront investment and infrastructure ownership

Figure 5: Comparison of cloud labs and SDLs

Self-driving laboratories

57. Whereas cloud labs primarily transform who can access laboratory capabilities and how experiments are executed remotely, SDLs represent a further step in automation by transforming how experimental decisions themselves are made. Recent advances in laboratory automation and AI have led to the emergence of SDLs that couple robotic experiment execution with data-driven decision-making. These systems are increasingly being deployed in chemistry and materials science and are beginning to influence how experimental work is organised, executed, and accessed. Comprehensive reviews describe a trajectory from bespoke, highly customised research systems towards more standardised and modular platforms, with close integration into broader digital research infrastructures.[29,30]

58. Comprehensive technical assessments of SDLs outline how the combination of automated hardware, integrated sensing, and AI-driven experiment planning can substantially accelerate experimental cycles, increase throughput, and improve reproducibility in chemistry and materials discovery. These analyses emphasise that SDL architectures can often be decomposed into generic components—such as orchestration software, modular synthesis or reaction units, and sensor/characterisation modules—facilitating reuse, scaling, and adaptation to new domains.[29]

59. A recent perspective on science acceleration and accessibility highlights that SDLs are not only performance-enhancing but also potentially transformative for access models. It describes both centralised SDL facilities and distributed SDL networks that can be accessed digitally, allowing users to design and run experiments remotely, with the system autonomously selecting and executing conditions in a closed loop.[30] These configurations may broaden participation in advanced experimentation and lower operational barriers for users who do not operate traditional laboratories.

60. Other community-level reviews of autonomous experimentation systems similarly emphasise that these platforms can shorten discovery timelines and support more

[29] Tom, Gary, Stefan P. Schmid, Sterling G. Baird, Yang Cao, Kourosh Darvish, Han Hao, Stanley Lo, et al. “Self-Driving Laboratories for Chemistry and Materials Science.” *Chemical Reviews* 124, no. 16 (August 13, 2024): 9633–9732. https://doi.org/10.1021/acs.chemrev.4c00055.

[30] Canty, Richard B., Jeffrey A. Bennett, Keith A. Brown, Tonio Buonassisi, Sergei V. Kalinin, John R. Kitchin, Benji Maruyama, et al. “Science Acceleration and Accessibility with Self-Driving Labs.” *Nature Communications* 16, no. 1 (April 24, 2025). https://doi.org/10.1038/s41467-025-59231-1.

systematic, data-rich experimentation, while also highlighting challenges related to data infrastructure, standardisation, and workforce development.[31,32]

Evolving access models, automation, and expertise

61. Across AI-supported synthesis tools, cloud labs, and SDLs, the literature points to increasing automation, modularity, and professionalisation.[27,28,29,30,31,33] Reviews describe a growing ecosystem of academic laboratories, industrial providers, and public-private initiatives contributing to more general-purpose, service-oriented platforms rather than one-off research implementations.[29,31]

62. Automated laboratories are also becoming more accessible through remote and digital models of use. They can be configured as shared resources that offer remote access to users with diverse skillsets, potentially including those without extensive hands-on experimental expertise.[30] From a broader policy and technology perspective, a recent review of autonomous SDLs notes that these systems are subject to multiple drivers and constraints, including cost, intellectual-property considerations, and safety and security concerns, which together make their long-term trajectory difficult to predict.[33]

63. Cloud labs and SDLs may also offer potential benefits for transparency and reproducibility, for example through standardised protocols and digital audit trails, but these possible advantages depend on how systems are designed and governed.[31,32]

64. At the same time, analyses of AI-enabled design and automated experimentation highlight that parts of the experimental cycle—such as route planning, condition selection, and iterative optimisation—are increasingly being shifted from human chemists to digital systems.[23] Comparable assessments in chemical engineering and synthetic biology describe how automation and AI may "deskill" complex tasks and

[31] Stach, Eric, Brian DeCost, A. Gilad Kusne, Jason Hattrick-Simpers, Keith A. Brown, Kristofer G. Reyes, Joshua Schrier, et al. "Autonomous Experimentation Systems for Materials Development: A Community Perspective." *Matter* 4, no. 9 (September 1, 2021): 2702–26. https://doi.org/10.1016/j.matt.2021.06.036.

[32] Cooper, Andrew I., Patrick Courtney, Kourosh Darvish, Moritz Eckhoff, Hatem Fakhruldeen, Andrea Gabrielli, Animesh Garg, et al. "Accelerating Discovery in Natural Science Laboratories with AI and Robotics: Perspectives and Challenges." *Science Robotics* 10, no. 106 (September 24, 2025). https://doi.org/10.1126/scirobotics.adv7932.

[33] Tobias, Alexander V., and Adam Wahab. "Autonomous 'Self-Driving' Laboratories: A Review of Technology and Policy Implications." *Royal Society Open Science* 12, no. 7 (July 16, 2025). https://doi.org/10.1098/rsos.250646.

widen access to capabilities that were previously confined to highly specialised environments.[34]

65. Emerging developments in more autonomous or "agentic" AI systems further suggest a transition from discrete decision-support tools towards integrated workflows. These systems can now autonomously coordinate multiple stages of design, evaluation, and optimisation. Importantly, agentic AI can persistently pursue broad objectives over extended periods, exploring multiple strategies and pathways in parallel to achieve goals, effectively "figuring out" solutions with minimal hands-on guidance. This hands-off, persistent operation can save significant time, accelerate experimentation cycles, and expand the practical reach of researchers.

66. These trends suggest that while AI-supported synthesis and automated laboratories offer substantial benefits for efficiency, reproducibility, and scientific access, they may alter how dual-use risks manifest and how they are governed.[34] Reduced reliance on tacit expertise, the ability to execute experiments remotely and autonomously, and digitally mediated access models may challenge traditional approaches to Convention compliance.

Misuse risk and governance implications

67. AI-supported synthesis tools and automated facilities bring significant benefits to research and technological development, including accelerating discovery, reducing time and cost barriers, and supporting access to specialised equipment. While these developments support legitimate innovation, they may also lower technical barriers relevant to misuse.

68. For example, some synthesis planning platforms operate as "black-box" services, where users can submit structures or objectives without insight into underlying models or datasets. In cases where access is granted without robust user verification or clear controls on allowed use, this may create potential avenues for misuse.

69. In a study that has been widely cited, a commercial drug-discovery model was re-parameterised to generate tens of thousands of molecules predicted to have very

[34] Groff-Vindman, Cindy S., Benjamin D. Trump, Christopher L. Cummings, Madison Smith, Alexander J. Titus, Ken Oye, Valentina Prado, Eyup Turmus, and Igor Linkov. "The Convergence of AI and Synthetic Biology: The Looming Deluge." *npj Biomedical Innovations* 2, no. 1 (July 1, 2025). https://doi.org/10.1038/s44385-025-00021-1.

high toxicity, including structures related to known CWAs.[35] These findings illustrate a dual-use concern for such AI models and that, in some configurations, they can provide capabilities that reduce the expertise traditionally required to explore hazardous chemical space and to identify potential synthetic targets of concern.

70. Proposals in the literature for governance of dual-use AI systems in the chemical and biological domains were examined. In the context of biological design tools, one recent analysis identifies dual-use capabilities of concern and proposes the use of targeted evaluations ("red-flag" tests) to detect models that can significantly assist with high-consequence misuse.[36] The authors recommend that model providers implement structured assessments and, where appropriate, technical safeguards to limit harmful functionality.

71. Although this analysis focuses primarily on biological systems and laboratory services, analogous approaches may be relevant for vendors of AI-enabled synthesis and retrosynthesis tools. Possible governance measures identified include:

    a. verification of user identity and, where appropriate, stated affiliation and purpose before granting access to advanced capabilities;

    b. technical filters or screening systems to detect and block attempts to design prohibited or especially hazardous chemicals; and

    c. red-flag evaluations of models prior to deployment to identify high-consequence dual-use capabilities.[28,36]

72. Engagement with vendors could support the diffusion of such practices, while also providing a channel for raising awareness of the Convention and possible misuse scenarios.

73. Considering that vendors of AI-supported synthesis tools differ markedly in their capabilities, access models, and internal safeguards, there may be value in the Secretariat maintaining an up-to-date awareness of the vendor landscape, which could:

    a. provide situational awareness of the types of capabilities that are commercially or openly available, including access models (for example, public web interface, API, or institutional licensing);

[35] Urbina, Fabio, Filippa Lentzos, Cédric Invernizzi, and Sean Ekins. "Dual Use of Artificial-Intelligence-Powered Drug Discovery." *Nature Machine Intelligence* 4, no. 3 (March 7, 2022): 189–91. https://doi.org/10.1038/s42256-022-00465-9.

[36] Pannu, Jaspreet, Doni Bloomfield, Robert MacKnight, Moritz S. Hanke, Alex Zhu, Gabe Gomes, Anita Cicero, and Thomas V. Inglesby. "Dual-Use Capabilities of Concern of Biological AI Models." *PLOS Computational Biology* 21, no. 5 (May 8, 2025). https://doi.org/10.1371/journal.pcbi.1012975.

b. help identify which vendors already employ user verification, content filters, or other safeguards, and where gaps may exist;

c. support targeted outreach and dialogue with providers whose tools may be most relevant to Convention-related risks; and

d. inform future technical assessments or exercises involving AI-enabled chemical design and remote laboratories.

Recommendation 4

The Secretariat should maintain an up-to-date list of vendors offering AI-enabled synthesis and retrosynthesis platforms and related computational chemistry solutions, with special attention given to open-source and proprietary platforms that are accessible to the public with no verification process. The OPCW should attempt to raise awareness of Convention-related risks with these companies and promote active governance approaches.

74. The TWG considers that such a list would not constitute endorsement of specific vendors but rather provide a basis for ongoing evaluation of technological developments and governance practices.

75. When AI-enabled synthesis or retrosynthesis tools are combined with remote execution services, digital workflows can in principle support the design and synthesis of complex molecules without the user directly handling precursors or operating equipment. In such configurations, traditional monitoring approaches based on procurement of chemicals and equipment may provide only a partial picture.

76. Reviews of automated laboratories therefore highlight the growing importance of governance mechanisms embedded within digital environments, including controls on platform access, authentication, logging, and job submission. These features may become increasingly relevant complements to established monitoring and verification approaches as remote and automated laboratory models mature.

77. The RAND study identifying cloud lab organisations notes that the convergence of automation, remote execution, and AI-enabled tools can create new opportunities for research and innovation, while also introducing specific risks if appropriate safeguards are not in place, including potential misuse for chemical or biological weapons development.[27]

78. A complementary non-proliferation and disarmament paper by the Stockholm International Peace Research Institute (SIPRI) identifies cloud labs—alongside other

emerging actors in the biotechnology ecosystem—as posing various chemical and biological weapons proliferation risks and export control challenges, and considers how best to apply governance measures.[28] The paper highlights that cloud labs may involve transfers of both tangible materials and intangible technology, with relevant activities mediated through digital interfaces rather than on-site human operation.

79. A recent policy-focused review of autonomous laboratories underscores that the societal implications of SDLs extend beyond the laboratory, touching on regulatory frameworks, intellectual property, workforce impacts, and security policy.[33] Safety and security aspects of SDLs and cloud labs are explicitly discussed, with the review noting that while these concerns appear manageable, they require proactive approaches, clear human accountability, and robust cybersecurity measures.

80. In light of these considerations, it was judged that systematic monitoring of technological trends, structured engagement with leading academic and industrial developers, and targeted technical exercises would assist the Secretariat in evaluating both opportunities and emerging risks associated with automated laboratories.

Recommendation 2

While automated laboratories are currently most widely deployed in advanced research environments, the field is rapidly professionalising. Commercial platforms, modular synthesis hardware, and AI-enabled orchestration tools are lowering operational barriers and enabling increasingly remote and automated workflows. To remain proactive, the TWG recommends that the OPCW formally monitor these developments and build internal capability to evaluate both opportunities and emerging risks. This should include systematic engagement with leading academic and industrial developers, periodic technical assessments, and targeted exercises to explore real-world use cases. Particular attention should be given to understanding how reduced reliance on human expertise, remote execution, and digital access models may evolve, as well as to identifying governance mechanisms that support responsible innovation while safeguarding against misuse.

81. The SAB's TWG on Education and Outreach previously emphasised that education, outreach, and sustained engagement with the scientific community and industry are essential to preventing the re-emergence of chemical weapons and supporting the

long-term implementation of the Convention.[37] Its work highlighted the value of partnerships with professional bodies, universities, and industry in promoting a culture of responsible chemistry and embedding Convention norms in everyday scientific practice.

82. Implementing one of the recommendations of this TWG, the OPCW Advisory Board on Education and Outreach was established to provide specialised advice on effective, sustainable education and outreach strategies relevant to the OPCW's mandate.[38] Members of this Board played a key role in developing The Hague Ethical Guidelines, which promote the responsible practice of chemistry.[39] Related initiatives, such as the compilation of chemistry codes of ethics and conduct, and the development of the Global Chemists' Code of Ethics,[40] have demonstrated how collaboration between the OPCW, professional societies, and other stakeholders can translate ethical principles into widely recognised guidance for practitioners.

83. Building on this foundation, subsequent analyses have underscored the role of education, outreach, and codes of conduct in reinforcing CBRN security objectives. A joint IUPAC/OPCW international workshop in 2005 recognised that long-term effectiveness depends on active engagement with educators, professional associations, and journal editors to integrate Convention-related topics into curricula, guidance documents, and professional norms.[41] More recent work on responsible science and CBRN security has highlighted that codes of conduct are most effective when supported by continuous dialogue and joint activities between scientists, policymakers, and security communities.[42]

[37] Final Report of the Temporary Working Group on Education and Outreach in Science and Technology Relevant to the Chemical Weapons Convention (SAB/REP/2/14, dated November 2014).

[38] "Advisory Board on Education and Outreach: Supporting the OPCW's Engagement with External Partners." Organisation for the Prohibition of Chemical Weapons, accessed November 12, 2025.

[39] "The Hague Ethical Guidelines." Organisation for the Prohibition of Chemical Weapons, accessed February 18, 2026.

[40] *Global Chemists' Code of Ethics*. American Chemical Society, accessed November 13, 2025.

[41] Pearson, Graham S., and Peter Mahaffy. "Education, Outreach, and Codes of Conduct to Further the Norms and Obligations of the Chemical Weapons Convention (IUPAC Technical Report)." *Pure and Applied Chemistry* 78, no. 11 (January 1, 2006): 2169–92. https://doi.org/10.1351/pac200678112169.

[42] Novossiolova, Tatyana, and Maurizio Martellini. "Promoting Responsible Science and CBRN Security through Codes of Conduct and Education." *Biosafety and Health* 1, no. 2 (September 2019): 59–64. https://doi.org/10.1016/j.bsheal.2019.08.001.

84. Similarly, in the context of the Biological and Toxin Weapons Convention, it has been highlighted that sustained engagement with life-science stakeholders, including through innovative communication tools and partnerships with professional societies and academic institutions, is necessary to build awareness of dual-use risks and treaty obligations.[43] These findings are relevant to chemistry and AI-enabled research, where comparable dual-use concerns arise and where communities of practice are often organised around professional societies, conferences, and journals.

85. Emerging literature on AI and dual-use research notes that AI research communities are increasingly confronted with questions about how to manage misuse risks, including in chemical and biological domains.[44] This work points to the importance of dialogue between AI developers, ethicists, and security experts, and suggests that professional societies and publishers can play a role in shaping norms and expectations. At a workshop in 2025, the NAS brought together journal editors, professional societies, and other stakeholders to consider how best to navigate the benefits and biosecurity risks of publishing *in silico* modelling and generative AI work involving biological systems, including the development of policies and safeguards at the publication stage.[45]

[43] Novossiolova, Tatyana, Simon Whitby, Malcolm Dando, and Lijun Shang. “Strengthening Biological Security after Covid-19: Using Cartoons for Engaging Life Science Stakeholders with the Biological and Toxin Weapons Convention (BTWC).” *Journal of Biosafety and Biosecurity* 4, no. 1 (June 2022): 68–74. https://doi.org/10.1016/j.jobb.2022.03.001.

[44] Hurst, Daniel, and Christopher Bobier. “Dual Use Research and Artificial Intelligence.” *AI & SOCIETY* 40, no. 7 (March 3, 2025): 5547–48. https://doi.org/10.1007/s00146-025-02263-4.

[45] “Navigating the Benefits and Risks of Publishing Studies of in Silico Modeling and Computational Approaches of Biological Agents and Organisms – a Workshop.” National Academies, accessed February 6, 2026.

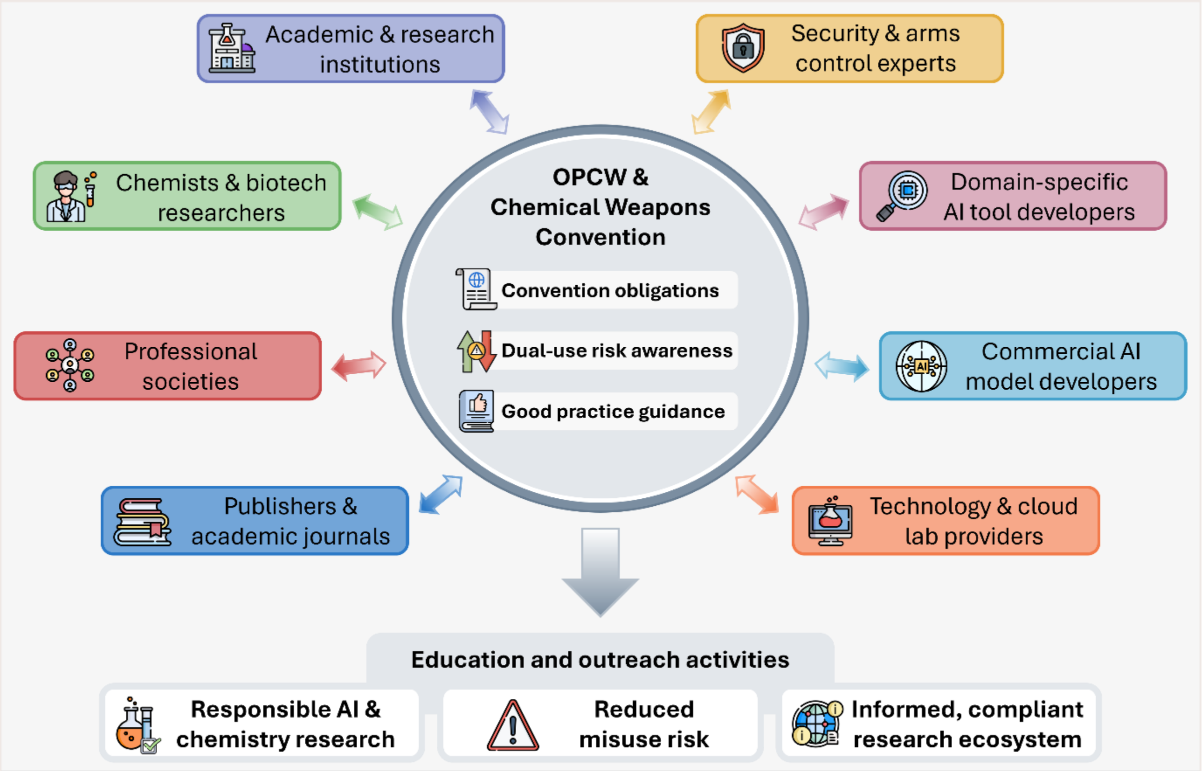

Academic & research institutions
Security & arms control experts
Chemists & biotech researchers
OPCW & Chemical Weapons Convention
Domain-specific AI tool developers
Convention obligations
Dual-use risk awareness
Professional societies
Commercial AI model developers
Good practice guidance
Publishers & academic journals
Technology & cloud lab providers
Education and outreach activities
Responsible AI & chemistry research
Reduced misuse risk
Informed, compliant research ecosystem

Figure 6: Potential strategic partnerships between key stakeholders and the OPCW

86. Taken together, these experiences indicate that strategic partnerships with AI developers, chemists, professional societies, and publishers—shown in Figure 6—can provide practical channels to raise awareness of the Convention and AI-related risks, and co-develop good practice for managing dual-use concerns. The TWG considers that such partnerships would complement existing OPCW education and outreach activities and could help ensure that evolving AI and chemistry communities remain informed about the Convention and the work of the OPCW. In this context, the TWG notes that outreach and engagement with technology providers—including cloud labs—can encourage compliance measures such as user due diligence, awareness of relevant control lists, and internal processes to identify suspicious experimental requests.[28] As the biotechnology and automated laboratory ecosystems expand and diversify, traditional outreach approaches no longer reach all relevant stakeholders, highlighting the need for sustained, targeted engagement.

Recommendation 5

The OPCW should build strategic partnerships with relevant AI and chemistry communities, as well as with leading publishers and academic journals that highlight the latest research in these fields, to facilitate dialogue between AI developers, chemists, and arms control experts. These partnerships would afford an opportunity to provide AI developers with a greater awareness of the Convention, the potential risks of AI in this context, and the work of the OPCW.

Misuse indicators and detection

87. As AI tools become more deeply embedded in chemical design, optimisation, and execution workflows, relevant indicators of potential misuse may increasingly manifest through digital interactions with computational platforms, rather than through traditional physical activities alone.

88. Peer-reviewed analyses indicate that AI systems used for molecular design, synthesis planning, and optimisation can automate elements of route exploration, screening, and prioritisation that previously relied heavily on tacit expertise. As noted earlier, this shift may increase the accessibility of sophisticated chemical capabilities to users with limited technical backgrounds, while simultaneously changing where observable signals of misuse may arise.[34]

89. A comprehensive meta-review of AI risks highlights misuse by malicious actors and accidental harmful outcomes as core risk categories and notes that behavioural indicators—such as anomalous digital usage patterns—may be useful for early detection of misuse.[46]

90. Draft guidance for managing dual-use AI models emphasises early identification of high-risk user behaviour, including access anomalies, irregular computational workloads, and use of remote or automated services for sensitive tasks.[47] Such indicators may be particularly relevant where design and execution are decoupled geographically through cloud-based laboratory systems.

[46] Slattery, Peter, Alexander K. Saeri, Emily A. C. Grundy, Jess Graham, Michael Noetel, Risto Uuk, James Dao, Soroush Pour, Stephen Casper, and Neil Thompson. "The AI Risk Repository: A Comprehensive Meta-Review, Database, and Taxonomy of Risks from Artificial Intelligence." arXiv, August 14, 2024.

[47] U.S. AI Safety Institute at NIST. "NIST AI 800-1 2pd: Managing Misuse Risk for Dual-Use Foundation Models." Second Public Draft: U.S. Department of Commerce, National Institute of Standards and Technology, January 2025.

91. Reviewing these findings, several categories of observable indicators relevant to Convention-related monitoring have been identified, including:

a. queries or design requests involving scheduled chemicals or highly toxic structures without legitimate purpose;[34]

b. repeated or escalating high-risk interaction patterns with chemical design or retrosynthesis platforms;[46]

c. use of anonymised or proxy access mechanisms to conduct sensitive computational tasks;[47] and

d. rapid iteration of novel precursors or intermediates lacking clear commercial or research justification.[34]

Recommendation 6

The OPCW should develop a list of indicators to identify AI misuse, which would enable authorities in States Parties to recognise such instances. Misuse of AI may be intentional, by a nefarious actor, or unintentional, arising from inadvertent mistakes, a lack of awareness, or insufficient expertise. Potential indicators may include:

a. acquisition or synthesis of scheduled or toxic chemicals, or novel derivatives/analogues, without legitimate context;

b. unusual query patterns on synthesis platforms;

c. use of anonymised application programming interfaces for sensitive queries; and/or

d. rapid prototyping of novel precursors or intermediates.

The Secretariat may consider holding a series of workshops with experts from States Parties to develop this list.

92. The TWG considers that such a list should be treated as a living resource, informed by evolving capabilities and by consultation with States Parties and technical experts.

Opportunities for the OPCW

93. The chemical space surrounding known CWAs contains thousands of potential analogues that may possess similar lethality but fall outside current control parameters. Recognising that AI models may be used to systematically explore

chemical space,[48,49] it was proposed that these same tools could also be leveraged to identify potential chemicals of concern. Used in this way, AI-enabled analysis could strengthen the OPCW's preparedness by supporting earlier identification and prioritisation of emerging or previously unknown chemical threats.

94. This preparedness could be further enhanced by using AI-supported retrosynthesis tools to identify novel synthetic pathways for CWAs that use unscheduled precursors. Employing advanced models to predict routes to known or potential CWAs could highlight "blind spots" in the verification regime where nefarious actors could circumvent the Schedules of the Annex on Chemicals to the Convention.

[48] Bilodeau, Camille, Wengong Jin, Tommi Jaakkola, Regina Barzilay, and Klavs F. Jensen. "Generative Models for Molecular Discovery: Recent Advances and Challenges." *WIREs Computational Molecular Science* 12, no. 5 (March 5, 2022). https://doi.org/10.1002/wcms.1608.

[49] Gao, Wenhao, Shitong Luo, and Connor W. Coley. "Generative AI for Navigating Synthesizable Chemical Space." *Proceedings of the National Academy of Sciences* 122, no. 41 (October 6, 2025). https://doi.org/10.1073/pnas.2415665122.

SUBGROUP 2: DATA CURATION, PROTECTION, AND RELIABILITY

Adoption and operationalisation of AI systems at the OPCW

Introduction

95. Many international organisations are exploring innovative AI solutions to enhance operational efficiency and human productivity, streamline processes, and support decision-making. In sensitive or critical domains, gains in operational efficiency directly contribute to security, safety, and effective mandate fulfilment. Some organisations, guided by the theme of "shaping responsible solutions for internal security",[50] are also developing capabilities that strengthen internal safeguards. Across these applications, organisations are aligning with emerging global norms, including privacy, transparency, and accountability.[50] As a verification and implementation body operating in the international security and disarmament domain, the OPCW must demonstrate that its adoption and operationalisation of AI adheres to these norms and is implemented responsibly.

96. Although AI encompasses a broad range of technologies—from computer vision to predictive analytics and workflow automation—systems capable of processing and understanding natural language are particularly relevant to several areas of the OPCW's operational work. Among these, large language models (LLMs) excel at administrative and analytical tasks such as document summarisation, translation, and information retrieval, making them directly applicable to the OPCW's workflows. In this context, Subgroup 2 considered how AI could be best leveraged by the Organisation.

97. However, the effective and responsible deployment of any such system depends significantly on the foundation upon which it is built: data. Data is an important foundation of every AI system, and the quality of an AI model's outputs is directly linked to the quality of the data it learns from and relies on. Careful curation helps ensure datasets are accurate, representative, and free from harmful biases; robust protection safeguards sensitive information and maintains system integrity; and reliability enables models to perform consistently, adapt safely, and resist manipulation. Subgroup 2 explored these issues and identified measures needed to ensure that any AI systems deployed by the OPCW function as intended, remain trustworthy, and can be applied safely and responsibly.

[50] "EU Innovation Hub Annual Event report 2024." Europol, November 28, 2024.

Proposed AI application 1: declarations processing

98. Since the Convention entered into force in 1997, States Parties have submitted regular declarations on facilities and activities relating to a range of chemicals, providing the OPCW with a significant volume of valuable data. However, in its current form, this information cannot be readily leveraged due to several challenges.

99. To begin with, declarations are received in the six official languages of the OPCW and are not standardised: nearly a third of the roughly 90 submitting States Parties provide non-standard formats, including printed, handwritten, or diverse electronic file types. As a result, all such data must be entered manually. Compounding this, the length of declarations varies dramatically—from half a page to more than 2,000 pages—making the process inefficient, time-consuming, and prone to transcription errors, while utilising considerable staff resources. The OPCW's physical archives also contain extensive hard copy verification materials yet to be digitised, and its digital archives include older, low-quality scans and files with insufficient metadata.

100. These limitations mean that the Secretariat lacks structured, machine-readable data needed to identify inconsistencies, anomalies, and trends that may warrant further attention—capabilities essential for any future use of AI tools.

101. To identify how the Secretariat could best leverage these data, efforts led by other international organisations facing similar challenges with declaration and report processing were examined. Notably, within the International Atomic Energy Agency (IAEA), the Department of Safeguards has begun developing AI-assisted systems, including LLM-based tools, to support the processing of reports in multiple formats, such as the digitisation of hard copy documents and extraction of information from digital submissions. The IAEA's experience offers valuable lessons for the OPCW, as both organisations face analogous challenges: diverse document formats, multiple languages, the need for high accuracy, and the critical importance of maintaining Member State confidence in the integrity of the verification process.

102. The IAEA Department of Safeguards uses an air-gapped information technology (IT) system to ensure data security and prevent information from being transmitted to external networks. In its use of AI systems, the IAEA maintains human-in-the-loop for all decision-making tasks but works to increase efficiency in routine tasks, such as through greater automation. This approach balances automation efficiency with quality assurance, ensuring that decision-making tasks receive appropriate human attention. Document content is preserved exactly as reported, rather than corrected for typographical errors, inconsistencies, or ambiguities during AI-assisted processing. This "as-declared" principle safeguards the integrity of State submissions and, supported by a confidence score, allows any discrepancies to be properly identified and investigated.

103. Considering the similarities in requirements and challenges faced by the IAEA and the OPCW, the TWG agrees that implementing a comparable AI-assisted declaration processing system at the OPCW could yield substantial benefits. Drawing on the IAEA's experience and lessons learned, three core capabilities that would be essential for such a system have been identified: digitisation of declarations, data extraction and structuring, and secure storage and accessibility. Together, these form a logical workflow (see Figure 7) from initial document receipt through final storage and retrieval, with human oversight integrated at critical points throughout.

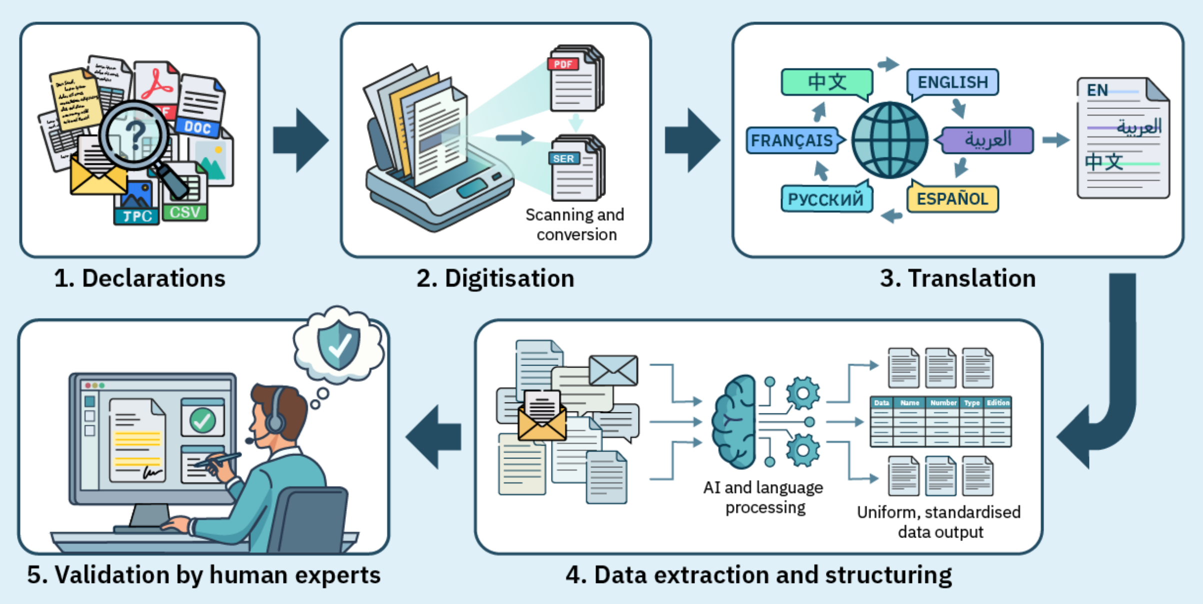


Figure 7: Workflow for an AI-assisted declaration processing system

104. In the digitisation process, the system must be capable of converting both historical and current declarations from various hard copy and electronic formats into machine-readable text, creating a foundation for all downstream processing. The original declaration should be preserved faithfully, following the "as-declared" principle mentioned above. This capability must support the six official languages of the OPCW, with translations validated by human reviewers who have professional proficiency in both the source language and the target language (English), to ensure they accurately reflect the original "as-declared" content. It was also noted that translating technical chemical terminology is especially challenging, since the same compound may be described differently across languages and naming conventions.

105. Subsequently, relevant data fields must be extracted from digital declarations—both newly digitised and those submitted in digital form—and be structured into formats suitable for analysis, including comparison across a State Party's submission history, and for reporting. This transforms declarations from narrative documents into queryable databases, enabling patterns, trends, and anomalies to be efficiently identified.

106. These databases should have semantic search capabilities to ensure efficient data access and retrieval. This differs from simple keyword search by understanding the meaning and context of queries, enabling users to find relevant information even when exact terminology varies. For example, a semantic search might retrieve information about “nerve agents” in response to a query about “organophosphorus chemical weapons”, recognising the conceptual relationship between these terms. This capability addresses current limitations in analysing declaration data and in preparing reports and statistical summaries. With semantic search capabilities, relevant information from a State Party’s declaration history could be retrieved, regardless of how that State Party chose to describe particular elements.

107. The development of such a system will require significant coordination between the Verification Division, the Information Services Branch, the Office of Confidentiality and Security, and the Office of Strategy and Policy, with careful attention to existing workflows, technical infrastructure, and staff capabilities. Furthermore, it was noted that similar systems in other organisations have required substantial initial investment in preparing training data, developing validation protocols, and building staff capacity to oversee AI-assisted processes.

108. The IAEA’s experience indicates that quality assurance protocols—such as benchmarking against known reference datasets and establishing error-rate thresholds that trigger systematic reviews—should be established from the outset. The TWG therefore proposes starting with a pilot that processes a limited set of declarations under close human oversight, before gradually expanding the system as confidence in its performance grows.

109. As the OPCW modernises its IT infrastructure, it is important to ensure that new systems are designed with AI compatibility and integration in mind. This applies not only to AI-assisted declaration processing but more broadly across organisational workflows and digital capabilities. Embedding AI-readiness into infrastructure design will facilitate future enhancements and help avoid the creation of technical barriers to adoption. Accordingly, ongoing software procurement and system development should systematically consider interoperability with AI tools—whether commercially sourced or custom-built—as part of evaluation and selection criteria.

Recommendation 7

The Secretariat should design, develop (or otherwise acquire and adapt), and implement a human-in-the-loop AI system to support the processing of declarations. This system should include the following core capabilities:

a. digitisation of declarations (historical and current): ability to convert all submissions into machine-readable format, to translate declarations (from multiple languages) following text conversion, and to preserve original submission fidelity;

b. data extraction and structuring: ability to extract relevant data fields from digitised declarations, to structure data in a format suitable for downstream analysis and reporting, and to enable an expert review process for all records that allows editing and approval for completion; and

c. secure storage and accessibility: ability to store digitised and structured data in a secure, queryable database (semantic search/retrieval enabled) and ensure traceability and auditability of all transformations and validations.

Ongoing and future software procurement, as well as information technology infrastructure modernisation, should consider compatibility with AI systems as part of the evaluation criteria.

110. Such an AI-assisted declaration processing system would enable the OPCW to fully leverage the valuable data it holds. It would automate time-intensive manual tasks, resulting in faster declaration processing and allowing more time for in-depth analysis of trends and anomalies. For example, it could help the Organisation more readily identify transfer discrepancies—situations in which declared imports and exports of scheduled chemicals between trading partners do not match.

111. The system would also enable automated data quality checks, reducing transcription errors and improving the reliability of pattern detection. Improved access to information could support faster response times during missions and more informed, data-driven decision-making. Additionally, the system would provide enhanced and more flexible reporting capabilities, supporting the generation of statistical reports for the Secretariat or States Parties. For example, these reports could include information on aggregate quantities of Schedule 2 chemicals traded in a given year, while respecting confidentiality requirements that prevent publication of certain data types, including production volumes per chemical for individual States Parties. By streamlining administrative tasks, an AI-assisted declaration processing system would allow staff to devote more time to higher-priority technical work and decision-making tasks.

Proposed AI application 2: chatbot

112. While examining the use of AI by the IAEA, a second use case applicable for OPCW purposes was identified. To improve efficiency and accessibility while alleviating staff workload, the Department of Safeguards at the IAEA has developed and implemented an in-house chatbot. This advanced tool is LLM-based and combines core language capabilities such as translation, transcription, and summarisation, in addition to data extraction, and multimodal processing. Analogous to its document processing system, the IAEA chatbot is hosted on-premises with no internet connectivity to ensure information security.

113. Envisaging the possible development and use of a similar general-purpose LLM-based chatbot at the OPCW, it was highlighted that such a system could assist in a range of general administrative tasks, including document translation and summarisation, as well as drafting reports and emails. Furthermore, the chatbot could be used to easily and rapidly access mission-critical information—for example, on equipment or chemical processes—by inspectors.

Recommendation 13

The Secretariat should design, develop (or otherwise acquire and adapt), and implement a custom, secure chatbot or agent for general-use cases. The system should operate within an air-gapped, secure environment. It should be capable of both assisting with general administrative tasks—such as document translation and summarisation, drafting reports and emails, and question and answer capabilities from input documents—as well as with more specific, programmatic uses, such as:

a. providing inspectors with quick access to technical information, which may include device operation, chemical process knowledge, and relevant information on chemical production and destruction facilities; and

b. assisting in the potential procurement of equipment and technology within the OPCW Technology and Training Hub framework.

Ongoing and future software procurement, as well as information technology infrastructure modernisation, should consider compatibility with AI systems as part of the evaluation criteria. It is also essential that training on the use of the chatbot and AI best practices is provided to OPCW staff.

Other applications of AI

114. The TWG considers that the adoption of AI at the OPCW has the potential to enhance efficiency and support informed decision-making. In the context of verification, AI

technologies could be applied not only to declarations processing, but also more broadly to strengthen capabilities and enhance personnel safety. This could include the integration of AI into sensors on uncrewed platforms, AI-driven generation of risk assessments for inspection planning, and analysis of open-source data through data mining—for example using satellite imagery to assess terrain and site accessibility. Further potential applications of AI at the OPCW are discussed elsewhere in this report.

Recommendation 8

The Secretariat should review OPCW verification practices to identify specific areas that could be enhanced by AI technologies. Possible applications include pattern recognition tasks—such as the detection of inconsistencies or anomalies in declarations—alongside remote sensing, risk assessment generation, and the analysis of open-source data through data mining.

AI governance for responsible deployment

Guiding principles

115. Given the sensitive nature of the information handled by the OPCW, any AI system it deploys—including the proposed declaration processing system and LLM-based chatbot—would be classified as "high-risk" under major regulatory frameworks, such as the EU AI Act.[51] This reflects that such systems would handle confidential State Party data, support critical verification decisions, and operate within legal frameworks where errors could have serious security, legal, and trust-related consequences. High-risk designation places significant obligations on developers and deployers to implement robust safeguards, maintain transparency, and ensure human oversight throughout AI-assisted processes. Global initiatives—such as the Toolkit for Responsible AI Innovation in Law Enforcement[52] developed by the International Criminal Police Organization (INTERPOL) and the United Nations Interregional Crime and Justice Research Institute (UNICRI)—further underscore the need for technical deployments to be anchored in strong ethical and governance frameworks.

[51] "High-Level Summary of the AI Act." EU Artificial Intelligence Act, accessed December 23, 2025.

[52] "Toolkit for Responsible AI Innovation in Law Enforcement." United Nations Interregional Crime and Justice Research Institute, accessed February 18, 2026.

116. The deployment of AI in the security domain must also align with established accountability frameworks. Europol's Accountability Principles for Artificial Intelligence underscore the principle of legality, requiring that all AI use be lawful and governed by formal, promulgated rules.[53] Accordingly, implementation must include mandatory assessments, such as human rights and data protection impact assessments (HRIAs and DPIAs, respectively), to ensure legitimate use and mitigate risks to fundamental rights. AI deployment and operationalisation should therefore be anchored in a robust governance framework aligned with emerging international standards, with particular emphasis on human oversight, accountability, and verifiable assurance across the technology lifecycle.

117. Building on lessons learned from the IAEA, the following guiding principles covering core areas of AI governance to inform the deployment of AI at the OPCW have been identified.

   a. Human decision-making: Experts retain final authority; AI augments, not replaces.
   b. Document fidelity: Original content is preserved; no unvalidated alterations.
   c. Accountability: Clear responsibilities and audit trails for all AI-assisted actions.
   d. Security and traceability: Data is protected, access-controlled, and fully auditable.
   e. Transparency: States Parties are fully informed about AI use, including the safeguards and human oversight mechanisms in place, to uphold trust.

118. The IAEA applies human-in-the-loop approaches to all critical processes, with no automated decision-making on matters of verification significance. This reflects a fundamental principle endorsed by the TWG more broadly: AI systems should augment, rather than replace, human experts by improving efficiency and effectiveness. Accordingly, the TWG proposes that the OPCW declaration processing system should integrate an expert review process that allows reviewers to validate and edit extractions, with records only approved when the structured output accurately represents the original declaration. Final decisions on content, interpretation, and verification implications must remain with qualified staff. The system must provide transparent workflows and comprehensive records to ensure it is always clear whether errors originate from AI processing or human oversight. Similarly, OPCW chatbot outputs used for operational or administrative purposes should also be subject to human validation before use. This approach preserves technical rigour by keeping experts accountable for the data quality and accuracy, while AI handles the time-intensive processing tasks. This principle of augmentation

[53] Akhgar, B., P.S. Bayerl, K. Bailey, R. Dennis, H. Gibson, S. Heyes, A. Lyle, A. Raven, and S. Fraser. *Accountability Principles for Artificial Intelligence (AP4AI) in the Internal Security Domain.* Europol, February 22, 2022.

rather than replacement should be embedded in system design, user training, and operational workflows.

119. To protect the legal integrity of State Party declarations, all submissions must be preserved in their original "as-declared" form. Consequently, any transformations—including digitisation or translation—should be documented and validated by experts, while systems must not alter, correct, or interpret declaration content.

120. Any deployed AI system must comply with requirements set forth in the Convention's Confidentiality Annex[54] and the OPCW Policy on Confidentiality,[55] which govern the protection of confidential information provided by States Parties. Furthermore, the generative nature of LLMs, coupled with their training on vast datasets, introduces unique security vulnerabilities requiring the establishment of mitigation strategies (see Table 3). A robust data management framework will therefore be pivotal in ensuring data reliability and protection.

121. To ensure the highest level of security for sensitive State Party information, the OPCW operates on air-gapped architecture—isolated from external networks and web-based applications. Any AI-assisted processing must be designed from the outset to function within this air-gapped environment, preferably on-premises or within a highly secure private cloud infrastructure. Strict access controls are paramount to safeguard sensitive data throughout the system's lifecycle.[56] The rigorous containment afforded by these approaches will protect data sovereignty by preventing confidential Secretariat or State Party data from being transmitted back to external models, a process referred to as data leakage.[57,58] A secure, isolated environment ensures that sensitive data are not captured, retained, and inadvertently exposed by the external model, reducing the risk of compromising ongoing operations.[59] Data storage must therefore be securely configured, in line with the OPCW's IT policy and recognised cybersecurity standards.[60] For AI systems used in critical infrastructure, deployment decisions should explicitly balance functionality

[54] "Confidentiality Annex." OPCW, accessed December 23, 2025.

[55] OPCW Policy on Confidentiality (C-I/DEC.13/Rev.1, dated 2 February 2006).

[56] *Security and Privacy Controls for Information Systems and Organizations.* National Institute of Standards and Technology, December 10, 2020.

[57] "LLM02:2023 - Data Leakage." The Open Source Foundation for Application Security, November 2024.

[58] Samanta, Diptisha. "When Prompts Leak Secrets: The Hidden Risk in LLM Requests." Keysight, August 4, 2025.

[59] "What Are the Main Risks to LLM Security?" Check Point Software, May 7, 2025.

[60] Kahana, Eran. "AI Data Stewardship Framework." Stanford Law School Blogs, March 9, 2023.

and security, with priority given to mitigating risks arising from the misuse of sensitive information.[61]

122. Considering the declarations processing system, complete traceability and auditability of all changes and validations should be maintained. The system should document when each declaration was received, when and how it was digitised, who validated the digitisation, when data was extracted, who approved the extraction, and who has accessed the data subsequently. This comprehensive audit trail will serve multiple purposes: it would ensure accountability for processing confidential information, provide States Parties with sufficient confidence in the system's integrity, and enable the OPCW to demonstrate that its verification processes meet appropriate standards of rigour and reliability.

123. The deployment of LLMs should ensure the implementation of robust validation and access controls to prevent malicious manipulation of the system through prompt injection attacks. These attacks involve inserting malicious input into the model's request, effectively misleading the LLM into generating harmful or inappropriate content, leaking sensitive information, or executing unauthorised actions.[59]

124. Comprehensive authentication, authorisation, and encryption measures are also essential to prevent unauthorised access and model theft. This includes the copying, extraction, or replication of OPCW ML models, algorithms, or their learned parameters (weights), which could be exploited to access sensitive data.

Table 3: Key LLM security vulnerabilities and mitigation strategies for internal deployment

Vulnerability	Description	Mitigation strategies
Data leakage[57]	Accidental disclosure of sensitive, confidential, or proprietary information during response generation	Secure, isolated environment to prevent external model access to sensitive input/output
Prompt injection	Malicious input used to override system instructions, leading to unauthorised actions or content generation	Implementation of rigorous processes for input validation, sanitisation, and continuous monitoring within the system
Model theft	Unauthorised copying or exfiltration of the proprietary LLM model or its weights	Robust authentication, authorisation, and encryption of the internal infrastructure to secure access

[61] *Mitigating Artificial Intelligence (AI) Risk: Safety and Security Guidelines for Critical Infrastructure Owners and Operators.* Department of Homeland Security, April 2024.

125. While these guiding principles establish a foundation for responsible AI use at the OPCW, it was noted that their effective application will depend on how AI systems are embedded within organisational processes and supported by staff and data practices. The operationalisation of AI systems requires workflow integration, investment in staff capacity, and robust data governance mechanisms to ensure they function as intended.

Workflow integration

126. It is crucial that the Secretariat prioritises a systematic redesign of workflows over isolated technology adoption, actively restructuring processes to integrate AI capabilities rather than simply layering new tools onto existing procedures.[62] This would ensure robust human-in-the-loop oversight, enabling experts to interpret model outputs, intervene when necessary, and validate accuracy before information is incorporated into critical decision-making processes.

Staff capacity

127. Capacity building in the Secretariat will be essential to support the effective integration of AI tools. The TWG therefore proposes that an internal capacity-building programme—depicted in Figure 8—be designed and implemented to facilitate the OPCW's transition to an AI-ready environment. This programme would encompass three interconnected areas: staffing and recruitment, training and skills development, and knowledge management and transfer. Together, these elements would ensure that AI augments human expertise without replacing human judgement, accountability, or decision-making authority to effectively implement the Convention. Once sufficient internal capacity is established, the programme could be extended to support capacity building across States Parties.

128. The TWG proposes that the Secretariat adopt a balanced staffing strategy combining technical AI specialists, subject-matter experts with AI literacy, and hybrid roles that bridge technical and domain expertise. The rationale for this is discussed below and subsequently summarised in Table 4. As a point of reference, it was noted that, within the IAEA, the Department of Safeguards is supported by dedicated data science and software engineering expertise for its AI applications. Furthermore, staff with

[62] Singla, Alex, Alexander Sukharevsky, Bryce Hall, Lareina A. Yee, and Michael Chui. "The State of AI in 2025: Agents, Innovation, and Transformation." McKinsey & Company, November 5, 2025.

verification policy and information security knowledge are closely involved in setting associated policies.

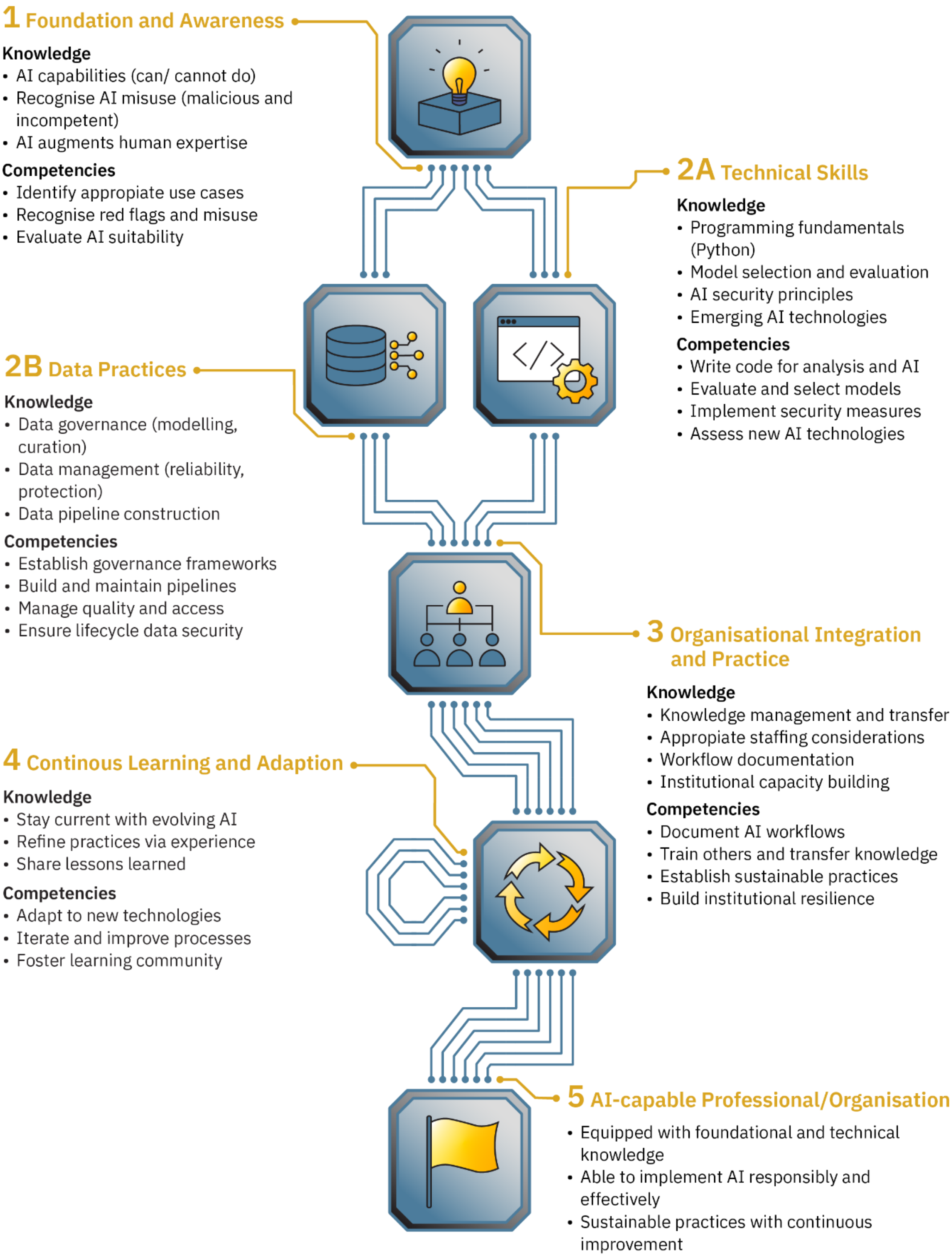
129. Specialised technical staff—primarily data scientists, data engineers, and software engineers—are critical to the development, iteration, and ongoing maintenance of advanced AI models and their supporting data infrastructure. Data scientists design and optimise models, while data engineers build and maintain the high-volume data pipelines that feed and monitor them, ensuring data quality and accessibility.[60] This foundation underpins documented operational efficiencies, including significant reductions in data preparation time.[63] Finally, software engineers are required to integrate new AI capabilities into existing systems, collaborating with subject-matter experts and ML engineers.[51]

Recommendation 10

The Secretariat should seek to hire staff with expertise in AI, including data scientists and software engineers. Expertise in this area is critical for the OPCW to fully leverage advances in AI in its work.

130. While technical AI specialists provide critical skills, domain experts are better equipped to identify scientifically implausible or procedurally inappropriate AI outputs. Sustainable implementation therefore requires upskilling existing OPCW staff by developing AI literacy, enabling them to effectively oversee AI-assisted processes, understand typical errors of AI systems, and maintain a healthy scepticism toward automated outputs. This includes the ability to interpret and interrogate AI outputs produced by partially or fully opaque ("black box") systems, drawing on explainability methods and contextual understanding rather than accepting results at face value. Staff should also be trained to recognise and mitigate incompetent misuse, which can arise from over-reliance on outputs generated by biased, unstable, or malfunctioning models, or from failing to initiate necessary human overrides, consistent with human-in-the-loop governance principles.

[63] Li, Jingquan. "Security Implications of AI Chatbots in Health Care." *Journal of Medical Internet Research* 25 (November 28, 2023). https://doi.org/10.2196/47551.



1 Foundation and Awareness

Knowledge

- AI capabilities (can/ cannot do)
- Recognise AI misuse (malicious and incompetent)
- AI augments human expertise

Competencies

- Identify apropiate use cases
- Recognise red flags and misuse
- Evaluate AI suitability

2A Technical Skills

Knowledge

- Programming fundamentals (Python)
- Model selection and evaluation
- AI security principles
- Emerging AI technologies

Competencies

- Write code for analysis and AI
- Evaluate and select models
- Implement security measures
- Assess new AI technologies

2B Data Practices

Knowledge

- Data governance (modelling, curation)
- Data management (reliability, protection)
- Data pipeline construction

Competencies

- Establish governance frameworks
- Build and maintain pipelines
- Manage quality and access
- Ensure lifecycle data security

3 Organisational Integration and Practice

Knowledge

- Knowledge management and transfer
- Appropriate staffing considerations
- Workflow documentation
- Institutional capacity building

Competencies

- Document AI workflows
- Train others and transfer knowledge
- Establish sustainable practices
- Build institutional resilience

4 Continous Learning and Adaption

Knowledge

- Stay current with evolving AI
- Refine practices via experience
- Share lessons learned

Competencies

- Adapt to new technologies
- Iterate and improve processes
- Foster learning community

5 AI-capable Professional/Organisation

- Equipped with foundational and technical knowledge
- Able to implement AI responsibly and effectively
- Sustainable practices with continuous improvement

Figure 8: Proposed programme to build internal AI capacity

131. Training should also cover best practices for AI use,[64] enabling them to critically assess which workflows could benefit from AI integration, how to leverage AI capabilities by restructuring existing processes, how to maintain quality control and accountability, and ultimately how to identify potential patterns of misuse. The TWG therefore proposes that this training cover workflow engineering, the technical aspects of how the system functions, the role and limits of explainability in AI-assisted decision-making, and the procedural aspects of how staff critically evaluate and validate AI-generated outputs.[65] It should offer hands-on, tactical instruction built around use-case-driven methodologies, supported by concrete examples, guided exercises, and appropriate implementation testing.[66]

132. Non-technical staff should receive tailored AI literacy training to provide them with a clear understanding of AI capabilities, limitations, and potential bias. Practical workshops that convene subject-matter experts and technical staff could enable the co-development of AI applications within the experts' domain. AI literacy could also be strengthened through rotation programmes, in which subject-matter experts are temporarily embedded in data science teams to provide domain guidance. In parallel, clear career pathways recognising AI literacy as a valuable professional development achievement should be established.

133. The recognition of malicious misuse requires integrating cybersecurity and supply chain security into the training mandate. Malicious misuse protocols are required to mitigate risks related to the data supply chain and the insertion of maliciously modified data.[67] Consequently, staff involved in technology acquisition should be trained on the importance of vendor transparency regarding the sources of data a tool was trained on and the transformations applied to that data.[68] This structural integration of procurement procedures into the risk mitigation protocol ensures that deployed systems are founded upon demonstrably trusted datasets and infrastructure.[67]

[64] "NSA's AISC Releases Joint Guidance on the Risks and Best Practices in AI Data Security." National Security Agency/Central Security Service, May 22, 2025.

[65] *Considerations for Deploying Artificial Intelligence Applications in the Nuclear Power Industry.* International Atomic Energy Agency, accessed November 12, 2025.

[66] "AI in National Security: Integrating Artificial Intelligence into Public Sector Missions." Coursera, accessed November 23, 2025.

[67] *AI Data Security: Best Practices for Securing Data Used to Train & Operate AI Systems.* The National Security Agency's Artificial Intelligence Security Center, May 2025.

[68] Rishel, Paige, Carol Smith, Brigid O'Hearn, and Rita Creel. "Artificial Intelligence in National Security: Acquisition and Integration." *Carnegie Mellon University, Software Engineering Institute's Insights (blog).* Carnegie Mellon's Software Engineering Institute (August 5, 2025). https://doi.org/10.58012/gfnb-pr02.

134. The OPCW should aim for baseline AI literacy across all personnel, with approximately five to ten subject-matter experts receiving advanced AI governance and oversight training. These experts would subsequently serve as dedicated AI-domain liaisons, able to participate in scoping AI projects and defining requirements and conduct operational validation testing of AI system outputs, while representing verification and compliance perspectives in AI governance decisions.

135. As AI-enabled systems are progressively introduced into core workflows, effective knowledge management and transfer will become increasingly important to ensure organisational retention and sharing of technical understanding, operational context, and institutional expertise. Knowledge transfer formalises the highly specialised expertise of data scientists and software engineers, encompassing secure deployment practices, model development methodologies, and the implementation of organisational data governance.[69]

136. Exploring the IAEA's knowledge management practices, several approaches that could be applicable to the OPCW due to similarities between both organisations—notably in the area of verification—have been identified. These include:

a. documentation of standard operating procedures for AI-assisted analytical workflows, ensuring consistency;

b. mentorship and rotation programmes pairing experienced inspectors/analysts with newer staff, ensuring transfer of tacit knowledge;

c. lessons-learned databases capturing insights, including from inspection missions and AI system performance issues;

d. regular technical workshops, bringing together field practitioners and headquarters analysts to share operational experiences and refine AI governance practices; and

e. formal documentation requirements for AI system development decisions, including rationale for model choices, training data sources, and validation approaches.

137. Consequently, the TWG proposes the adoption and implementation of a similar structure at the OPCW to fully leverage the specialised expertise of data scientists, software engineers, and subject-matter experts. This expertise should be clearly documented and made accessible to future staff, thereby preserving organisational knowledge and mitigating risks associated with personnel turnover.

[69] Gomstyn, Alice, and Alexandra Jonker. "What Is Data Stewardship?" IBM, December 24, 2025.

Table 4: Justification for required staffing

Recommendation component	Primary domain function	Strategic justification (source)	Organisational impact
Subject-matter experts with AI literacy	Business analysis, partnering with data scientists and engineers to achieve accurate and functional workflows	Drive organisational change, ensure adoption of new processes, ensure accuracy	Capturing strategic value from AI; achievement of high performer status[62]
Data scientists	Model design, iteration, and complex analytics deployment[56]	Drive organisational transformation, innovation, and growth objectives[62]	Capturing strategic value from AI; achievement of high performer status[62]
Data engineers	Infrastructure development, pipeline construction, data preparation	Identified as most in-demand technical roles; essential talent strategy component[62]	Efficient data curation; foundation for scalable, trustworthy AI systems[70]
Software engineers	System integration, scaling, end-to-end ML feature integration[56]	Required for informed supervision and critical assessment; mandatory for explainability[65]	Operational resilience; assurance of scientific and technical rigour
Knowledge management/ transfer	Documentation, institutionalising AI-centric workflows and practices[56]	Essential management practice for achieving sustained business impact[62]	Institutional resilience: continuity of expertise and scaled AI adoption[70]

138. It is envisaged that the capacity-building initiative would be multi-phase and evolving, rather than a one-time training programme. The roles and responsibilities associated with this AI capacity-building initiative are set out in a RACI chart in Annex 6, which assigns those responsible, accountable, consulted, or informed. Considering the rapid pace of AI technological development, associated with an increasing risk of misuse in chemical weapons contexts, the programme should be designed for

[70] Arora, Simran Singh. "How Data Governance Improves AI Success?" Medium, October 23, 2025.

adaptability and continuous improvement, prioritising practical applications, governance literacy, and preparedness for evolving technical roles.

Data governance

139. For the OPCW, data governance is not exclusively an IT compliance exercise; it is essential for ensuring data integrity—maintaining accuracy, completeness, and fidelity to its original source—thereby enabling explainable and traceable system outputs,[70] and mitigating operational and security risks. The principal areas of data governance are shown in Figure 9 and the relationship between data governance, AI system integrity, and compliance is summarised in Table 5. Establishing a structured data governance framework within the Organisation's operational infrastructure is therefore critical. It should prioritise comprehensive data protection strategies, addressing the core requirements for protection, reliability, and trust throughout the entire AI system lifecycle.

140. The IAEA has implemented several initiatives in the context of nuclear security and safety that offer relevant lessons for data management in verification contexts. The Agency has emphasised robust cybersecurity measures and established remote data transmission infrastructure to ensure secure collection of safeguards data from facilities worldwide. For data reliability, the IAEA conducts interlaboratory comparisons to assess data accuracy, as demonstrated by their work with Japanese laboratories on marine samples near the Fukushima Daiichi Nuclear Power Plant. These efforts collectively aim to promote responsible and effective use of technology in the nuclear sector, ensuring that data is curated, protected, and reliable for critical applications—objectives that parallel OPCW's verification requirements.

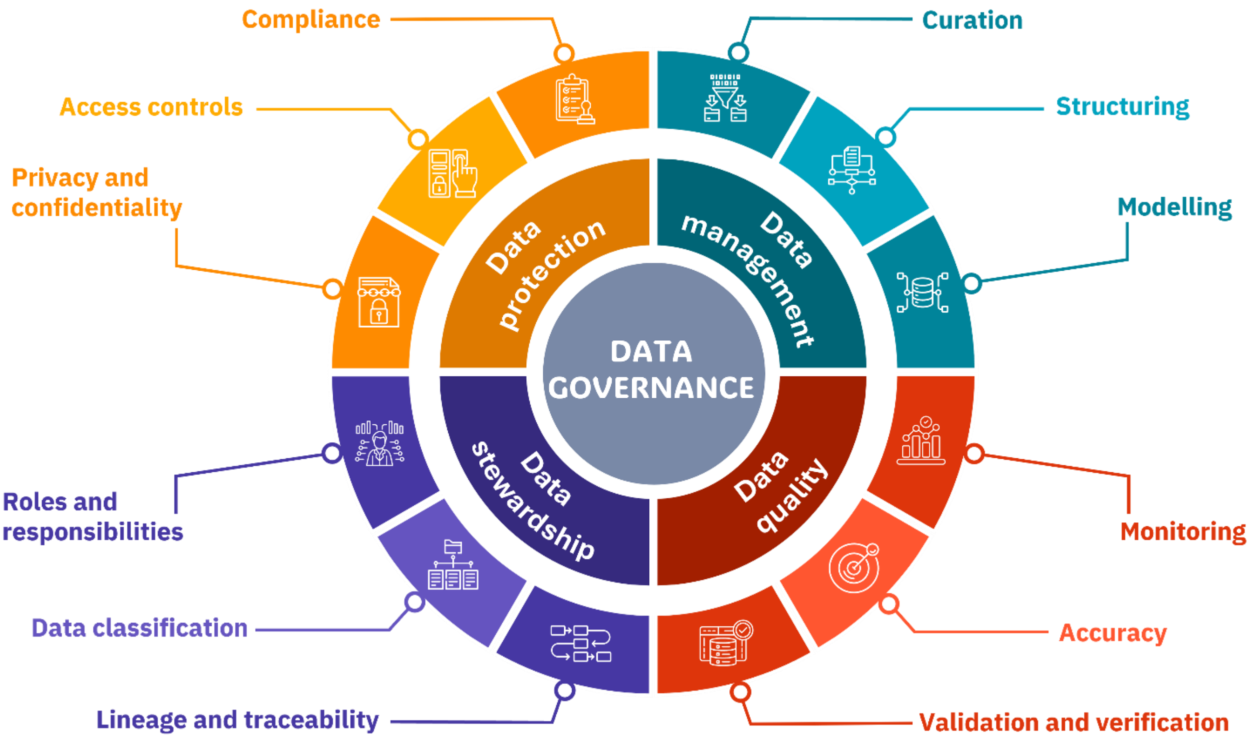


Figure 9: Overview of data governance

141. Data protection strategies should include technical controls such as tracking data provenance, leveraging trusted infrastructure, and employing digital signatures to authenticate reliable revisions.[64] These would ensure protection of sensitive and confidential information—through role-based access controls, appropriate data classifications, and audit procedures—while mitigating risks across the AI data supply chain, including unauthorised access, data leakage, loss, malicious modifications, and data drift.[64]

142. Data reliability—maintaining data accuracy, consistency, and completeness—depends on the consistent enforcement of the technical controls defined by the governance framework. Failure to implement such controls leads to poor model performance, reduced institutional trust, and high failure rates of AI deployments.[70] Governance must therefore function not as a bureaucratic layer, but as a core enabling infrastructure that supports reusable, auditable, and explainable data as a foundation for advanced AI systems, including enterprise-level agentic AI.[70]

143. Effective AI deployment within the OPCW will rely on a structured relationship between data governance, stewardship, and management. Governance sets the rules and standards, stewardship ensures accountability in applying them, and management—through data modelling, curation, and structuring—transforms raw data into accurate, consistent, and machine-readable formats.

144. Data stewardship guarantees the integrity and quality of data used by AI systems, maintaining effective, compliant, and ethically aligned AI processes.[69] It also supports successful data curation by promoting accessibility, usability, and security.[69] Since AI outcomes are functionally dependent on the quality and integrity of input data, clearly defined data ownership establishes accountability for data quality, classification, and integrity at an organisational level. This ensures responsibility for data is embedded within governance structures, fulfilling internal requirements and providing a necessary human layer of responsibility for AI-driven outcomes.

145. Data stewards, who are frequently subject-matter experts, are specifically trusted with managing metadata, tracing data lineage, classifying sensitive data, and defining necessary data quality metrics.[69] High-quality, standardised data input reduces operational friction and accelerates the AI model development cycle by eliminating the need for extensive data rework.[70] Evidence from the financial services sector indicates that organisations implementing robust data quality and governance strategies are able to reduce the time required to prepare data for AI models by approximately 75%.[71]

146. Furthermore, roles and responsibilities should be identified and formalised for the continuous human oversight of data processes, requiring that clear acceptable use policies be developed and systematically enforced.[60]

[71] Galvez, Rachel. "AI Success – Powered by Data Governance and Quality." Precisely, July 11, 2025.

Table 5: Mapping data governance components to security and compliance objectives

Recommendation component	Justification rationale (source)	Impact on AI system integrity	Compliance/risk mitigation
Data modelling, curation, and structuring	Ensures high-quality, standardised, and accessible data input[70]	Higher trust, faster model development, reduced rework cost[70]	Accuracy, reliability, and operational integrity of outcomes[64]
Data stewardship/owners	Defines quality metrics and tracing data lineage[69]	Consistent data interpretation, improved institutional audit readiness[69]	Accountability, regulatory risk reduction via audit trails[70]
Access controls/protection	Safeguards sensitive data within isolated, secure operating environments[56]	Prevention of unauthorised access and mitigation of malicious data modification[64]	Cybersecurity environment maintenance, policy enforcement[60]

AI capacity building in States Parties

147. In 2024, the Secretariat held two events dedicated to exploring and deepening its understanding of the opportunities and risks posed by AI with regard to its work and, more broadly, to the implementation of the Convention.[8,11] These events underscored varying degrees of AI development and capabilities across States Parties. While some possess advanced AI technologies supported by robust and sophisticated data infrastructure, enabling them to manage Convention-related information, others have insufficient expertise and resources, as well as inadequate or non-existent governance frameworks to appropriately safeguard sensitive data.

148. Data curation, protection, and reliability are fundamental to AI development and deployment, as they ensure the generation of accurate, trustworthy, and effective AI systems able to support the implementation of the Convention. Disparities in AI readiness, technical infrastructure, and regulatory maturity across Member States may therefore lead to inconsistencies in data quality and reliability.

149. To address this, approaches for strengthening capacity in States Parties with less developed AI technologies and infrastructure were considered. In doing so, capacity-building programmes implemented by the OPCW and other international organisations were examined for their potential application in an AI context, highlighting key parallels.

150. Since the Laboratory Assistance Programme was first established in December 2002,[72] the OPCW has successfully employed twinning partnerships to strengthen the technical competence of laboratories in Member States with developing or transition economies. Through structured partnerships between laboratories with advanced capabilities (Assisting Laboratories) and those with developing capabilities (Assisted Laboratories), and by leveraging well-defined approaches such as technical evaluation visits, mentoring, and infrastructure support, it has been demonstrated that competence gaps in chemical analysis can be effectively bridged. The proven success of this model provides a solid foundation for addressing emerging technical and/or technological challenges that extend beyond traditional chemical analysis, including data- and digitally driven capabilities.

151. The TWG underscores the potential of leveraging such partnerships to address AI capacity gaps and systematically strengthen data management competencies, recognising these as essential for States Parties to benefit from AI technologies. Based on the Laboratory Twinning and Assistance Programme, the TWG proposes that an analogous twinning initiative for AI, coordinated and facilitated by the Secretariat, be developed.

152. States Parties with advanced AI capabilities play a key role in this capacity-building process, and the TWG encourages them to provide resources, expertise, technical assistance, and training, while sharing best practices and experiences. Training should be comprehensive and cover a wide variety of aspects—from basic principles to advanced applications—relevant to the implementation of the Convention. Technical assistance may also include access to specialised software, datasets, computational resources, and analytical tools. This role equates to that of the Assisting Laboratory.

153. States Parties with emerging AI capabilities (Assisted Laboratories) would also play a critical role in the success of this initiative due to their unique perspectives and the implementation challenges they are facing. The importance of sharing specific use cases and requirements to inform international collaborations on data management approaches, addressing real-world constraints and diverse operational contexts, was emphasised.

[72] In 2020, the Laboratory Twinning and Assistance Programme (S/1887/2020, dated 4 August 2020) integrated and subsequently replaced the Laboratory Assistance Programme (S/328/2002/Rev.1, dated 19 December 2002) and the Laboratory Twinning Initiative (S/1397/2016, dated 14 July 2016).

Recommendation 16

States Parties and the Secretariat should develop and establish a twinning initiative for the responsible and effective integration of AI technologies to support the implementation of the Convention. The Secretariat would facilitate partnerships enabling States Parties with advanced AI capabilities to "twin" with States Parties with emerging AI capabilities. These partnerships would support capacity-building measures, including training and technical assistance, exchange of best practices and knowledge, and the promotion of a shared understanding of responsible AI use and its potential risks within the context of the Convention.

154. To guide the development of an OPCW AI-focused capacity-building framework, initiatives addressing AI capability gaps and capacity-building efforts led by other international organisations were examined. International efforts—including the United Nations General Assembly resolution on "Enhancing International Cooperation on Capacity-Building of Artificial Intelligence",[73] the Global Digital Compact,[74] and the AI Capacity-Building Action Plan for Good and for All[75]—emphasise the importance of making AI benefits accessible to all countries, particularly developing ones. Such initiatives advocate the provision of training, technical assistance, and best practices to help these countries harness AI's potential while mitigating its risks. They also highlight principles directly relevant to the OPCW: promoting secure and responsible cross-border data sharing and use, ensuring AI fairness, safety, and reliability, and supporting capacity building that strengthens not only technical skills but also governance, ethics, and institutional capabilities.

155. The International Telecommunication Union's (ITU's) AI for Good initiative also plays a significant role in the AI capacity-building landscape, particularly in bridging capability gaps between countries with advanced and developing AI ecosystems.[76] The initiative has developed several relevant mechanisms, particularly in the context of AI skills, governance, data use, and digital transformation. For example, the AI Skills Coalition is a United Nations-led platform for AI education and capacity

[73] *Enhancing international cooperation on capacity-building of artificial intelligence* (A/RES/78/311). United Nations, July 5, 2024.

[74] The Global Digital Compact is a comprehensive global framework for digital cooperation and governance of AI.

[75] Artificial Intelligence Capacity-Building Action Plan for Good and for All (A/79/545). United Nations, October 23, 2024.

[76] "AI for Good." AI for Good, accessed December 23, 2025.

building.[77] It offers a range of training courses on AI fundamentals and its responsible use, available in multiple languages, supporting the broader democratisation of AI learning.

156. Other OPCW TWGs have also recognised the importance of capacity building through international networks and partnerships. For example, the TWG on the Analysis of Biotoxins recommended the establishment of an informal network of biotoxin analysis laboratories to facilitate the sharing of knowledge, resources, and expertise between States Parties with advanced capabilities and those with emerging ones, with the aim of strengthening global efforts in forensic analysis.[78]

157. An examination of these international initiatives, together with the OPCW Laboratory Twinning and Assistance Programme, revealed several elements essential for developing capacity-building frameworks that effectively address technical competence gaps. These include:

a. forming structured partnerships that pair entities with advanced capabilities with those seeking to develop such capabilities, with clear roles and responsibilities for both partners;

b. implementing tangible support mechanisms rather than abstract commitments. For existing AI initiatives, these include practical training programmes, technical assistance—such as access to tools and datasets—and pilot implementations enabling hands-on learning;

c. leveraging existing frameworks and international standards rather than developing entirely new proprietary approaches;

d. establishing clear eligibility criteria—matching capable and committed partners—and operational procedures;

e. applying transparent coordination mechanisms and established implementation processes; and

f. recognising that capacity building is a medium- to long-term endeavour requiring sustained commitment and flexible funding models.

158. Taking these findings into account, the TWG proposes several actions to support effective AI capacity building. First, the Secretariat could provide training—both in-person and online—and technical development assistance for States Parties with emerging AI capabilities. This should cover data collection, pre-processing, and analysis techniques, as well as ethical considerations in AI deployment.

[77] "AI Skills Coalition." AI for Good, accessed December 23, 2025.

[78] Report of the Scientific Advisory Board's Temporary Working Group on the Analysis of Biotoxins (SAB/REP/1/23, dated April 2023).

159. To support data curation and sharing, the TWG proposes that the Secretariat establish a centralised data repository, which would be accessible to all States Parties. This would facilitate the curation and sharing of high-quality, anonymised datasets relevant to Convention-related AI applications—with contributions encouraged from States Parties—thereby providing resources essential for AI development and validation. In addition, the TWG suggests that the OPCW compile and disseminate information on real-world use cases where AI has been successfully applied in Convention-related activities, highlighting both successes and challenges.

160. The TWG proposes that the Secretariat facilitate collaborative AI projects on Convention-related activities between States Parties with advanced AI capabilities and those with emerging ones, encompassing joint data collection, analysis, and application development. The Group encourages the Secretariat to disseminate the results and best practices established through these projects, creating a knowledge base that would benefit the broader OPCW community and ensuring the responsible and effective integration of AI strategies and methodologies.

161. To strengthen data protection measures, the Secretariat should develop and share guidelines and best practices on data protection and cybersecurity for AI applications. The guidelines should cover data encryption, access controls, and secure data storage to ensure that States Parties are suitably prepared to protect sensitive information against unauthorised access and cyber threats. The TWG proposes that the Secretariat leverage existing international data security standards to strengthen data protection in States Parties, rather than develop new OPCW-specific frameworks. These standards could include International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2022 (for information security, cybersecurity, and privacy protection),[79] ITU Telecommunication Standardization Sector (ITU-T) X.2210 (provides implementation guidelines for digital watermarking),[80] and ITU-T Y.3054 (defines the framework for trust-based media services).[81]

162. To promote and ensure data reliability and quality, the Secretariat could implement a quality assurance framework for data used in AI applications, leveraging existing standards such as ISO/IEC Technical Report 24028:2020 (trustworthiness in AI

[79] *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC 27001:2022). International Organization for Standardization and International Electrotechnical Commission, October 2022.

[80] *Implementation guidelines for digital watermarking* (ITU-T Recommendation X.2210). International Telecommunication Union, Telecommunication Standardization Sector, this recommendation is currently under the traditional approval process.

[81] *Framework for trust-based media services* (ITU-T Recommendation Y.3054). International Telecommunication Union, Telecommunication Standardization Sector, May 2018.

systems)[82] and ISO 24138:2024, the new standard for the International Standard Content Code.[83] This framework should include validation protocols and standards to ensure data accuracy, consistency, and reliability. Volunteer audits and peer reviews by third parties, invited by either the Secretariat or States Parties, could be conducted to maintain exacting standards of data integrity.

Recommendation 15

The Secretariat should design, develop, and implement a capacity-building programme for States Parties that:

a. provides information on the latest AI capabilities;
b. enables the recognition of AI misuse, both malicious and accidental;
c. develops data governance capabilities (including data modelling, curation, and structuring, data stewardship and ownership, and identifying access controls);
d. develops data management capabilities (data reliability and protection, enforcing access controls);
e. promotes the use of AI-supported simulation and communication tools, particularly to enhance chemical safety and emergency response capabilities; and
f. shares guidance and best practices for the safe and responsible use of AI in chemical production and research.

163. The beneficiaries of such a programme would include National Authorities (managing chemical industry declarations, facility inspections, and compliance reporting), OPCW Designated Laboratories and analytical facilities (leveraging data governance frameworks for AI-assisted chemical analysis), and national research and regulatory agencies (overseeing AI deployment in sensitive or dual-use chemical research contexts). The programme scalability is required, in addition to the establishment of a comprehensive framework intended for stakeholders with substantial resources, such as National Authorities in States Parties with advanced AI capabilities. In parallel, modular, tiered guidance should enable States Parties with limited resources to adopt elements progressively. It is recognised that the full implementation of all staffing and infrastructure recommendations may not be feasible for every State

[82] *Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence* (ISO/IEC TR 24028:2020). International Organization for Standardization and International Electrotechnical Commission, May 2020.

[83] *Information and documentation — International Standard Content Code (ISCC)* (ISO 24138:2024). International Organization for Standardization, May 2024.

Party, and priority should be assigned to core data governance and training in recognising AI misuse.

164. Key steps in the proposed approach to adopting and operationalising AI at the OPCW and building capacity in States Parties are shown in Figure 10.

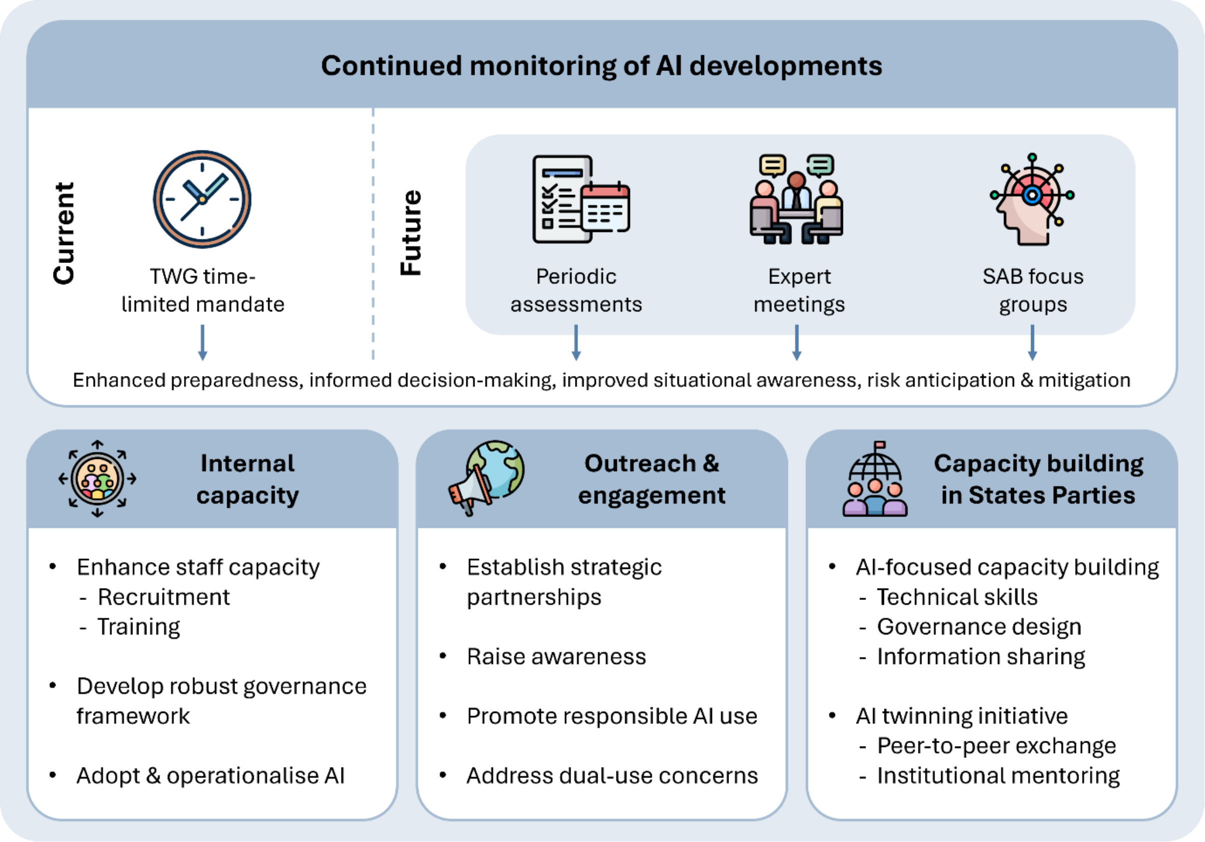

Continued monitoring of AI developments
Current
TWG time-limited mandate
Future
Periodic assessments
Expert meetings
SAB focus groups
Enhanced preparedness, informed decision-making, improved situational awareness, risk anticipation & mitigation
Internal capacity
• Enhance staff capacity
- Recruitment
- Training
• Develop robust governance framework
• Adopt & operationalise AI
Outreach & engagement
• Establish strategic partnerships
• Raise awareness
• Promote responsible AI use
• Address dual-use concerns
Capacity building in States Parties
• AI-focused capacity building
- Technical skills
- Governance design
- Information sharing
• AI twinning initiative
- Peer-to-peer exchange
- Institutional mentoring

Figure 10: Proposed approach to adopting AI and building capacity

SUBGROUP 3: DATA PREDICTION AND FUSION

Introduction

165. Subgroup 3 focused on exploring how detection and analysis capabilities can be enhanced through AI—specifically, the use of AI for molecular property and spectral prediction, data generation, and data/sensor fusion, while also considering associated misuse risks.

166. The prediction and generation of properties and data, as well as the fusion of data from multiple sources, are areas of scientific research that are benefitting significantly from advances in AI. In the chemical sciences, ML and deep learning approaches have evolved from simple pattern recognition tools into predictive systems capable of handling complex molecular interactions and high-dimensional chemical and spectral datasets. In this context, AI techniques are increasingly used to infer physical, chemical, and spectral properties of substances from limited or indirect inputs, generate synthetic data that augment scarce or incomplete datasets, and integrate heterogeneous streams of data—such as analytical measurements, sensor outputs, and relevant metadata. These capabilities are particularly relevant for verification activities, where rapid interpretation of complex and high-dimensional data is essential.

167. Property and spectral prediction models allow estimation of key characteristics, such as toxicity, stability, reactivity, or spectroscopic signatures, without requiring exhaustive experimental measurement. Data/sensor fusion approaches combine inputs from multiple analytical techniques or monitoring systems, enabling patterns, anomalies, or signatures of interest to be identified with greater sensitivity and robustness than would be possible using any single data source in isolation.

168. The valuable potential of these approaches is illustrated by developments beyond the chemical domain. The impact is perhaps most visibly demonstrated by the awarding of the 2024 Nobel Prize in Chemistry for advances in computational protein design and structure prediction,[84] enabled by tools such as AlphaFold, an AI system developed by Google DeepMind that predicts a protein's three-dimensional structure from its amino acid sequence.[85] By reducing the time required to predict protein folding from years to days or even hours, AlphaFold highlights how AI-driven property prediction can dramatically accelerate and enhance scientific research. While the

[84] "Nobel Prize in Chemistry 2024." Nobel Prize, October 9, 2024.

[85] Jumper, John, Richard Evans, Alexander Pritzel, Tim Green, Michael Figurnov, Olaf Ronneberger, Kathryn Tunyasuvunakool, et al. "Highly Accurate Protein Structure Prediction with AlphaFold." *Nature* 596, no. 7873 (July 15, 2021): 583–89. https://doi.org/10.1038/s41586-021-03819-2.

specific applications differ, the underlying methodological shift has direct relevance in the chemical domain, which was explored in depth by Subgroup 3.

AI in property, spectra, and data prediction

Molecular property prediction

169. Molecular property prediction enables the estimation of key physicochemical, toxicological, and spectral characteristics of substances without requiring their synthesis or experimental measurement. This capability supports rapid screening, risk assessment, and prioritisation across large areas of chemical space, which is particularly valuable for novel, hypothetical, or poorly characterised compounds. It is most commonly applied in drug discovery, chemical safety, and materials design, where these predictions can accelerate research and reduce experimental costs.

170. Recent advances in AI, particularly ML and deep learning, have revolutionised molecular property prediction by enabling models trained on millions of known molecules to accurately predict properties of previously unseen compounds (see Figure 11). These models can predict a wide range of properties—including solubility, melting and boiling points, partition coefficients, and reactivity—without requiring expensive experimental measurements or time-consuming quantum mechanical calculations.[86,87,88] By using diverse molecular representations,[89] from classical descriptors to graph-based encodings, AI-powered molecular property prediction allows researchers to rapidly screen thousands of candidate compounds and prioritise the most promising ones for synthesis and testing.

[86] Liyaqat, Tanya, Tanvir Ahmad, and Chandni Saxena. "Advancements in Molecular Property Prediction: A Survey of Single and Multimodal Approaches." *Archives of Computational Methods in Engineering* 33, no. 1 (July 26, 2025): 613–43. https://doi.org/10.1007/s11831-025-10317-5.

[87] Rollins, Zachary A., Alan C. Cheng, and Essam Metwally. "MolPROP: Molecular Property Prediction with Multimodal Language and Graph Fusion." *Journal of Cheminformatics* 16, no. 1 (May 22, 2024). https://doi.org/10.1186/s13321-024-00846-9.

[88] Marimuthu, Aravindh Nivas, and Brett A. McGuire. "Machine Learning Pipeline for Molecular Property Prediction Using ChemXploreML." *Journal of Chemical Information and Modeling* 65, no. 11 (May 20, 2025): 5424–37. https://doi.org/10.1021/acs.jcim.5c00516.

[89] Thameem, Muhammed, Obaid AlHmoudi, Ahmad Al Salloum, Naeema Al Darmaki, Ali Elkamel, and Ali A. AlHammadi. "Molecular Property Prediction: Input Types and Information Processing in Machine Learning Models." *Results in Engineering* 29 (March 2026): 109241. https://doi.org/10.1016/j.rineng.2026.109241.

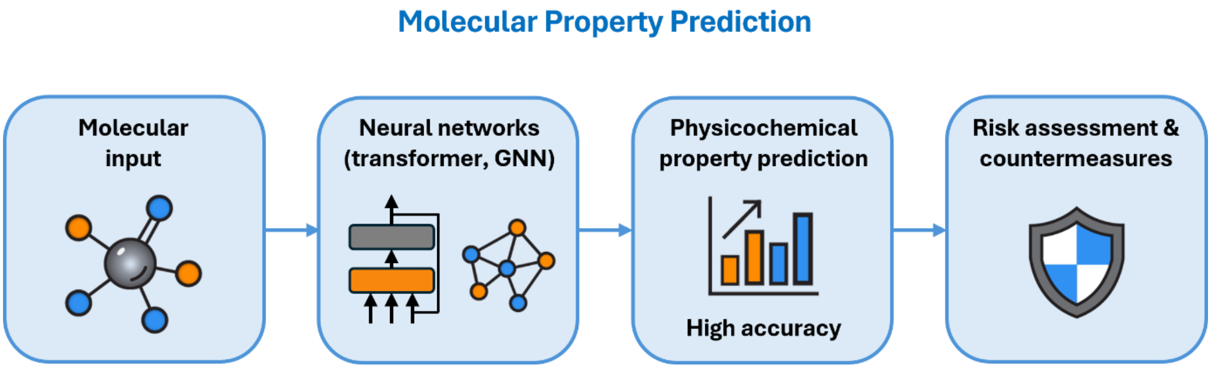

Molecular Property Prediction
Molecular input
Neural networks (transformer, GNN)
Physicochemical property prediction
High accuracy
Risk assessment & countermeasures

Figure 11: AI-driven molecular property prediction

171. Vapour pressure is a key physicochemical property that influences a substance's volatility, environmental persistence, and potential routes of exposure, making its accurate prediction essential for chemical safety and risk assessment when considering toxic chemicals.[90] AI models trained on thermodynamic databases can predict vapour pressure with accuracies approaching experimental measurements, while ML approaches that leverage molecular structure features enable estimation even for compounds lacking experimental data. In operational contexts, these predictions are especially important for informing inhalation hazard evaluations, guiding environmental monitoring strategies, and determining detection and protective equipment requirements.

172. In addition to vapour pressure prediction, toxicity prediction is also crucial for chemical safety assessment. Deep learning models can now be used to predict acute toxicity (LD_{50} and LC_{50} values), chronic toxicity, carcinogenicity, mutagenicity, and organ-specific toxicological effects across multiple species with accuracies that often exceed the reproducibility of traditional animal testing. For example, data fusion read-across structure activity relationship models achieved an average of 87% balanced accuracy across nine toxicity tests for 190,000 chemicals, outperforming the average 81% reproducibility of animal tests themselves.[91] These AI-driven toxicity predictions enable rapid safety screening of novel compounds, identification of potential CWAs based on structural similarity to known toxic substances, and assessment of environmental hazards without extensive animal testing. For chemical security applications, AI toxicity models can predict the lethality and physiological

[90] Hyun Nam, Ji, Seul Lee, Seongil Jo, Jaeoh Kim, Jooyeon Lee, Jahyun Koo, Byounghwak Lee, Keunhong Jeong, and Donghyeon Yu. "Improving Vapor Pressure Prediction through Integration of Multiple Molecular Representations: A Super Learner Approach." *Journal of Chemometrics* 39, no. 2 (February 10, 2025): 1–19. https://doi.org/10.1002/cem.70003.

[91] Luechtefeld, Thomas, Dan Marsh, Craig Rowlands, and Thomas Hartung. "Machine Learning of Toxicological Big Data Enables Read-across Structure Activity Relationships (RASAR) Outperforming Animal Test Reproducibility." *Toxicological Sciences* 165, no. 1 (July 11, 2018): 198–212. https://doi.org/10.1093/toxsci/kfy152.

effects of hypothetical compounds, allowing proactive identification of potential threats before they are synthesised.[92]

173. The utility of AI-driven property prediction extends beyond research applications into practical chemical management and safety systems. Automated generation of safety data sheets will become increasingly feasible as AI models reliably predict hazard classifications, handling precautions, and emergency response measures based solely on molecular structure or limited experimental data. Regulatory agencies can leverage these tools for faster chemical registration processes, pre-market safety assessments, and prioritisation of substances requiring detailed experimental evaluation.

Spectral prediction

174. Complementing molecular property prediction, AI is increasingly being applied to the prediction and generation of spectra, a capability that is relevant for verification activities.[93] Spectral information provides the primary means by which chemicals are detected and characterised using analytical techniques such as mass spectrometry (MS), gas chromatography-mass spectrometry (GC-MS), infrared (IR) spectroscopy, and nuclear magnetic resonance (NMR) spectroscopy.

175. In this context, forward and inverse modelling are complementary approaches employed to relate chemical structure and spectra. They are often used together and can be particularly valuable in complex or data-limited environments. Forward modelling (structure-to-spectrum approach) involves predicting spectra from a known molecular structure, and is commonly used to simulate expected measurements or generate reference data (see Figure 12). AI models such as graph neural networks (GNNs) can predict spectra from a compound's molecular structure orders of magnitude faster than traditional methods, such as density functional theory. Numerous tools, like RT Pred, FraGNNet, and Caspre, have been developed

[92] Jeong, Keunhong, Jin-Young Lee, Seungmin Woo, Dongwoo Kim, Yonggoon Jeon, Tae In Ryu, Seung-Ryul Hwang, and Woo-Hyeon Jeong. "Vapor Pressure and Toxicity Prediction for Novichok Agent Candidates Using Machine Learning Model: Preparation for Unascertained Nerve Agents after Chemical Weapons Convention Schedule 1 Update." *Chemical Research in Toxicology* 35, no. 5 (March 23, 2022): 774–81. https://doi.org/10.1021/acs.chemrestox.1c00410.

[93] Feng, Shuo, Meng Huang, Yanbo Li, Aoran Cai, Xiaoyu Yue, Song Wang, Linjiang Chen, Jun Jiang, and Yi Luo. "Intelligent Understanding of Spectra: From Structural Elucidation to Property Design." *Chemical Society Reviews* 54, no. 18 (August 20, 2025): 8243–86. https://doi.org/10.1039/d4cs01293c.

for predicting retention times and spectral data,[94,95,96] with growing accuracy, while increasingly able to accommodate complexity and nuance.

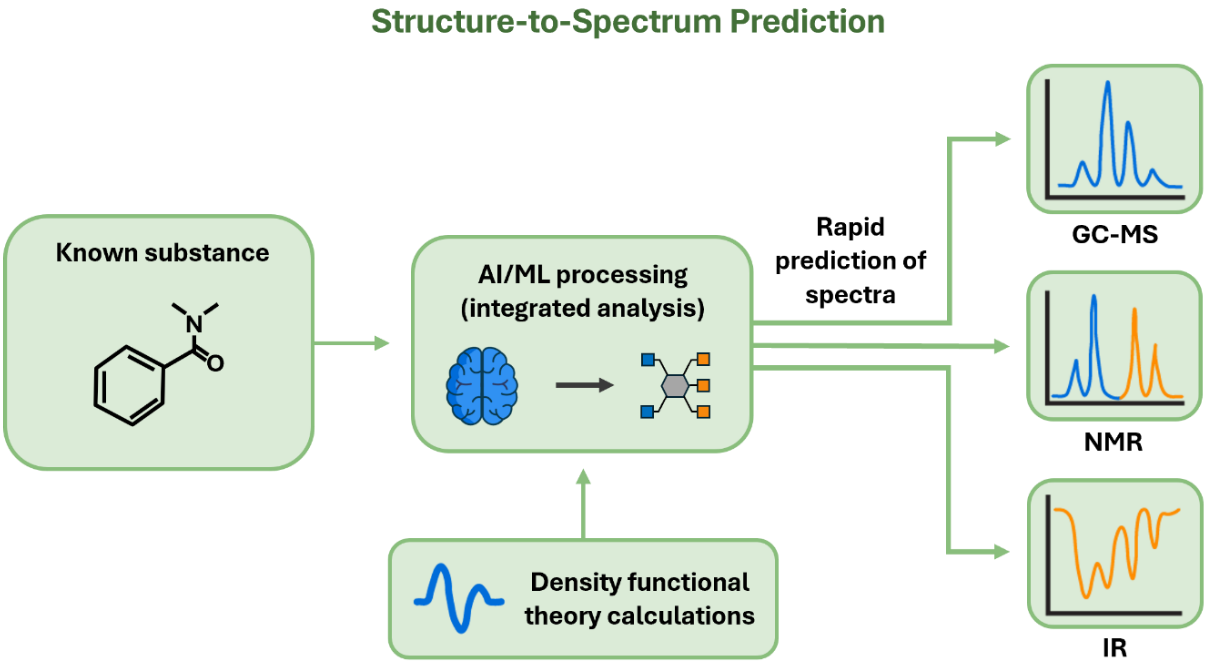

Structure-to-Spectrum Prediction
Known substance
N
O
AI/ML processing (integrated analysis)
Rapid prediction of spectra
Density functional theory calculations
GC-MS
NMR
IR

Figure 12: Forward modelling in spectral prediction

176. Vibrational spectroscopy, encompassing Raman and IR, provides a molecular "fingerprint" based on the vibrational modes of chemical bonds. However, these techniques face significant challenges in the field. For example, Raman signals are notoriously weak and often overwhelmed by fluorescence from organic matter or substrates, resulting in a low signal-to-noise ratio.[97] Vibrational spectroscopy is therefore benefitting from AI-driven predictive capabilities. Neural networks trained

[94] Zakir, Mahi, Marcia A. LeVatte, and David S. Wishart. "RT-Pred: A Web Server for Accurate, Customized Liquid Chromatography Retention Time Prediction of Chemicals." *Journal of Chromatography A* 1747 (April 26, 2025): 465816. https://doi.org/10.1016/j.chroma.2025.465816.

[95] Young, Adamo, Fei Wang, David S Wishart, Bo Wang, Russell Greiner, and Hannes Röst. "FraGNNet: A Deep Probabilistic Model for Tandem Mass Spectrum Prediction." *Transactions on Machine Learning Research*, August 27, 2025. https://doi.org/10.48550/arXiv.2404.02360.

[96] Sajed, Tanvir, Zinat Sayeeda, Brian L. Lee, Mark Berjanskii, Fei Wang, Vasuk Gautam, and David S. Wishart. "Accurate Prediction of ^{1}H NMR Chemical Shifts of Small Molecules Using Machine Learning." *Metabolites* 14, no. 5 (May 19, 2024): 290. https://doi.org/10.3390/metabo14050290.

[97] Luo, Ruihao, Juergen Popp, and Thomas Bocklitz. "Deep Learning for Raman Spectroscopy: A Review." *Analytica* 3, no. 3 (July 19, 2022): 287–301. https://doi.org/10.3390/analytica3030020.

on extensive vibrational spectroscopy databases can predict IR absorption bands and Raman scattering intensities from molecular structures, capturing the complex relationships between chemical bonds, molecular geometry, and spectroscopic signatures.[98,99] These AI models can account for factors such as intramolecular hydrogen bonding, conformational flexibility, and environmental effects that traditional rule-based approaches struggle to capture. The ability to generate predicted IR and Raman spectra enables rapid pre-screening of candidate structures during unknown compound identification, assessment of spectral interferences in complex mixtures, and optimisation of detection methods for specific target analytes. Advanced models can also predict how spectra change under different conditions—such as temperature, solvent, and pressure—providing deeper insights into molecular behaviour and improving field detection reliability.

177. Despite being one of the most information-rich analytical techniques, NMR spectroscopy has traditionally required expert interpretation due to the complexity of chemical shift patterns, coupling constants, and conformational effects. AI has revolutionised NMR prediction through deep learning models that learn directly from molecular structures to predict proton (^{1}H) NMR, carbon-13 (^{13}C) NMR, and even two-dimensional NMR spectra with remarkable accuracy.[100,101] Graph neural networks that explicitly model molecular connectivity and stereochemistry have achieved near-experimental accuracy for many compound classes. These AI-powered NMR predictions accelerate structure elucidation by narrowing down candidate structures, verifying synthetic products without extensive spectroscopic analysis, and enabling

[98] Ren, Hao, Hao Li, Qian Zhang, Lijun Liang, Wenyue Guo, Fang Huang, Yi Luo, and Jun Jiang. "A Machine Learning Vibrational Spectroscopy Protocol for Spectrum Prediction and Spectrum-Based Structure Recognition." *Fundamental Research* 1, no. 4 (July 2021): 488–94. https://doi.org/10.1016/j.fmre.2021.05.005.

[99] Sorrentino, Salvatore, Alessandro Gussoni, Francesco Calcagno, Gioele Pasotti, Davide Avagliano, Ivan Rivalta, Marco Garavelli, and Dario Polli. "Mol2Raman: A Graph Neural Network Model for Predicting Raman Spectra from SMILES Representations." *Digital Discovery* 5, no. 1 (November 25, 2025): 161–76. https://doi.org/10.1039/d5dd00210a.

[100] Jeong, Keunhong, Tae In Ryu, Seung-Ryul Hwang, Yoonjae Cho, Kyoung Chan Lim, Ung Hwi Yoon, Jin-Young Lee, Young Wook Yoon, and Hey Jin Jeong. "Precisely Predicting the ^{1}H and ^{13}C NMR Chemical Shifts in New Types of Nerve Agents and Building Spectra Database." *Scientific Reports* 12, no. 1 (November 24, 2022). https://doi.org/10.1038/s41598-022-24647-y.

[101] Li, Yunrui, Hao Xu, Ambrish Kumar, Duo-Sheng Wang, Christian Heiss, Parastoo Azadi, and Pengyu Hong. "TransPeakNet for Solvent-Aware 2D NMR Prediction via Multi-Task Pre-Training and Unsupervised Learning." *Communications Chemistry* 8, no. 1 (February 20, 2025). https://doi.org/10.1038/s42004-025-01455-9.

automated spectral interpretation that was previously possible only through expert human analysis.

178. Chemical space is vast, and reference libraries for analytical techniques contain only a fraction of existing molecules. When a spectrum does not match a library entry, traditional analysis hits a dead end.[102] In these instances, forward modelling can be invaluable. It can be leveraged to generate *in silico* libraries comprising millions of molecules that have never been physically synthesised or analysed, thereby significantly augmenting experimental libraries. This generative capability is transformative for chemical identification, enabling the experimental spectrum of an unknown substance to be compared not only against existing libraries but also against AI-predicted spectra, dramatically expanding identification coverage.[101]

179. Mass spectrometry, particularly tandem mass spectrometry (MS/MS), is the gold standard for identifying small molecules and metabolites. As this field faces a significant "library problem", MS spectral prediction is helping address the longstanding challenge of interpreting complex fragmentation patterns, with bespoke AI models shifting MS analysis from matching to prediction. Furthermore, deep learning models trained on large spectral databases can now predict electron ionisation, electrospray ionisation, and MS/MS fragmentation patterns directly from molecular structures.[103]

180. Inverse modelling (spectrum-to-structure approach) works in the opposite direction to forward modelling, seeking to infer the most likely chemical structures from a measured spectrum or combined spectra (see Figure 13). This can now be achieved with high accuracy, reducing the need for manual, expert interpretation of spectra. Models like MassGenie use transformer-based deep learning to predict the molecular structure directly from an MS/MS spectrum.[104] By learning the fragmentation rules of

[102] Nguyen, Julia, Richard Overstreet, Ethan King, and Danielle Ciesielski. "Advancing the Prediction of MS/MS Spectra Using Machine Learning." *Journal of the American Society for Mass Spectrometry* 35, no. 10 (September 11, 2024): 2256–66. https://doi.org/10.1021/jasms.4c00154.

[103] Jeong, Keunhong, Youngjoon Jeon, Sein Min, Tae In Ryu, Young Wook Yoon, Yoonjae Cho, Seung-Ryul Hwang, Hye Jin Jeong, and Sung Soo Kim. "Density Functional Theory–Spectroscopy Integrated Identification Method Encompassing Experimental and Theoretical Analyses for Designer Drug Stimulants." *Advanced Intelligent Systems* 7, no. 10 (March 14, 2025). https://doi.org/10.1002/aisy.202500111.

[104] Shrivastava, Aditya Divyakant, Neil Swainston, Soumitra Samanta, Ivayla Roberts, Marina Wright Muelas, and Douglas B. Kell. "MassGenie: A Transformer-Based Deep Learning Method for Identifying Small Molecules from Their Mass Spectra." *Biomolecules* 11, no. 12 (November 30, 2021): 1793. https://doi.org/10.3390/biom11121793.

molecules (how they break apart under energy), the AI model can propose structures for “unknown” spectra, effectively performing *de novo* identification.

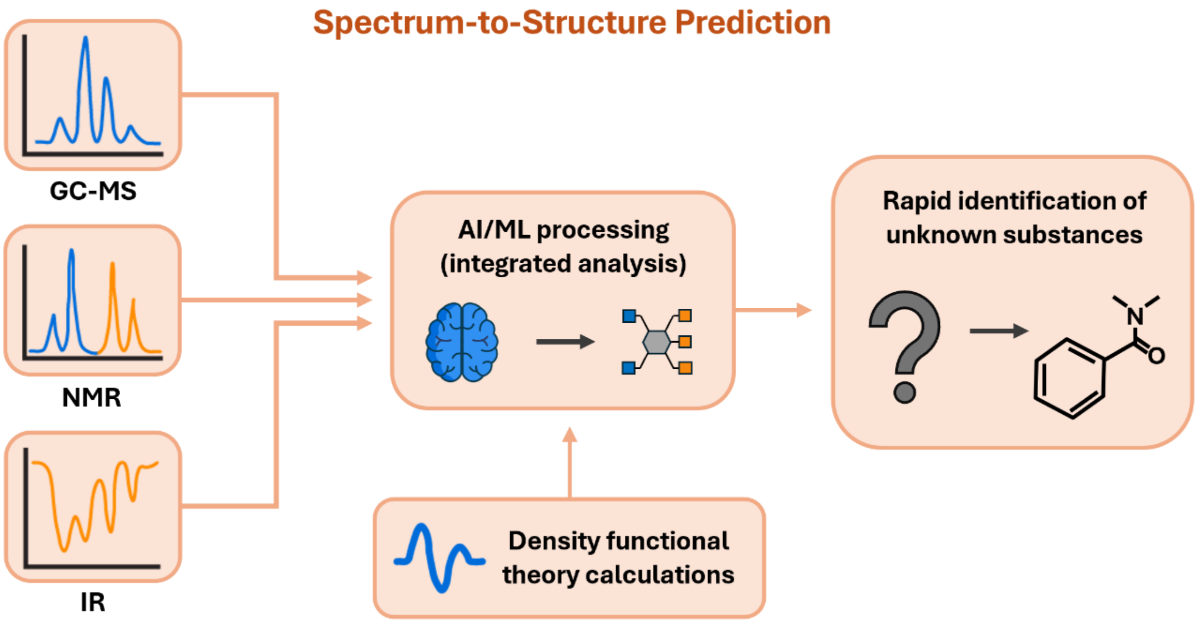

Spectrum-to-Structure Prediction
GC-MS
NMR
IR
AI/ML processing (integrated analysis)
Density functional theory calculations
Rapid identification of unknown substances
?
N
O

Figure 13: Inverse modelling in substance identification

AI in data/sensor fusion

181. Traditional manual interpretation of spectral data is resource-intensive, and the interpretation of complex datasets presents even greater challenges. Data streams from modern analytical instruments and sensors are growing exponentially, with velocity, volume, and variety exceeding the cognitive bandwidth of human analysts and the capabilities of classical chemometric algorithms.

182. AI is fundamentally transforming chemical data fusion by enabling the integration and interpretation of heterogeneous datasets that were previously analysed in isolation. Generic ML models, such as off-the-shelf image classifiers, are ill-suited for the specific nuances of chemical spectral data, requiring bespoke models that account for instrument-specific noise, matrix effects, and overlapping signals to achieve high-fidelity detection. Deep learning architectures—such as convolutional neural networks for spatial data, recurrent neural networks for temporal sequences, and transformer models for attention-based integration—can automatically learn complex patterns, identify subtle correlations invisible to human analysts, and provide probabilistic assessments of uncertain or incomplete information. These capabilities enable AI systems to fuse information from disparate sources including analytical instruments, ground-based sensors, and environmental monitoring stations, creating situational awareness that exceeds the sum of individual data streams.

183. While bespoke AI models enhance the performance of individual sensors, the most robust defence against false alarms and ambiguity is the integration of multiple, distinct sensing modalities. Multi-sensor fusion is the algorithmic combination of data from independent sensors to create a composite result that is more accurate and reliable than any single sensor could achieve.

184. The core justification for sensor fusion in chemical defence is "orthogonality". Orthogonal sensors measure fundamentally different physical or chemical properties of a substance. When sensors are orthogonal, their failure modes are uncorrelated; a substance that triggers a false positive on sensor A is highly unlikely to trigger a false positive on sensor B.[105]

185. Data fusion can be conducted at different levels. Low-level fusion combines raw signals before any feature extraction occurs. This is computationally intensive but preserves the maximum amount of information. For example, Raman and Fourier-transform infrared (FTIR) spectral data can be combined into a single "super-spectrum". Research on lung cancer detection utilised this approach, concatenating the spectral vectors of Raman and FTIR data. The fused model achieved significantly higher classification accuracy (identifying biomarkers) than either technique alone.[106] The FTIR data provide information on functional groups, while Raman data provide complementary information on the carbon backbone, creating a complete molecular picture.[107]

186. Mid-level (feature-level) fusion extracts features—such as peak locations or specific spectral bands—from each sensor individually and then concatenates these vectors for AI classification. This is exemplified in "electronic noses" (e-noses), where non-specific gas sensor arrays generate patterns. Extracting features from the transient response (the rise time and decay time of the sensor signal) and fusing them allows

[105] Wang, Peng, Zhaoyan Fan, David O. Kazmer, and Robert X. Gao. "Orthogonal Analysis of Multisensor Data Fusion for Improved Quality Control." *Journal of Manufacturing Science and Engineering* 139, no. 10 (August 24, 2017). https://doi.org/10.1115/1.4036907.

[106] Hano, Harun, Beatriz Suarez, Charles H. Lawrie, and Andreas Seifert. "Fusion of Raman and FTIR Spectroscopy Data Uncovers Physiological Changes Associated with Lung Cancer." *International Journal of Molecular Sciences* 25, no. 20 (October 11, 2024): 10936. https://doi.org/10.3390/ijms252010936.

[107] Yang, Xien, Zhongyu Wu, Quanhong Ou, Kai Qian, Liqin Jiang, Weiye Yang, Youming Shi, and Gang Liu. "Diagnosis of Lung Cancer by FTIR Spectroscopy Combined with Raman Spectroscopy Based on Data Fusion and Wavelet Transform." *Frontiers in Chemistry* 10 (January 26, 2022). https://doi.org/10.3389/fchem.2022.810837.

the system to identify odours based on the kinetic interaction of the gas with the sensor, not just the steady-state response.[108]

187. High-level (decision-level) fusion combines the independent sensor classifications (for example “agent present” or “safe”), and a fusion algorithm (such as a Bayesian network or weighted voting) makes the final determination. The VipIR chemical analyser uses a form of decision fusion called smart spectral processing: FTIR results constrain Raman searches, and vice versa.[109] For example, if the FTIR identifies a chlorinated compound, the Raman algorithm restricts its search space to chlorinated compounds, drastically reducing the probability of a mismatch.

188. The mathematical engines behind fusion are evolving from simple logic gates to probabilistic AI. Bayesian inference can update the probability of a hypothesis (for example “chemical attack”) as more evidence becomes available. It is particularly effective for fusing data from sensors with known error rates. In the EU-SENSE project (European Sensor System for CBRN Applications) of the European Union, Bayesian networks were used to fuse data from stationary and mobile sensors, providing a probabilistic estimate of the threat level.[110]

189. Multi-modal neural networks can learn to fuse dissimilar data types, such as thermal imagery and gas sensor data. In fire detection systems, a one-dimensional convolutional neural network processes the gas signals while a two-dimensional convolutional neural network processes the thermal images; their outputs are merged in a fully connected layer. This fusion achieved perfect classification of fire types in tests, distinguishing between real smoke and nuisance aerosols (e-cigarettes).[111]

190. Context-aware fusion incorporates environmental data—such as wind speed, humidity, and temperature—into the fusion model. This is critical because chemical sensors respond differently under varying conditions. A fusion algorithm can learn to “trust” the electrochemical sensor less in low humidity and “trust” the

[108] Yan, Jia, Ruihong Sun, Tao Liu, and Shukai Duan. “Domain-Adaptation-Based Active Ensemble Learning for Improving Chemical Sensor Array Performance.” *Sensors and Actuators A: Physical* 357 (August 2023): 114411. https://doi.org/10.1016/j.sna.2023.114411.

[109] “Combining Raman and FTIR Spectroscopy into One Analytical Method.” Southern Scientific, November 27, 2025.

[110] Norbert, Kopp, and Koch-Eschweiler Helge. “Improved Detection of Chemical Threats by Sensor Data Fusion.” *Security and Defence Quarterly* 37 (March 8, 2022): 70–93. https://doi.org/10.35467/sdq/144296.

[111] Milli, Musa, and Mehmet Milli. “Reducing False Positives in Building Fire Detection Systems via Multiple Metal Oxide Sensors.” *IEEE Access* 13 (September 5, 2025): 157537–50. https://doi.org/10.1109/access.2025.3606584.

photoionisation detector more, dynamically adjusting the weight of each sensor based on the environment.[111]

191. In the field of spectral analysis, ML techniques have improved the interpretation of MS, IR, and NMR data, among others. New approaches can analyse multi-modal spectroscopic data simultaneously, significantly reducing analysis time while improving identification accuracy. Notably, recent integrated identification methods combining experimental GC-MS, NMR, and IR data with density functional theory calculations have proven effective in identifying unknown terrorist chemical mixtures and designer drug stimulants.[103,112] AI-enhanced spectroscopy can now rapidly identify contaminants in drug formulations and detect trace pollutants in complex environmental mixtures.[113]

Potential for misuse

192. While AI-driven chemical property prediction and spectral analysis tools offer substantial benefits for legitimate research and security applications, they also present significant dual-use risks that could facilitate chemical weapons development. Some of these risks are shown in Figure 14.

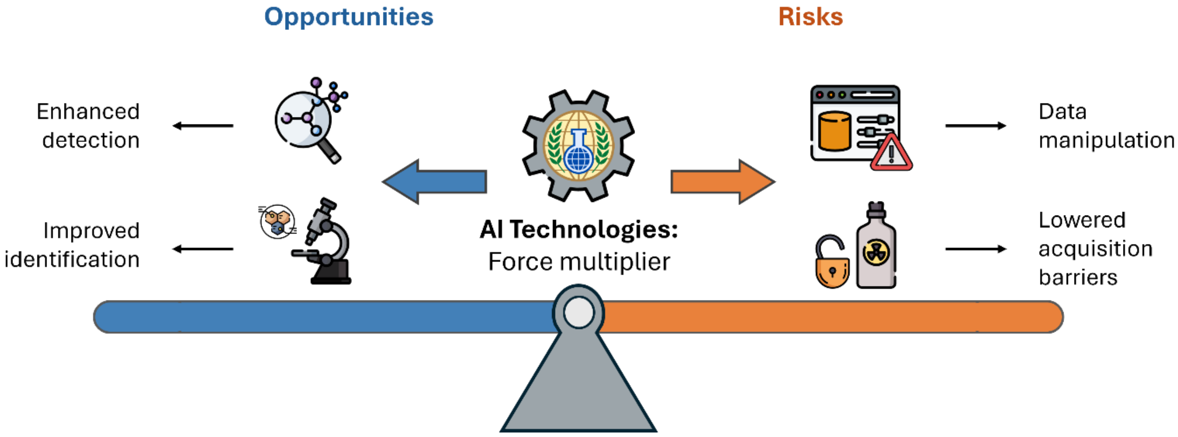


Figure 14: Opportunities and risks posed by chemical prediction using AI tools

[112] Jeong, Keunhong, Honghyun Kim, Sein Min, Young Wook Yoon, Yoonjae Cho, Choon Hwa Park, Tae In Ryu, Seung-Ryul Hwang, and Sung Keon Namgoong. “DFT–Spectroscopy Integrated Identification Method on Unknown Terrorist Chemical Mixtures by Incorporating Experimental and Theoretical GC-MS, NMR, IR, and DFT-NMR/IR Data.” *Analytical Chemistry* 96, no. 2 (December 28, 2023): 694–700. https://doi.org/10.1021/acs.analchem.3c03647.

[113] Qin, Yiheng, Qiannan Duan, Haoyu Wang, Yonghui Bai, Yihao Qin, Liulu Yao, Fan Song, Mingzhe Wu, and Jianchao Lee. “Advances and Innovations in Machine Learning-Based Spectral Detection Methods for Trace Organic Pollutants.” *The Analyst* 151, no. 2 (December 9, 2025): 356–88. https://doi.org/10.1039/d5an00903k.

193. The same AI models that enable rapid toxicity screening for pharmaceutical safety can, in principle, be repurposed to systematically identify harmful chemicals.[35] Publicly accessible ML platforms for property prediction may allow malicious actors to computationally screen large numbers of molecular variants to identify compounds with properties conducive to weaponisation—without the need for overt or traceable laboratory experimentation. This accessibility lowers traditional knowledge and resource barriers, making it increasingly feasible for individuals with limited formal chemistry training to exploit these advanced tools to prioritise or identify novel or hypothetical toxic chemicals for further consideration.

Recommendation 14

To enhance preparedness for future chemical weapons threats, the Secretariat should explore the utility of complementary AI-supported tools to systematically understand and map the chemical space surrounding known chemical warfare agents. Such tools could include AI-driven retrosynthesis and synthesis-planning approaches to identify potential novel routes to chemical warfare agents and their precursors, particularly those relying on uncontrolled or non-scheduled chemicals. They could also encompass predictive models for spectral information and other key properties relevant to risk assessment and detection, including toxicity, vapour pressure, stability, and detectability.

194. Data integrity threats pose another dimension of AI-related risk. Machine learning techniques could be used to deliberately craft inputs designed to deceive AI-based detection systems, resulting in false negatives in which hazardous substances go undetected.[114] By exploiting knowledge of model behaviour, sophisticated adversaries could generate "adversarial molecules"—hazardous compounds whose spectra are intentionally designed to be misclassified as benign by AI identification systems.

195. As the Secretariat and States Parties increasingly rely on AI-powered tools, ensuring the integrity, provenance, and security of training data, model parameters, and analytical outputs becomes a critical challenge, requiring enhanced technical safeguards and governance controls. (See Subgroup 2's findings for further discussion on this topic.)

[114] Hartung, Thomas, and Nicole Kleinstreuer. "Challenges and Opportunities for Validation of AI-Based New Approach Methods." *ALTEX* 42, no. 1 (January 14, 2025). https://doi.org/10.14573/altex.2412291.

Opportunities for the OPCW

196. The integration of AI into the CBRN domain could enhance detection, prevention, response, and mitigation capabilities, providing a means to navigate large datasets that would overwhelm human teams.[115] As a force multiplier, AI offers significant opportunities to augment the OPCW's detection and identification capabilities in particular (see Figure 15). AI-enabled molecular property prediction can support the identification of relevant compounds of concern, including the characterisation of novel or previously unknown substances and their associated physicochemical and toxicological properties. Similarly, AI-based spectral prediction and analysis can strengthen detection capabilities for both known and unknown compounds, while also supporting chemical forensics investigations.

197. The fusion of data from multiple sensors and data streams can further enhance the performance, robustness, and reliability of detection and safety platforms. In parallel, AI-driven approaches may contribute to the development of improved medical countermeasures for chemical weapons exposure, mirroring advances already observed across the pharmaceutical sector.

198. Capable of predicting critical properties—such as vapour pressure and toxicity[92] in addition to spectral properties with high accuracy, AI models could be used to expand detection libraries and develop protection protocols pre-emptively. This will ensure that the Secretariat and States Parties are equipped to identify and respond to novel agents immediately upon their emergence, rather than waiting for a confirmed-use event to characterise the threat.

199. AI tools could be used to deepen the Organisation’s understanding of chemicals relevant to the Convention. This is particularly pertinent for the four new entries added to Schedule 1 of the Annex on Chemicals to the Convention in 2020. For these substances—organophosphorus and carbamate-based nerve agents—there remains a paucity of information available in the public domain.[116] This lack of data presents a challenge for the OPCW, which relies heavily on detailed knowledge of physicochemical properties to inform decisions such as the selection of appropriate protection or detection equipment.

[115] *Department of Homeland Security Report on Reducing the Risks at the Intersection of Artificial Intelligence and Chemical, Biological, Radiological, and Nuclear Threats.* Department of Homeland Security, April 26, 2024.

[116] Hotchkiss, Peter J. “The World’s Chemical-Weapons Stockpiles Are Gone — but a New Challenge Looms.” *Nature* 623, no. 7987 (November 14, 2023): 459–459. https://doi.org/10.1038/d41586-023-03509-1.

200. By leveraging AI, it could be possible to predict the properties of these poorly characterised chemicals and to assess their similarities to, and differences from, well-studied compounds. Such assessments could provide an initial indication of whether existing protocols remain adequate or whether modifications may be required. In addition, these predictive capabilities could support horizon scanning by identifying other chemicals with relevant properties that may warrant consideration in future amendments to the Annex on Chemicals.

201. Current chemical detection infrastructure is heavily reliant on library matching and manual interpretation: a sensor detects a signal, and software compares it against a pre-existing database of known signatures. This approach works very well in certain situations, such as for known industrial chemicals in controlled environments, but faces additional uncertainties in more challenging scenarios, such as that of novel threats or complex mixtures.

202. AI-driven approaches, specifically those utilising deep learning and ML, can augment detection and identification capabilities in these challenging scenarios. For example, this means that novel agents or precursors can potentially be identified even if they have no prior experimental reference spectra, by matching observed fragmentation patterns against predictions for suspected structures. AI models can rapidly generate predicted spectra for potential CWAs, their precursors, degradation products, and structural analogues, creating comprehensive reference libraries that support identification even when standard reference materials are unavailable.[112]

203. In forensic investigations of illicit drug laboratories or improvised chemical devices, AI-predicted spectra help identify novel synthetic routes, unusual precursors, and designer variants that evade traditional detection. AI spectral prediction tools provide critical capabilities for threat identification and verification. When investigating suspected use of chemical weapons, field samples often contain complex mixtures of degradation products, environmental contaminants, and unknown substances, the analysis of which is complex, but can be aided with different AI tools.

204. Combining different data streams, whether from analytical instrumentation or from totally different areas can prove very useful in detection and monitoring. The integration of multiple spectroscopic techniques—combining AI-predicted MS, IR, Raman, and NMR data—provides orthogonal confirmation of molecular identity with high confidence, enabling definitive identification of trace-level contaminants in complex matrices. This multi-modal AI-enhanced approach represents the future of chemical detection, where predicted spectral databases expand coverage from thousands of known compounds to millions of hypothetical structures, ensuring that detection and identification capabilities keep pace with the evolving chemical threat landscape. Furthermore, data fusion approaches utilising remote monitoring systems (such as sensors deployed on uncrewed platforms) can enhance inspector safety.

Validated pattern recognition models can enable real-time hazard assessment at a standoff distance, ensuring that automated systems can reliably distinguish between the presence of toxic or benign chemicals in the field, allowing mission teams to adapt accordingly to a given scenario.

205. Predictive models are increasingly being used in the development of medicines, where rapid, simulation-driven *in silico* methods are beginning to replace slow, laboratory-based trial-and-error approaches. AI is now enhancing multiple stages of pharmaceutical research and development, from target identification and validation, through *de novo* molecule design, to property and parameter optimisation. This enables vastly larger numbers of candidate molecules to be explored and screened computationally before any synthesis is required, allowing researchers to focus experimental efforts on the most promising compounds.

206. Traditionally, the development of a new drug from initial discovery to market approval can take 10 to 15 years and incur substantial costs, with much of this time spent identifying viable candidates. AI-driven approaches are significantly compressing the early stages of this pipeline, with some taking as little as two to three years, alongside marked cost savings. There are now multiple AI-designed drug candidates that have progressed to Phase II clinical trials, and AI has also demonstrated value in drug repurposing.[117,118] During the COVID-19 pandemic, for example, BenevolentAI identified baricitinib as a potential therapeutic candidate within 48 hours by analysing existing biomedical data.[119]

207. These developments highlight the potential for AI-enabled drug discovery methods to be applied to the development of new medical countermeasures for chemical weapons exposure—an area in which progress has historically been slow. By enabling *in silico* design, screening, and optimisation of candidate therapeutics, AI has the potential to substantially accelerate the identification of effective medical

[117] Xu, Zuojun, Feng Ren, Ping Wang, Jie Cao, Chunting Tan, Dedong Ma, Li Zhao, et al. "A Generative AI-Discovered TNIK Inhibitor for Idiopathic Pulmonary Fibrosis: A Randomized Phase 2a Trial." *Nature Medicine* 31, no. 8 (June 3, 2025): 2602–10. https://doi.org/10.1038/s41591-025-03743-2.

[118] "Efficacy and Safety of REC-2282 in Patients With Progressive Neurofibromatosis Type 2 (NF2) Mutated Meningiomas (POPLAR-NF2)." ClinicalTrials – National Library of Medicine, October 10, 2025.

[119] Richardson, Peter J., Bruce W. Robinson, Daniel P. Smith, and Justin Stebbing. "The AI-Assisted Identification and Clinical Efficacy of Baricitinib in the Treatment of COVID-19." *Vaccines* 10, no. 6 (June 15, 2022): 951. https://doi.org/10.3390/vaccines10060951.

countermeasures and reduce development timelines, improving preparedness and response capabilities.[120]

208. To ensure the scientific rigour and legal defensibility of these new tools and approaches, implementation must be grounded in established expertise. Baseline data must be accurate and defendable. The recent OPCW AI Research Challenge will provide a wealth of information relevant to compound, spectral, and property prediction, as well as application of AI methods to chemical forensics workstreams, representing a first step in understanding the veracity and utility of *in silico* generated data and spectra. In addition, discussions and workshops with the OPCW Designated Laboratories and other research entities will be essential to validate these bespoke models against reference standards and existing protocols and best practices. Any AI-augmented workflow must meet strict performance criteria required for OPCW verification activities.

Recommendation 9

The Secretariat should evaluate existing—and, where necessary, develop—AI models to augment chemical detection and identification capabilities. These bespoke models should support the analysis of spectral data, evaluate the utility of multi-sensor fusion for chemical identification, and validate the performance of AI-driven pattern recognition in remote monitoring systems (such as sensors deployed on uncrewed platforms). Outcomes from the OPCW AI Research Challenge may provide useful inputs in this regard. Workshops with OPCW Designated Laboratories could further help identify promising AI models suitable for integration into analytical chemistry workstreams.

[120] "The Age of AI in the Life Sciences." *National Academies Press*, April 23, 2025. https://doi.org/10.17226/28868.

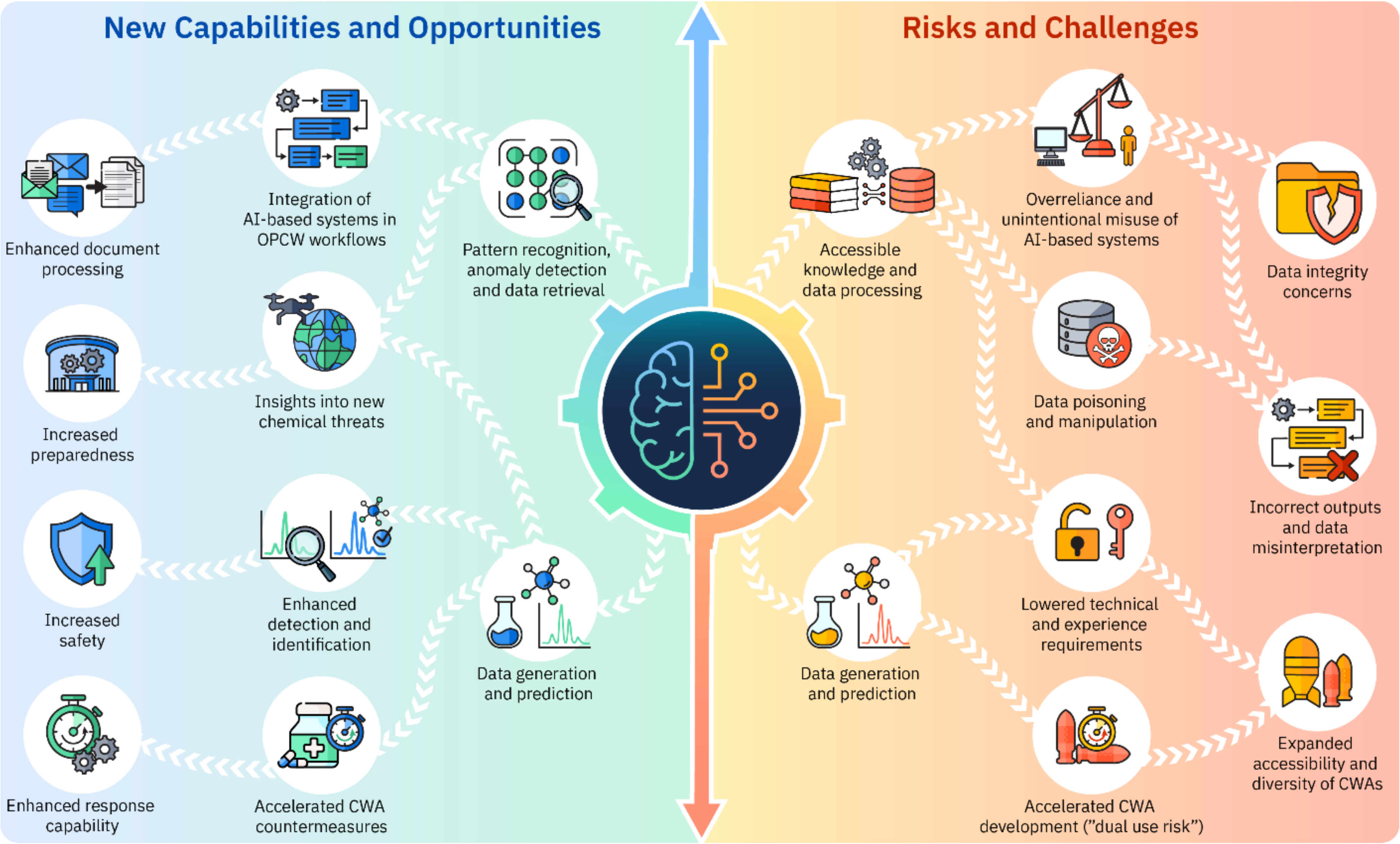

New Capabilities and Opportunities
Enhanced document processing
Integration of AI-based systems in OPCW workflows
Pattern recognition, anomaly detection and data retrieval
Increased preparedness
Insights into new chemical threats
Increased safety
Enhanced detection and identification
Data generation and prediction
Enhanced response capability
Accelerated CWA countermeasures
Risks and Challenges
Accessible knowledge and data processing
Overreliance and unintentional misuse of AI-based systems
Data integrity concerns
Data poisoning and manipulation
Incorrect outputs and data misinterpretation
Lowered technical and experience requirements
Data generation and prediction
Expanded accessibility and diversity of CWAs
Accelerated CWA development ("dual use risk")

Figure 15: New capabilities, opportunities, and risks associated with enhanced data prediction and generation, alongside increased access

SUBGROUP 4: SIMULATION AND TRAINING

209. By nature, many traditional training and simulation tools are static, relying on pre-defined scenarios, fixed scripts, and limited branching paths. However, the integration of AI is transforming their capabilities, enabling more realistic, adaptive,[121] and scalable environments. AI-enhanced systems can generate highly immersive settings, making them invaluable for simulating hazardous or complex situations where real-world testing is difficult or unsafe.

210. This dynamism supports personalised learning by adapting scenarios in real time based on performance and evolving user needs, adjusting difficulty and content to ensure effective progression. AI also enables real-time comprehensive feedback and assessment, significantly reducing the delay between training and evaluation, and can be used to predict future performance through data-driven analytics.

211. During the mandate of the TWG, Subgroup 4 devoted its efforts to exploring AI-supported simulation and training tools. The subgroup focused on identifying existing state-of-the-art technologies in this area, while considering potential future applications and addressing gaps, specifically within the context of meeting OPCW training needs.

AI in training tools

212. AI is being increasingly integrated into traditional training tools, such as XR platforms,[122,123] digital twins,[124] and simulations. For example, advanced AI models can now simulate chemical dispersion and reaction pathways in real-time, offering a

[121] Kabudi, Tumaini, Ilias Pappas, and Dag Håkon Olsen. "AI-Enabled Adaptive Learning Systems: A Systematic Mapping of the Literature." *Computers and Education: Artificial Intelligence* 2 (2021): 100017. https://doi.org/10.1016/j.caeai.2021.100017.

[122] Ning, Xinyu, Yan Zhuo, Xian Wang, Chan-In Devin Sio, and Lik-Hang Lee. "When Generative Artificial Intelligence Meets Extended Reality: A Systematic Review." *International Journal of Human–Computer Interaction*, September 30, 2025, 1–21. https://doi.org/10.1080/10447318.2025.2565392.

[123] Fernández-Arias, Pablo, Antonio del Bosque, Georgios Lampropoulos, and Diego Vergara. "Applications of AI and VR in High-Risk Training Simulations: A Bibliometric Review." *Applied Sciences* 15, no. 10 (May 2025): 5424. https://doi.org/10.3390/app15105424.

[124] Kreuzer, Tim, Panagiotis Papapetrou, and Jelena Zdravkovic. "Artificial Intelligence in Digital Twins—A Systematic Literature Review." *Data & Knowledge Engineering* 151 (May 2024): 102304. https://doi.org/10.1016/j.datak.2024.102304.

superior alternative to static emergency planning.[125] These tools could be used to enhance the emergency response capacity of States Parties, allowing first responders to "wargame" hazardous scenarios and optimise resource allocation before an incident occurs.

213. AI can also enhance the design and delivery of chemical-related tabletop exercises. A growing number of commercial tools and providers are incorporating AI either to enrich the tabletop exercise experience itself or to support the development of more complex and dynamic scenarios.[126] In addition, AI can be used to integrate emerging features into exercises, such as simulated social media environments, enabling trainees to respond in real time to the rapid spread of misinformation and disinformation and to practise timely clarification and communication strategies.

214. The emergence of multimodal foundation models also has the potential to enhance AI supported training tools. By processing and integrating multiple forms of data simultaneously—including text, speech, images, video, and sensor inputs—these models can enable more sophisticated scenario generation, richer contextual understanding of trainee behaviour, and more realistic interaction with both virtual agents and autonomous systems. These models could also be applied to train embodied intelligence, including robots, drones, and other uncrewed or autonomous vehicles, preparing them to operate safely and effectively in complex CBRN environments.

Recommendation 12

The Secretariat should use AI to simulate chemical facilities, production process equipment, and incident scenarios for training relevant staff, including inspectors. Multimodal foundation models should be leveraged to support training for embodied intelligence—including robots, drones, and other uncrewed or autonomous vehicles—enabling realistic and context-aware interactions across multiple data modalities.

AI-enhanced extended reality training tools

215. The primary focus area of Subgroup 4 was the integration of AI in XR platforms. Extended reality is an emerging umbrella term for all immersive technologies, including augmented reality (AR), virtual reality (VR), and mixed reality (MR). Although

[125] Bajwa, Ammar. "AI-Based Emergency Response Systems: A Systematic Literature Review on Smart Infrastructure Safety." *American Journal of Advanced Technology and Engineering Solutions* 1, no. 01 (March 5, 2025): 174–200. https://doi.org/10.63125/xcxwpv34.

[126] "About Opsbook." Opsbook, accessed February 18, 2026.

some argue that VR is not part of XR—because XR is often defined as technologies that extend the real world rather than fully replace it—for clarity and consistency, the term XR is used in this report to include all modalities.

216. Extended reality platforms are rapidly incorporating AI into their core technologies. For example, Apple and Meta are using AI for eye, hand, and voice tracking in their Vision Pro and Quest platforms, respectively. Samsung and Google are partnering to develop a Galaxy XR system with AI embedded into the operating system, enabling a wide range of applications. Table 6 presents examples of current XR platforms and systems.

217. In the CBRN domain, XR training tools are gaining traction and being leveraged to increase knowledge transfer and improve operational preparedness and safety.[127,128,129] They are also being used for military applications, such as in simulating high-threat environments in both urban and rural areas, as well as civilian first-response applications, including handling chemical incidents and providing medical treatment following exposure.[130,131,132]

218. The results of the European Union funded VERTIgO project[133] were presented to the TWG. This project focused on the development of a VR training ecosystem for CBRN military and civilian operators and is currently used by the Italian Joint NBC Defense School. An advanced version of this training tool will also be used in Project 104 of the European Union CBRN Risk Mitigation Centres of Excellence,[134] supporting crime

[127] Altan, Burak, Servet Gürer, Ali Alsamarei, Damla Kıvılcım Demir, H. Şebnem Düzgün, Mustafa Erkayaoğlu, and Elif Surer. "Developing Serious Games for CBRN-e Training in Mixed Reality, Virtual Reality, and Computer-Based Environments." *International Journal of Disaster Risk Reduction* 77 (July 2022): 103022. https://doi.org/10.1016/j.ijdrr.2022.103022.

[128] Dočkalová, Veronika. "JCBRN Defence COE Looks to Extended Reality." JCBRN Defence COE, January 10, 2024.

[129] *Study, Design, Building and Deployment of a CBRN XR Training Platform*. NATO Science and Technology Organization, December 29, 2025.

[130] Sayler, Kelley M. *Military Applications of Extended Reality*. Congressional Research Service, June 17, 2025.

[131] "OneArc." OneArc, accessed February 6, 2026.

[132] "SimX Virtual Reality Medical Simulation." SimX, accessed February 6, 2026.

[133] "VERTIgO: Virtual Enhanced Reality for inTeroperable traIning of CBRN military and civilian Operators." European Union, accessed January 19, 2026.

[134] "Project 104: TRACE ME – sTRengthening crime scene forensics and prosecution cApabilities in investigating Cbrn incidEnts in the Middle East region." European Union, accessed January 19, 2026.

scene investigation training within simulated illegal laboratories. The system includes performance evaluation and can operate in both single- and multi-user modes.

Table 6: Examples of XR platforms

Platform/System	Type	Description
CBRND HoloTrainer	AR	Suite of simulators providing collaborative training on CBRN detection devices, with remote access capability
Magic Leap 2	AR	Tethered headset by Magic Leap with patented optical technology. Suited for medical and industrial applications
HoloLens 2	MR	Headset by Microsoft with high-resolution holographic displays, advanced hand and eye tracking, and spatial audio. Designed for industrial applications
Varjo XR-4	MR	High-resolution headset by Varjo, with a wide field of view and advanced eye-tracking. Designed for professional and industrial applications, the Secure Edition may be used completely offline
HazVR	VR	Hazardous materials training tool by NextGen Interactions, used for training first responders
Meta Quest 3	VR	Low-cost headset by Meta with high-resolution displays, designed primarily for recreational use
SimX Virtual Manikin	VR	Medical training platform by SimX, with customisable CBRN chemical exposure scenarios
VirtHT	VR	Full-body system developed for the Bundeswehr (German armed forces) in collaboration with HGXR. Includes haptic vest and shock belt, 4-dimensional effects, and optional integration with replica weapons for enhanced realism
VIVE Pro Series	VR	High-resolution system by VIVE with a wide field of view and precision room-scale tracking. Designed for professional and enterprise applications
XR1403	XR	Standalone XR training system combining a full-face CBRN protective mask with a VR headset, developed by Fondazione SAFE and Mestel Safety, to support immersive CBRN training

219. The University of Vienna, in cooperation with the non-profit organisation Fondazione SAFE, has developed an AI "add-on" component to XR training by enabling interaction with non-player characters. The introduction of non-player characters can be a significant advantage because they enhance realism by replicating human behaviour and interactions, creating unpredictable scenarios that more closely mirror real life. In this add-on, the characters respond dynamically to the trainee's tone and phrasing—such as providing incorrect answers in response to aggressive questioning—offering a novel approach to interview training in chemical incident investigations.

Advantages, challenges, and limitations

220. AI-enhanced immersive CBRN training tools offer a number of advantages over traditional methods and these are summarised in Table 7.[135] First, they can provide substantial cost savings. Immersive tools enable complex, full-scale exercises involving hazardous substances and specialised equipment to be replaced by, or supplemented with, virtual scenarios. This can significantly reduce costs by minimising consumables, travel expenses, and training-site infrastructure, thereby supporting more frequent training opportunities. Lower resource requirements may also enable smaller training facilities—including those in developing countries where cost constraints are significant—to access advanced training capabilities that would otherwise be difficult to implement.[136] However, any potential cost savings would need to be balanced against the costs associated with maintaining and updating XR systems.

221. Second, immersive training tools can increase operator safety and minimise environmental risk by reducing or eliminating the need for high-hazard training environments, including those involving CWAs. In a virtual setting, trainees can safely rehearse scenarios that would be particularly dangerous in real life, such as large-scale contamination involving a persistent CWA or the inspection of a cache of old chemical weapons.

222. Third, XR systems enable a high level of both scenario repetition and variability. The scenarios of current systems can include both indoor and outdoor environments and can take place during the day or night, under a range of simulated weather conditions

[135] Murtinger, Markus, Emma Jaspaert, Helmut Schrom-Feiertag, and Sebastian Egger-Lampl. "CBRNe Training in Virtual Environments: SWOT Analysis & Practical Guidelines." *International Journal of Safety and Security Engineering* 11, no. 4 (August 31, 2021): 295–303. https://doi.org/10.18280/ijsse.110402.

[136] U.S. Embassy Manila. "U.S., Philippines Inaugurate Training Center for Biological and Chemical Security Threat Response." US Embassy in the Philippines, February 23, 2024.

(depicted in Figure 16). Virtual environments are highly flexible and can be restarted and modified as often as desired and practised until tactics, techniques, procedures, and protocols are executed without error. In contrast, this is only possible to a limited extent in traditional exercises. This flexibility also extends to training location: in principle, XR training can take place anywhere. This supports the implementation of multinational, multi-location exercises, enabling specialists from different countries to meet virtually and practise scenarios collaboratively.

Figure 16: XR scenario versatility and connectivity

223. Fourth, by leveraging ML and neural networks to simulate complex scenarios that mimic human behaviour under stressful conditions, it is possible to test different response strategies and evaluate the effectiveness of various measures. Machine learning and neural networks can also be used to develop decision support systems that can analyse threat scenarios and recommend actions. Such systems can process data in real time, improving decision-making in critical situations.

224. Finally, the extensive evaluation and feedback opportunities provided by AI offer a significant didactic advantage. For example, AI enables the capture and analysis of large quantities of data, including physical indicators such as heart rate, stress levels, movement, and visual focus during the exercise, as well as equipment choice and operational decisions. These indicators—often available in real time—along with

action logs facilitate a comprehensive after-action review and enable the trainer to provide targeted and impactful feedback. Consequently, XR-based training can be far more effective than traditional methods.

Table 7: Summary of advantages, limitations, and challenges of XR-based training

Advantages	Limitations / Challenges
Reduced training costs (less travel, infrastructure, consumables)	Initial investment and ongoing maintenance costs
Safe simulation of hazardous scenarios; reduced environmental risk	Cybersickness risk, especially in VR; user safety considerations
High scenario repetition and variability	Risk of trainees perceiving training as a "game"
Flexible virtual environments (weather, time, indoor/outdoor conditions)	Physical burden (heat, PPE restrictions, equipment weight) difficult to simulate
Remote and multinational collaborative training	Requires instructor training and technical oversight
AI-driven dynamic scenarios and adaptive training	Requires careful scenario design to ensure realism
Real-time data analysis and decision-support capabilities	Lower perceived stress due to absence of real danger
Extensive performance evaluation and targeted feedback	Real-world transfer gap; risk of overconfidence
Personalised learning through analytics	Requires integration into broader training programmes
Increased training frequency and accessibility	Protection of sensitive operational or organisational information
Potential for future enhancements (haptics, olfactory, advanced sensors)	Computational demands; interoperability and standards still evolving

225. Despite its clear advantages, AI-supported XR-based training poses several challenges and limitations that require careful consideration.[137] First, it is paramount

[137] Regal, Georg, Daniele Pretolesi, Helmut Schrom-Feiertag, Jaison Puthenkalam, Massimo Migliorini, Elios De Maio, Francesca Scarrone, et al. "Challenges in Virtual Reality Training for CBRN Events." *Multimodal Technologies and Interaction* 7, no. 9 (September 11, 2023): 88. https://doi.org/10.3390/mti7090088.

to ensure the comfort and safety of trainees using XR platforms. Cybersickness may occur across all XR modalities, although it is most common and severe in VR due to the stronger sensory mismatch between visual motion and physical motion. This form of motion sickness—often triggered by motion-intensive simulations—can cause dizziness, nausea, headaches, and disorientation. However, it can be mitigated through a combination of design choices, hardware improvements, and user-centred practices. Safety precautions must also be taken to prevent users wearing headsets from injuring themselves on real-world objects.

226. A second challenge is scenario realism. For virtual training to be effective, it must replicate real-life operations as closely and credibly as possible. Currently, neither VR nor AR can fully replicate the logistical, physiological, and sensory realities of a real CBRN operation. For example, the absence of real danger reduces stress levels. In addition, the lack of equipment carried, obstacles, odours, and heat significantly decreases the physical burden compared with operational conditions. The challenge for developers is therefore to create simulations that are as realistic as possible within the limits of current technology, and to design them so that they can be adapted to different scenarios and environments. It would be beneficial if users could create their own scenarios to provide better flexibility and enhance training opportunities.

227. Training while wearing personal protective equipment (PPE) and carrying and using equipment is crucial for experiencing and becoming accustomed to key limitations such as reduced field of vision, restricted mobility, heat stress, and increased physical burden. Training in an exclusively virtual environment cannot provide this essential experience. Integrating real-world PPE and critical equipment, such as sampling and detection tools, into the virtual environment will therefore be vital for developing effective and realistic training. During the third meeting of the TWG, members were able to view and trial a recently developed XR-adapted integrated CBRN respirator to understand its capabilities.[138] Such developments will enhance the effectiveness of future XR training in the CBRN domain.

228. Extended reality training can only achieve its full instructional value if it is meaningfully embedded in a broader training programme, and an effective evaluation and lessons-learned methodology is an essential part of this process. Extended reality technologies could hinder the learning process if not applied appropriately. In particular, it is important that trainees do not perceive immersive training simply as a game, which may occur if scenarios can be repeatedly restarted without consequence. Train-the-trainer programmes are therefore necessary to ensure that

[138] "XR1403" Ocean Reef Group, January 19, 2026.

instructors can manage the scenarios effectively, resolve technical problems, and make efficient use of digital evaluation tools.

229. Future developments could help address several of the current challenges and limitations of XR tools. For example, the integration of additional components—such as autonomous sensory meridian response (ASMR) triggers,[139,140] olfactory elements, haptic feedback (including force feedback and weight simulation),[141,142] medical modules, chemical dispersion models, or diverse sensor inputs including vision, speech, and contextual data—would increase the realism of training scenarios and enhance their effectiveness.

230. Integration with AI would enable more advanced data analytics, dynamic scenario generation, and sensor fusion capabilities. Optimisation of computational resources, for instance through model compression and fine-tuning, will also be important as higher realism and lower latency demand substantial processing power.

231. Future research should explore improvements in human-computer interaction, enabling AI algorithms to respond naturally to speech and gestures and facilitating more intuitive, real-world communication within XR environments. To broaden the application of AI in XR systems and enhance interoperability, the development of unified standards and interfaces is also recommended.

Operationalisation of AI-supported XR training tools at the OPCW

232. Through Subgroup 4's detailed examination of AI-supported XR-based training tools, the TWG recognises that adoption of these tools by the Secretariat could be highly beneficial in enhancing its training capability. Such tools would enable safer, more flexible, and repeatable training, applicable to a range of relevant situations. These

[139] Peng, Danyang, Tanner Person, Kinga Skierś, Ruoxin Cui, Mark Armstrong, Kouta Minamizawa, and Yun Suen Pai. "asmVR: Enhancing ASMR Tingles with Multimodal Triggers Based on Virtual Reality." *SIGGRAPH Asia 2023 XR*, November 28, 2023, 1–2. https://doi.org/10.1145/3610549.3614597.

[140] Ling, Jiaxuan. *Enhancing Autonomous Sensory Meridian Response (ASMR) through personalised triggers in virtual reality.*, 2025. https://doi.org/10.26021/15842.

[141] Topliss, Jack, Stephan Lukosch, Euan Coutts, and Tham Piumsomboon. "Is Modularity the Future of Haptics in XR? A Systematic Literature Review." *Virtual Reality* 29, no. 2 (April 24, 2025). https://doi.org/10.1007/s10055-025-01147-8.

[142] Stellmacher, Carolin, Michael Bonfert, Ernst Kruijff, and Johannes Schöning. "Triggermuscle: Exploring Weight Perception for Virtual Reality through Adaptive Trigger Resistance in a Haptic VR Controller." *Frontiers in Virtual Reality* 2 (January 14, 2022). https://doi.org/10.3389/frvir.2021.754511.

could include routine inspections as well as complex contingency operations, and settings such as large chemical manufacturing plants, abandoned facilities, laboratories, or high-threat environments. This would provide valuable training opportunities in environments that would otherwise be inaccessible. While noting the many advantages and the relatively low cost of AI-supported XR-based training tools, it was recognised that their adoption would nevertheless involve start-up and maintenance costs, as well as time and careful consideration to ensure adequate realism.

233. States Parties could adopt AI-supported XR tools to enhance national preparedness, including identifying appropriate PPE and detectors, exercising response plans, and supporting incident command, medical response, hazard assessment, and evacuation procedures. The chemical industry could similarly use digital twins to improve hazard assessment and emergency planning. The Secretariat should consider how these applications could be incorporated into its capacity-building programme.

234. Before instituting a new training capability, assessing existing skill levels within the Secretariat to develop role-appropriate training is important. The TWG advocates the development of AI literacy across the Secretariat, which could be leveraged not only for XR-based training tools but also for other AI applications that may be adopted in the future. In addition, the TWG highlights the need for specialised technical staff, such as a data scientist, who would play a key role in establishing and maintaining the training infrastructure and adapting algorithms where required.

235. The TWG considers that AI would be fundamental not only in generating realistic training scenarios, but also in associated processes, such as planning, equipment selection, and considering safety and security implications, thereby contributing to an effective immersive experience. The integration of user-friendly dashboards was identified as essential to simplifying these advanced tools, ensuring accessibility and maintaining focus on training outcomes rather than underlying algorithms. Training systems should also be designed to allow instructors to monitor exercises in real time and to intervene as necessary, including by modifying scenario parameters, introducing injects, or pausing or terminating exercises as required for safety, learning effectiveness, or technical reasons. It was also noted that criteria would be needed to assess the quality and suitability of prospective AI tools.

236. It is essential that data governance—and data protection in particular—be carefully considered in the design, development, and deployment of AI-supported XR training systems. During immersive training, large volumes of sensitive data may be generated and collected.[143] It is imperative that this information, which may be

[143] Bernardo, Vítor. "Extended Reality." European Data Protection Supervisor, November 2023.

personal, organisational, or operational in nature, as well as the underpinning algorithms, are adequately protected, and that training systems comply with all relevant data protection and security regulations. This includes the implementation of robust controls to prevent unauthorised access, appropriate data classification, and the anonymisation of user data. The TWG further proposes that training systems should be capable of operating offline, thereby providing an additional layer of protection for sensitive data.

237. Immersive simulations may expose trainees to distressing and potentially traumatising scenarios rendered with a high level of realism. The psychological impact of such training should therefore be carefully considered, with appropriate support mechanisms and stress-level monitoring in place, enabling scenarios to be adapted or discontinued if necessary. The development of guidelines could help ensure that trainees do not experience adverse psychological effects as a result of XR-based training and that any staff member who is unable to fully utilise XR tools due to physiological responses is not disadvantaged in terms of performance evaluation, career progression, or work opportunities.

238. Cognitive bias may be unintentionally introduced into XR-based training through scenario design, data selection, and automated assessment mechanisms. If left unaddressed, such biases could reinforce narrow perspectives or habitual responses. Mitigation measures include the use of diverse scenario sets, regular review of training content, transparent evaluation criteria, and the retention of human oversight through instructor-led supervision and structured after-action reports.

239. While AI-enhanced XR-based training may be highly effective when appropriately implemented, it cannot replace physical training entirely.[135] It should be viewed as a complementary approach to traditional training methods that will supplement the development of certain practical skills—such as sampling, decontamination, note-taking, or donning PPE under time pressure—that still require hands-on training. Furthermore, the skills acquired through “live agent” training—exercises involving the controlled presence and handling of actual CWAs—cannot be reproduced through immersive methods and should therefore remain part of the OPCW inspectors’ training programme. A considered combination of virtual and traditional training will ensure a comprehensive, effective, and resilient training framework that maximises learning outcomes while maintaining operational realism.

Recommendation 11

AI-supported XR tools should be developed and deployed to train operational Secretariat staff, including inspectors and staff in the Office of Special Missions. Development should be based upon a detailed scenario and user-needs analysis and supported by a clear concept of operations. Key requirements for XR training tools should include:

a. realistic, dynamic training scenarios, including contingency operations, with AI-generated injects;
b. integration with real equipment, such as detectors and personal protective equipment;
c. user-defined scenario creation;
d. instructor oversight, including real-time intervention and performance evaluation tools;
e. AI-driven evaluation and feedback;
f. secure, controlled operation, including offline capability and robust data protection; and
g. advanced realism and future readiness, including non-player characters, digital twins for chemical facilities, and future sensory enhancements.

---o---

ANNEX 1: Glossary of Terms

This glossary provides definitions of key technical terms that are used in this report, with illustrative examples of potential relevance to the activities of the OPCW and the Convention. These examples are provided for context and understanding, and do not constitute recommendations for implementation.

Disclosure: This glossary was developed with the assistance of AI technology to help ensure accuracy, clarity, and comprehensiveness of the technical definitions provided.

Term	Definition
Access Control	Security policies and technical systems that regulate who can view, modify, or use specific data and systems within an organisation. Access control combines organisational rules about permissions with technical infrastructure, including authentication methods, to ensure that sensitive information is only accessible to authorised personnel based on their roles and responsibilities. *See also: Data Security*
Air-Gapped	A security measure in which a computer system or network is physically isolated from external networks, including the internet, to prevent unauthorised access or data transfer. Air-gapped systems are used to protect highly sensitive information by ensuring that data cannot be transmitted externally without deliberate and controlled intervention. *See also: Data Security*
Algorithm	A step-by-step set of instructions that tells a computer how to solve a problem or complete a task. AI algorithms are special because they can adapt and improve their performance by learning from data, rather than following the same fixed steps every time. *See also: Machine Learning, Neural Network*

Application Programming Interface (API)

A set of rules and protocols that allows different software systems to communicate and exchange information with each other. APIs enable applications to request services, data, or functionality from other systems without needing to understand their internal workings, supporting interoperability and automation.

Artificial Intelligence (AI)

Technology that uses mathematical and statistical methods to enable computers to perform tasks that normally require human thinking, such as recognising patterns, understanding language, and making decisions. Unlike traditional computer programmes that follow pre-written rules, AI systems analyse data to discover relationships and make predictions based on what they learn.

See also: Machine Learning, Deep Learning, Neural Network

Augmented Reality (AR)

Technology that overlays digital information—such as images, data, or instructions—onto the real-world environment, typically viewed through smart glasses, mobile devices, or headsets. AR enhances situational awareness by combining virtual elements with the physical world, supporting applications such as guided workflows, visualisation, and contextual training.

Automation

The principle and practice of using technology to perform tasks without constant human intervention. Automation involves analysing processes to identify which activities can and should be handled by technology rather than manually, based on factors like repetitiveness, rule-based nature, and efficiency gains. Modern automation can range from simple repetitive tasks to more versatile, adaptive systems that can handle varied situations and make decisions based on changing conditions.

See also: Workflow Automation

Bayesian

An approach to statistics and modelling based on updating probabilities as new information becomes available. Bayesian methods combine prior knowledge with observed data to estimate uncertainty and refine predictions, and are commonly used in machine learning, risk assessment, and decision-making under uncertainty.

Bias (Algorithmic)

Systematic errors or unfair outcomes in AI systems that may disadvantage certain groups or produce skewed results. Bias can emerge from training data, algorithm design, or deployment practices, potentially affecting the reliability and fairness of AI applications in verification and monitoring activities.

Cloud Infrastructure

The underlying digital and computational resources, including servers, storage, and networking, that support cloud-based applications and services. In scientific contexts, cloud infrastructure enables remote execution of experiments, data storage, and AI-driven computation without requiring local hardware.

See also: Cloud Laboratory

Cloud Laboratory

A remotely accessible laboratory that allows users to design and execute chemical or biological experiments through digital interfaces. Cloud laboratories integrate automation, robotics, and data management systems, enabling users without local facilities to perform experiments, rapidly iterate procedures, and access advanced instrumentation from virtually anywhere.

See also: Self-Driving Laboratory (SDL), Automation

Concatenation

The process of linking or joining two or more elements—such as strings of text, data fields, or sequences—end-to-end to form a single continuous unit. In computing and data processing, concatenation typically refers to combining strings or datasets without altering their individual content.

Convolutional Neural Network (CNN)

A type of deep learning model particularly suited for analysing spatial or grid-like data, such as images or spectroscopic maps. CNNs automatically detect patterns, features, and correlations in complex datasets, making them useful for tasks like spectral classification and chemical imaging analysis.

See also: Neural Network, Deep Learning

Data Curation

The process of actively selecting, evaluating, and transforming raw information from various sources into reliable, well-documented datasets that can be discovered and used for future applications. Data curation involves making decisions about what information is valuable, verifying its accuracy, preserving the context of how it was originally collected or presented, and organising it at the appropriate level of detail to support different analytical needs and use cases.

See also: Data Management

Data Engineer

A technical specialist who builds and maintains the computer systems and infrastructure that handle an organisation's data. Data engineers create the technological foundation that allows data to be collected, stored, processed, and accessed reliably and securely by others in the organisation.

Data Governance

The strategic framework that establishes who has authority over organisational data, what policies govern its use, and how decisions about data are made. Data governance defines roles, responsibilities, and standards for data quality, security, and compliance, ensuring data is treated as a valuable organisational asset with clear accountability and oversight.

See also: Data Owner, Data Steward, Data Management

Data Management

The operational implementation of data governance policies through the practical activities of collecting, storing, organising, maintaining, and utilising data throughout its lifecycle. Data management involves the day-to-day processes and technologies that could ensure OPCW information assets remain accurate, accessible, secure, and useful for organisational purposes.

See also: Data Governance, Data Curation, Data Security

Data Mining

The process of analysing large datasets to identify patterns, relationships, or trends using statistical methods, machine learning, and computational techniques. Data mining supports knowledge discovery by extracting useful information from complex or high-volume data.

Data Model

A blueprint or map that defines how information is organised, what types of data exist, and how different pieces of information connect to each other within a system. Data models serve as a guide for understanding how to navigate from one piece of information to another and establish the rules for how data relates across an organisation. Multiple data models can be linked together to connect different datasets or systems, enabling comprehensive analysis across various domains of information.

See also: Data Structuring

Data Owner

The individual or organisational unit with ultimate authority and accountability for specific datasets within an organisation. Data owners are responsible for defining access policies, ensuring data quality, making decisions about data usage and sharing, and ensuring compliance with relevant regulations and organisational policies.

See also: Data Governance, Data Steward

Data Scientist

A professional who combines statistical analysis, machine learning techniques, and domain expertise to extract insights from complex datasets. In OPCW applications, data scientists may develop predictive models for verification activities or apply AI techniques to support detection and analysis of prohibited activities.

Data Security

The protection of data and information systems from unauthorised access, corruption, theft, or loss through technical, administrative, and physical safeguards. Data security focuses on maintaining the integrity, availability, and confidentiality of organisational information assets, ensuring they remain accurate, accessible to authorised users, and protected from cyber threats and other risks.

See also: Access Control

Data Steward

A designated individual who combines subject matter expertise with data management responsibilities to oversee specific datasets on a day-to-day basis. Data stewards understand both the technical aspects of the data and its business context, ensuring data quality, monitoring usage, implementing governance policies, and serving as the primary point of contact for data-related questions within their domain of expertise.

See also: Data Governance, Data Owner

Data Structuring

The technical process of organising curated data into standardised, machine-readable formats that enable efficient storage, retrieval, and automated processing. Data structuring involves defining data types, establishing field formats, creating consistent naming conventions, and ensuring that information is arranged in ways that computer systems can easily access, search, and analyse.

See also: Data Model

Deep Learning

An advanced form of machine learning that can analyse complex information like images, text, or audio. Deep learning systems can handle sophisticated tasks such as recognising objects in photographs or understanding written documents, making them useful for processing diverse types of data relevant to OPCW activities.

See also: Machine Learning, Neural Network, Convolutional Neural Network (CNN)

Digital Twin

A virtual representation of a physical object, system, or environment that mirrors its real-world characteristics and behaviour using data, models, and simulations. Digital twins enable monitoring, analysis, testing, and training in a controlled virtual setting, supporting scenario planning, risk assessment, and operational decision-making without affecting real-world systems.

Explainability

The extent to which the internal workings, decisions, or predictions of an AI or machine learning model can be understood and interpreted by humans. Explainability provides insight into why a model produces a particular output, helping users trust, validate, and diagnose AI-driven analyses, particularly in high-stakes domains such as chemical detection and safety.

Extended Reality (XR)

An umbrella term encompassing immersive technologies that blend physical and digital environments, including virtual reality, augmented reality, and mixed reality. XR enables varying levels of immersion and interaction, supporting training, simulation, collaboration, and visualisation across a wide range of operational and educational contexts.

See also: Virtual Reality (VR), Augmented Reality (AR), Mixed Reality (MR)

Fourier-Transform Infrared Spectroscopy (FTIR)

An analytical technique that measures the absorption of infrared radiation by a sample to identify molecular vibrations. FTIR produces a spectrum representing chemical bonds and functional groups, allowing for rapid identification and characterisation of substances.

See also: Spectral Data, Raman Spectroscopy

Graph Neural Network (GNN)

A type of machine learning model designed to analyse data structured as graphs, such as molecules where atoms are nodes and bonds are edges. GNNs can capture the relationships between components in a network, enabling predictions of chemical, physical, or spectral properties, and supporting AI-driven tasks like molecular property prediction and structure elucidation.

See also: Neural Network, Deep Learning

High-Dimensional Data

Data that contain a very large number of variables or features relative to the number of observations. High-dimensional data arise in areas such as spectroscopy, genomics, and chemical sensing, where each sample can be represented by thousands of measurements, requiring specialised statistical or AI methods to extract meaningful patterns and avoid overfitting.

Large Language Model (LLM)

An AI program that mimics the decision-making abilities of human experts in specific domains. These systems use knowledge bases and inference rules to provide recommendations or analysis, potentially supporting chemical weapons identification or verification procedures.

See also: Natural Language Processing (NLP)

Machine Learning

A type of artificial intelligence where computers learn to perform tasks by finding patterns in examples and data, rather than being programmed with specific rules. The system improves its performance as it processes more examples, enabling it to make predictions or decisions about new situations it has not seen before, potentially supporting various OPCW analytical tasks.

See also: Deep Learning, Algorithm

Mass Spectrometry

An analytical chemistry technique used to identify what substances are present in a sample by analysing their unique characteristics at a molecular level. Mass spectrometry provides precise identification of chemical compounds, degradation products, and related materials with high sensitivity and accuracy, making it a powerful tool for determining the composition of unknown samples.

See also: Spectral Data

Metadata

Data that describes other data, providing contextual information such as origin, format, author, date of creation, classification level, or processing history. Metadata helps organise, manage, and retrieve information efficiently and supports traceability, governance, and quality control within data systems.

Mixed Reality (MR)

Technology that combines elements of both physical and virtual environments, allowing digital objects to be anchored to and interact with the real world in real time. Using specialised headsets, users can see and manipulate virtual content alongside physical objects, enabling collaborative workflows, spatial visualisation, and interactive training scenarios.

Multimodal Models

AI models designed to process and integrate multiple types of data, such as text, images, audio, or video, within a single system. By combining information across modalities, these models can perform more complex reasoning and understanding than models restricted to a single data type. Multimodal foundation models are a class of multimodal models trained on large-scale datasets to provide versatile capabilities across different tasks and domains.

Natural Language Processing (NLP)

The fundamental AI technology that enables computers to work with human language in all its forms—reading text, understanding speech, parsing grammar and meaning, and generating responses. NLP is the underlying capability that makes it possible for computers to communicate naturally with people and process language-based information, serving as the foundation for applications like translation, document analysis, and conversational AI systems.

See also: Large Language Model (LLM)

Neural Network

A type of AI system designed to process information in a way loosely inspired by how the human brain works. These systems can recognise complex patterns and relationships in data, making them useful for tasks like image recognition or data analysis.

See also: Deep Learning, Machine Learning

Orthogonality

In chemical sensing or analytical contexts, the concept that two measurements or sensors operate independently, measuring distinct physical or chemical properties. Orthogonal measurements reduce correlated errors, increase reliability, and improve confidence in multi-sensor detection strategies.

Pattern Recognition

The automated identification of regularities or structures in data. In OPCW contexts, this could include recognising signatures of chemical processes or detecting anomalies in declaration data.

Precursor

A chemical compound used as a starting material in the production of another substance. Precursors undergo chemical reactions or transformations to form the desired target compound, serving as the initial building blocks in synthetic pathways.

Raman Spectroscopy

An analytical technique that measures the inelastic scattering of light by molecules to provide information on vibrational, rotational, and other low-frequency modes. Raman spectra offer molecular “fingerprints” complementary to FTIR, useful for identifying chemical composition and structural features.

See also: Fourier-Transform Infrared Spectroscopy (FTIR), Spectral Data

Remote Sensing

The collection of information about places, objects, or activities from a distance, typically using satellites, aircraft, or drones equipped with cameras and sensors. AI can enhance these capabilities to automatically analyse imagery and detect changes or activities of interest.

Retrosynthesis

The computational process of determining possible synthetic pathways to produce a target chemical compound by working backward from the final product to identify starting materials and reaction sequences. Retrosynthesis analysis can develop alternative synthesis routes for existing compounds, design new pathways to create novel derivatives, assess the feasibility of producing specific chemicals, and evaluate the complexity of different synthetic approaches.

See also: Synthesis, Precursor

Self-Driving Laboratory (SDL)

An advanced automation system that can independently design, execute, and analyse processes with minimal human intervention, using AI to optimise conditions, interpret results, and plan subsequent activities. These systems can handle diverse applications from research experiments to production and synthesis operations, offering scalable solutions with smaller physical footprints. Self-driving laboratories can adapt to produce different outputs by leveraging similar underlying processes and methodologies, making them highly versatile for various analytical, research, or manufacturing needs.

See also: Automation, Workflow Automation, Cloud Laboratory

Semantic Search

A search approach that focuses on understanding the meaning and context of a user's query rather than relying solely on exact keyword matches. Semantic search uses natural language processing and contextual analysis to retrieve relevant information even when different terminology or phrasing is used, improving accuracy and usability in large or complex datasets.

Software Engineers

Professionals who design, develop, test, and maintain software systems and applications. Software engineers apply engineering principles to create reliable and scalable digital solutions, often collaborating with data scientists, machine learning engineers, and subject-matter experts to implement and integrate AI capabilities.

Spectral Data

Information obtained from analytical techniques that measure the interaction of matter with electromagnetic radiation, such as infrared (IR), nuclear magnetic resonance (NMR), or Raman spectroscopy. Spectral data provide molecular "fingerprints" that reveal chemical composition, structure, and properties of substances, enabling identification, verification, and quality control.

See also: Fourier-Transform Infrared Spectroscopy (FTIR), Raman Spectroscopy, Mass Spectrometry

Synthesis

The deliberate chemical process of producing a target compound from simpler starting materials or precursors. Synthesis involves planning reaction pathways, selecting reagents and conditions, and executing laboratory procedures to generate a desired chemical product, whether for research, pharmaceutical, or industrial applications.

See also: Retrosynthesis, Precursor

Training Data

The dataset used to teach machine learning algorithms how to make predictions or decisions. The quality, representativeness, and accuracy of training data directly impact AI system performance and reliability.

Transformer Models

A class of deep learning architectures designed to process sequential data using attention mechanisms. Transformers can capture long-range dependencies and contextual relationships in data, making them well-suited for tasks such as natural language processing, spectral prediction, and multi-modal chemical data integration.

Uncrewed Platforms

Systems or vehicles that operate without an onboard human operator, typically controlled remotely or functioning autonomously using sensors and software. Examples include aerial, ground, surface, or underwater platforms used for monitoring, inspection, data collection, or operational tasks.

Validation

The process of testing whether an AI system meets its requirements and performs as expected for its intended use. Validation involves evaluating the system's accuracy, reliability, and performance using independent data to confirm it works properly in real-world situations before deployment.

Vapour Pressure

A measure of the tendency of a substance to evaporate, defined as the pressure exerted by its vapour in equilibrium with its liquid or solid phase at a given temperature. Vapour pressure influences volatility, environmental persistence, inhalation risk, and chemical handling requirements, making it an important parameter for safety assessment and regulatory considerations.

Virtual Reality (VR)

Technology that creates realistic, computer-generated environments that users can explore and interact with using special equipment like headsets and controllers. VR enables immersive training, realistic simulations, and remote collaboration as if people were physically present in the same space.

Workflow Automation

The automation of entire business processes or sequences of tasks, coordinating multiple steps, systems, and decision points to complete complex procedures with minimal human intervention. Workflow automation orchestrates how work moves through an organisation, ensuring consistent execution of multi-step processes and maintaining quality and compliance standards.

See also: Automation, Self-Driving Laboratory

ANNEX 2: TWG on AI – Terms of Reference

1. Artificial intelligence (AI) is emerging as a powerful enabling technology that is increasingly being integrated into many other disciplines and technologies, including biotechnology, robotics, and drones. The resultant synergistic effect can significantly enhance capabilities beyond what each technology can achieve in isolation. AI is accelerating progress in chemistry and related fields, in addition to making associated processes cheaper, faster, and more effective.

2. AI, particularly in relation to risks, governance, and regulation, is continuing to capture significant attention, both nationally and regionally, in addition to coming to the fore within a range of international organisations, including the United Nations and the OPCW. In its recent comprehensive scientific report submitted to the Fifth Review Conference (RC-5/DG.1, dated 22 February 2023), the Scientific Advisory Board (SAB) identified a number of potential risks posed by the misuse of AI, including its use and integration in other technologies, as well as opportunities that this technology may afford the OPCW in its implementation of the Chemical Weapons Convention (the Convention).

3. Given the novelty of AI, its unprecedented pace of development, and its rapid inclusion in many fields, it behoves the OPCW to identify and understand the potential impacts AI might have on its mission to achieve a world free of chemical weapons, to prevent the re-emergence of chemical weapons, and to promote the peaceful uses of chemistry. Consequently, in accordance with paragraph 9 of the terms of reference of the SAB (Annex to C-II/DEC.10/Rev.1, dated 2 December 2004), the Director-General has decided to establish a Temporary Working Group (TWG) on Artificial Intelligence and has appointed Dr Catharina Müller-Buschbaum as the Chairperson of the Group.

4. Through a review of current AI capabilities and technology adoption, the objective of the TWG is to understand the impact of the technology on the object and purpose of the Convention and identify the risks to and opportunities for its implementation. The findings will be considered by the SAB and recommendations will be provided to the Director-General.

5. The TWG will consist of individuals who have expertise in AI, especially in the context of the chemical sciences. Group members may have expertise in a range of subfields of AI, including machine learning, deep learning, natural language processing, robotics, and computer vision; the application of AI in research and/or industry relating to chemical sciences or data analytics; AI ethics and governance; or experience of implementation of the Convention. The TWG will comprise qualified members of the SAB as well as representatives from the chemical industry and

relevant academic and scientific organisations. Guest speakers from all geographical regions will be invited to assist the TWG in its collection of data and information, and formulation of advice.

6. The TWG will provide a summary of the current state of the art, and expected near-term progress to be made, in the following areas:

   a) synthesis and retrosynthesis prediction;
   b) automated and remote synthesis and production of chemicals;
   c) data curation, protection, and reliability;
   d) property, spectral, and data prediction and generation;
   e) data/sensor fusion for augmented detection and analysis; and
   f) simulation and training.

7. While considering the six technical areas set out in question 6, the TWG should ensure that the following questions are also addressed:
   a) What new capabilities are being enabled, that is, what can be done now that was not possible before? Consider both opportunities and risks.
   b) What are the current limitations and challenges to further progress, and which obstacles are likely to remain difficult or impossible to overcome?
   c) What external, non-technical factors exist that may accelerate or enable progress and/or technology adoption or slow it down?

8. The TWG is also requested to consider how advances in AI will impact the implementation of the Convention and the work of the OPCW by considering the following questions:
   a) What red flags or anomalies could help in identifying the potential misuse of AI systems?
   b) Which specific AI applications are sufficiently mature for the OPCW to utilise in augmenting its capabilities?
   c) What changes will be seen in industry in the coming years as AI becomes increasingly integrated into chemical production processes?
   d) How might AI impact verification efforts, either by increasing risks or by presenting opportunities?
   e) What existing guardrails and governance frameworks in the AI domain could be used, or further developed, to prevent the misuse of AI within the context of the Convention?
   f) How can the OPCW promote the responsible use of AI in relation to the Convention?

9. The TWG will also highlight and consider any other application areas of AI that may be relevant within the context of this work.

10. On the basis of this in-depth review and assessment, the TWG will provide a list of recommended short- and long-term actions to ensure that AI can be harnessed for good and that its associated risks can be mitigated or, as a minimum, closely monitored.

11. The Director-General might pose additional, related questions to the TWG, through the SAB.

12. The TWG will exist for a period of one year starting on 1 January 2025. Thereafter, its work will be reviewed by the SAB and the Director-General, and a decision will be made as to whether it should continue its work and, if so, whether these terms of reference should be revised.

ANNEX 3: Members of the TWG on AI

	Participants	Affiliation
1	Dr Roy Forbes	University of Witwatersrand, South Africa
2	Prof. Matthew Gaunt	University of Cambridge, United Kingdom of Great Britain and Northern Ireland
3	Prof. Anya Gryn’ova	University of Birmingham, United Kingdom of Great Britain and Northern Ireland
4	Prof. Jason Hein	University of British Columbia, Canada
5	Prof. Keunhong Jeong*†	Korea Military Academy, Republic of Korea
6	Prof. Anneli Kruve	Stockholm University, Sweden
7	Dr Michael Kuiper	Google DeepMind, United Kingdom of Great Britain and Northern Ireland
8	Mr Arthur Li	Chemical.AI, Canada
9	Prof. Imee Su Martinez*	University of Philippines-Diliman, Philippines
10	Prof. José L. Medina-Franco	National Autonomous University of Mexico, Mexico
11	Prof. Hajar Mousannif	Cadi Ayyad University, Morocco
12	Dr Catharina Müller-Buschbaum*	Accenture, Germany
13	Col. Günter Povoden	CBRN Defence Centre, Austrian Armed Forces, Austria
14	Ms Molly Strausbaugh	CAS, United States of America
15	Dr Tongning Wu	China Academy of Information and Communications Technology, China

* Member of the SAB during the mandate of the TWG

† Since completion of the TWG’s mandate, Prof. Jeong has taken up a position at Sogang University, Republic of Korea

ANNEX 4: Invited Speakers at Meetings of the TWG on AI

Speaker	Affiliation
First meeting	
Ms Joana Iljazi	Google DeepMind, United Kingdom of Great Britain and Northern Ireland
Dr Stanisław Jastrzębski	molecule.one, Poland
Dr Teodoro Laino	IBM Research Europe, Switzerland
Second meeting	
Dr Mohamed Amine Chadi	Cadi Ayyad University, Morocco
Prof. Bin Fang	Beijing University of Posts and Telecommunications, China
Prof. Bartosz Grzybowski	Ulsan National Institute of Science and Technology, Republic of Korea and Polish Academy of Sciences, Poland
Dr Simon See	NVIDIA AI Technology Center, Singapore
Dr Ning Xia	Chemical.AI, China
Third meeting	
Prof. Carolina Horta Andrade	Federal University of Goiás, Brazil
Mr Andrea D’Angelo	Fondazione Security and Freedom for Europe, Italy
Prof. Robert Pollice	University of Groningen, Netherlands
Dr Luke Rogers	On Demand Pharmaceuticals, United States of America
Mr Paul Schneeweiss	International Atomic Energy Agency (IAEA)
Ms Mariella Steinöcker	Vienna University of Technology, Austria

ANNEX 5: How the TWG on AI Leveraged AI

Methodology: AI as a Collaborative Partner

The relationship between human experts and AI tools throughout the duration of this TWG can best be characterised as genuinely collaborative rather than hierarchical. Human experts provided domain knowledge, strategic direction, quality control, contextual judgment, and final decision-making authority. AI tools provided tireless analytical capacity, rapid synthesis, organisational structure, consistency maintenance, and creative alternatives when initial approaches proved inadequate. The combination enabled faster iteration cycles, more comprehensive analysis, better-organised content, and higher-quality outputs than either humans or AI could produce independently.

In particular, Claude Sonnet 4.5, accessed through Claude Projects, enabled the TWG to maintain continuity across multiple working documents, draft iterations, and work sessions spanning several months. This capability proved particularly valuable given that TWG members contributed at different times and through different channels, as the AI system could synthesise inputs from various sources into coherent draft text while preserving the technical accuracy and nuance of expert contributions.

For visual content development, the TWG employed Nano Banana, an AI-based graphics generation tool, to generate custom illustrations that visually represent key concepts or points in the report. TWG members used different prompting techniques, some developed with other AI models to input into Nano Banana to enable image generation. These initial illustrations were then redrawn and/or restyled manually to ensure they depicted the ideas exactly as needed.

The TWG's experience with AI-assisted report development offers several lessons relevant to the broader question of how the Secretariat might integrate AI capabilities into its workflows. First, AI tools prove most valuable when deployed as collaborative partners rather than as simple automation of routine tasks. Second, maintaining human expert review, integration, and oversight at all stages remains essential for ensuring accuracy, contextual appropriateness, and alignment with organisational requirements. Third, the availability of institutional memory and continuity across work sessions represents a substantial advantage over traditional approaches where context and rationale may be lost between meetings or when personnel change. Fourth, the combination of multiple complementary AI tools (in this case, different language models and specialised graphics generation) provides redundancy and validation that strengthens confidence in outputs.

ANNEX 6: AI Implementation RACI Chart

Roles and Responsibilities for AI Capacity Building

This RACI matrix defines accountability and collaboration across AI implementation activities.

R = Responsible (does the work) | A = Accountable (final decision authority) | C = Consulted (provides input) | I = Informed (kept updated) | SME = subject-matter expert

Note: Cross-functional collaboration is essential. Multiple RACI assignments reflect the need for teamwork and coordination across roles.

Activity	SME with AI Literacy	Data Scientists	Data Engineers	Software Engineers	Knowledge Management & Transfer
1. Strategic Planning and Requirements					
Define AI use cases	**A/R**	**R**	**I**	**C**	**I**
Assess organisational readiness	**A/R**	**C**	**C**	**C**	**C**
Set success metrics	**A/R**	**C**	**I**	**C**	**I**
2. Data Governance					
Data governance framework	**C**	**C**	**A**	**C**	**R**
Data modelling and structuring	**I**	**C**	**A**	**C**	**R**
Data stewardship protocols	**C**	**I**	**A**	**I**	**R**
Determine access controls	**C**	**C**	**A**	**C**	**R**

Activity	SME with AI Literacy	Data Scientists	Data Engineers	Software Engineers	Knowledge Management & Transfer
3. Data Management					
Data pipeline construction	I	C	A	R	I
Data profiling and quality analysis	C	A/R	C	I	I
Data quality assurance	C	C	A	R	I
Data reliability and protection	C	I	A	R	C
Enforce access controls	I	I	A	R	C
4. Model Development					
Model design and selection	C	A	C	C	I
Model training and iteration	I	A	R	C	I
Model validation	C	A	C	R	I
Model performance evaluation	C	A	C	R	I
5. System Integration					
Technical architecture design	C	C	C	A/R	I
ML feature integration	I	C	R	A	I

Activity	SME with AI Literacy	Data Scientists	Data Engineers	Software Engineers	Knowledge Management & Transfer
System deployment	C	C	C	A	I
System testing	C	C	C	A	I
6. Quality Assurance and Oversight					
Human review protocols	A	C	C	C	R
Performance monitoring	C	C	C	A	R
Compliance validation	C	C	A/R	C	C
Error analysis and correction (domain/content)	A/R	C	C	C	I
Technical debugging and system fixes	C	C	C	A/R	I
7. Documentation and Knowledge Transfer					
Workflow documentation	C	C	C	C	A/R
Training materials development	C	C	I	I	A/R
Knowledge base maintenance	C	I	I	I	A/R
Standard operating procedures	C	C	C	C	A/R

Activity	SME with AI Literacy	Data Scientists	Data Engineers	Software Engineers	Knowledge Management & Transfer
8. Ongoing Operations					
System maintenance	**I**	**C**	**C**	**A/R**	**I**
Model retraining	**C**	**A**	**R**	**C**	**I**
Continuous improvement	**R**	**R**	**R**	**R**	**A**
Incident response	**C**	**C**	**C**	**A/R**	**C**

Page left intentionally blank

0 1 0 1 0 1 1 1 0 1 0 0
1 1 1 1 0 1 0 1 0 0 1 0
0 1 0 0 1 0 1 1
0 1 0 0 1 0 0 1 0 1 0 0
1 1 1 0
0 1 0 0 0 1 1
1 0 0 1 0 0 0
0 0 0 1 0 1 0 1 0 0
0 1 0 0 1 1 1 1 0 1 0
0 0 1 1 1 0 1 0 0 0 1
0 1 0 1 0 1 0
1 0 0 0 1 0 0 1 0 0 0 0
1 0 0 0 1 0 1 0 1 0 1 0
0 1 0 0 0 1 0 0 0 0 0 0
1 0 0 0 1 1 0 0 1 0 0 1
1 1 1 0 1 0 1 0 0 1 0 0
0 1 0 0 0 0 0 0 1 0 0 0
0 0 1 0 0 1 0 0 0 0 0 0
1 0 1 0 1 1 1 0 1 0 0 1
1 1 1 0 1 0 1 0 0 1 0 0
1 0 0 1 1 0 0 0 1 0 0 0
1 0 0 0 0 1 0 0 0 0 0 0
1 0 0 0 1 1 0 0 1 0 1 0
0 1 0 0 1 0 0 0 1 0 1 0
1 0 0 0 1 0 1 0 0 1 0 0
0 0 0 0 1 0 0 1 1 1 1 0
1 0 0 0 1 1 0 0 0 1 0 0
0 0 0 0 1 0 0 0 0 1 1 0
1 0 0 1 0 0 0 0 1 0 0 0
1 0 1 0 1 0 0 1 1 0 1 0
1 0 0 1 0 0 1 0 1 0 0 0
0 1 1 0 1 0 0 0 0 0 1 0
1 0 0 1 1 0 0 0 0 1 0 0
0 0 0 0 1 0 1 0 1 1 1 0
1 0 0 0 1 0 1 0 1 0 0 0
0 0 1 0 1 0 1 0 0 0 0 0
1 0 0 1 1 1 1 0 1 0 0 1
1 1 0 0 1 0 1 0 0 1 1 0
0 1 0 1 1 1 0 0 0 1 0 0
0 0 0 0 1 0 1 0 1 1 1 0
1 0 0 1 1 1 1 0 1 0 1 0
0 1 0 0 1 0 0 1 0 1 1 0
1 0 0 1 0 0 1 0 1 0 0 1
1 1 0 0 1 0 0 0 1 1 1 0
0 1 0 0 0 0 0 0 1 0 1 0
1 0 0 0 1 0 0 1 1 1 1 0
1 0 0 0 1 1 1 0 1 0 0 0
1 0 1 0 1 0 1 0 1 0 0 0
1 0 0 1 0 0 0 0 1 0 0 0
1 0 1 0 1 0 1 0 0 1 0 0
0 1 0 0 0 0 0 0 1 0 0 0
1 1 0 0 1 0 0 1 1 1 1 0
1 0 1 0 0 1 0 0 0 1 0 0
0 0 0 0 1 0 0 0 0 0 1 0
0 1 0 0 0 0 0 0 1 0 1 0
1 1 1 0 1 0 0 1 1 1 1 0
1 0 1 0 0 1 0 0 1 0 0 1
1 0 0 0 1 0 0 0 1 0 0 0
0 1 0 0 0 0 0 0 1 0 0 0
1 1 0 0 1 0 1 0 0 1 0 0