EU Non-Proliferation and Disarmament Consortium

Promoting the European network of independent non-proliferation and disarmament think tanks

NON-PROLIFERATION AND DISARMAMENT PAPERS

No. 98 May 2025

CLOUD LABS AND OTHER NEW ACTORS IN THE BIOTECHNOLOGY ECOSYSTEM: EXPORT CONTROL CHALLENGES AND GOOD PRACTICES IN OUTREACH

KOLJA BROCKMANN, LAURIANE HÉAU AND GIOVANNA MALETTA

I. INTRODUCTION

Biotechnology is a highly innovative field that is pursuing advances in areas from drug discovery to synthetic biology, biomanufacturing, personalized medicine, gene therapy and sustainable green technology solutions. At the broadest level, it involves the application of science and technology to living organisms and their parts and products to alter living or non-living materials to produce knowledge, goods and services.[1] The biotechnology sector, which is better described as an ecosystem, encompasses a growing set of companies, universities and other research organizations and a vibrant do-it-yourself (DIY) biology community. Advances in biotechnology and the increasingly diverse profiles of new entrants to the biotechnology ecosystem pose a range of chemical and biological weapon (CBW) proliferation risks and export control challenges.

Cloud laboratories (cloud labs) are an example of a new actor entering the biotechnology ecosystem that is pioneering a new business model. Cloud labs exemplify how developments in emerging technologies converge in a way that poses challenges for the application of export controls. Cloud labs are fully automated, modular laboratories paired with artificial intelligence (AI) agents that provide analytical and assistance capabilities. Commercial providers offer these labs to customers for remote use, promising to perform a wide range of experiments, analyses or other lab work as a service.

[1] Friedrichs, S. and van Beuzekom, B., 'Revised proposal for the revision of the statistical definitions of biotechnology and nanotechnology', OECD Science, Technology and Industry Working Papers, 2018/01; and Cuffari, B., 'Top 5 emerging trends in life science and biotech for 2025', AZO Life Sciences, 6 Mar. 2025.

SUMMARY

The biotechnology ecosystem encompasses an expanding set of companies, start-ups, universities and other research organizations and a vibrant do-it-yourself biology community. Advances in biotechnology and the increasingly diverse profiles of new entrants to the ecosystem pose a range of chemical and biological weapon (CBW) proliferation risks and export control challenges. Among them, cloud laboratories (cloud labs) are an example of a new actor entering the biotechnology ecosystem that is pioneering a new business model. Cloud labs exemplify how developments in emerging technologies converge in a way that poses challenges for the application of export controls. Cloud lab providers offer fully automated, modular laboratories to customers for remote use to perform experiments and increasingly artificial intelligence-enabled research and analyses. Managing the CBW risks posed by cloud labs and other new actors in the biotechnology ecosystem requires awareness by relevant stakeholders and effective export control compliance measures. European Union member states and Australia Group participating states should therefore continue to assess and discuss the development of cloud labs, work to provide relevant guidance materials and develop good practices for conducting outreach activities targeting cloud lab providers and other relevant actors to reduce CBW proliferation risks.

ABOUT THE AUTHORS

Kolja Brockmann is an independent consultant and a Senior Researcher (non-resident) working with the SIPRI Dual-Use and Arms Trade Control Programme.

Lauriane Héau is a Researcher with the SIPRI Dual-Use and Arms Trade Control Programme.

Giovanna Maletta is a Senior Researcher with the SIPRI Dual-Use and Arms Trade Control Programme.

Cloud labs and other new actors are at risk of becoming targets of illicit procurement, foreign acquisition and technology theft, while their awareness of these proliferation risks varies significantly. A key element of managing these risks is the effective implementation of export control compliance functions alongside the robust and integrated application of biosafety, biosecurity and research security measures.[2] However, levels of awareness among these new entrants to the biotechnology ecosystem about the compliance obligations they create is often limited. The adoption of new technologies and working methods by actors within the biotechnology ecosystem thus poses substantial challenges for the effective implementation and enforcement of export controls.[3]

The Australia Group (AG) is an informal group of 43 participants, which includes all the European Union (EU) member states and the EU as a participant with full voting rights, that seeks to contribute to preventing the proliferation of CBWs by coordinating and harmonizing participants' export controls.[4] The AG participants agree on common guidelines for the responsible transfer of dual-use materials, equipment, technology and software, and maintain several common control lists that define relevant items.[5] The AG seeks to contribute to the implementation of states' obligations under the 1972 Biological and Toxin Weapons Convention (BWC) and the 1993 Chemical Weapons Convention. It is the main forum in which states discuss both technological advances in the area of chemical and biological technology and the application of export controls to related dual-use items.

This paper aims to help EU member states and other AG participants reduce CBW proliferation risks by improving the application of and compliance with export controls by new actors in the biotechnology ecosystem.[6] Section II explores the CBW proliferation risks associated with trends in the biotechnology ecosystem and introduces particularly relevant types of actor. Section III provides an in-depth case study of cloud labs, as an example of an emerging actor in the biotechnology ecosystem that poses particular CBW proliferation risks and export control challenges. The case study unpacks the possible application of export controls during the different steps of using a cloud lab and explores challenges linked to the implementation and enforcement of controls, in particular controls on intangible transfers of technology (ITT) and software. Section IV first outlines the range of awareness-raising and outreach instruments used to engage with exporters. It then discusses good practices encountered in targeted outreach to actors in the biotechnology ecosystem, as well as how these activities and practices can be applied in ways that use synergies with biosafety, biosecurity and research security measures. The paper concludes with recommendations for the EU and its member states, and for AG participating states more generally, on how to address export control challenges posed by cloud labs and how to improve outreach practices and activities to strengthen awareness of new actors in the biotechnology ecosystem of CBW proliferation risks, export control obligations and appropriate compliance practices.

II. ACTORS IN THE BIOTECHNOLOGY ECOSYSTEM AND PROLIFERATION RISKS

The biotechnology ecosystem fosters innovation and new scientific and commercial solutions without conforming to the traditional dynamics and hierarchies of, for example, the pharmaceutical industry and its domination by major drug companies. Instead, new actors, including agile start-up companies such as cloud laboratories and bio-foundries, pursue innovative approaches. These approaches explore the convergence of biology, chemistry and emerging technologies using new business models and practices and rely on venture capital and innovation research and development funding. In the EU and worldwide, states are trying to foster biotechnology to address societal, scientific and environmental challenges—and to find commercial

[2] Research security refers to a range of measures to safeguard against risks related to openness and international collaboration with third countries in critical technology fields, such as undesired transfers, interference in or misuse of research and threats to research integrity. Héau, L., *The EU Research Security Initiative: Implications for the Application of Export Controls in Academia and Research Institutes* (EUNPDC: Stockholm, Mar. 2025).

[3] Brockmann, K., Bauer, S. and Boulanin, V., *Bio Plus X: Arms Control and the Convergence of Biology and Emerging Technologies* (SIPRI: Stockholm, 2019).

[4] Australia Group, 'Introduction', [n.d.]; and Australia Group, 'Objectives of the Group', [n.d.].

[5] Australia Group, 'Guidelines for Transfers of Sensitive Chemical or Biological Items', [n.d.]; and Australia Group, 'Common Control Lists', [n.d.].

[6] This paper combines two unpublished EUNPDC ad hoc briefs that the authors submitted and presented to the EU and the Australia Group during two webinars in March and May 2025.

success.[7] Conversely, the changing composition and volatility of the sector and the nature of its new entrants pose a range of CBW proliferation risks and challenges for export controls.

Proliferation risks linked to trends in the biotechnology ecosystem

Expansion and diversification of the biotechnology ecosystem

The convergence of biology, chemistry, AI and other emerging technologies is increasingly reflected in the composition of the ecosystem of actors participating in biotechnology development, the intersection, interaction and alignment of technologies, and the way scientific research is conducted as a result of these technologies and disciplines moving closer together.[8] In particular, AI and data science start-ups are increasingly involved in the development and optimization of biotechnology. For example, cloud laboratories specifically seek to marry advances in laboratory robotics, AI and bioinformatics to create greater efficiency, reduce prices and make advanced biological experiments accessible to an even wider range of global customers. The range of actors participating and thus emerging as CBW relevant dual-use technology holders is not only expanding but also becoming more diverse and therefore not as easily targeted by outreach efforts aimed at raising awareness of export control obligations.

Limited awareness of export controls and of proliferation risks in the biotechnology ecosystem

Established companies and larger professional research organizations in the chemical and biological sector generally have a high level of awareness of their compliance obligations, including those related to export controls and sanctions, as well as the underlying CBW proliferation risks and national security concerns.[9] The level of awareness, allocation of resources and quality of compliance structures among the range of new and non-traditional actors are often considerably lower—if they exist at all. Universities and other research organizations continue to struggle with the implementation of export control compliance functions. Actors pursuing novel business models for which the applicability of export controls is still unclear, such as certain digital service providers, similarly struggle to adopt appropriate internal compliance programmes (ICPs). The expansion and diversification of stakeholders that form part of the biotechnology ecosystem mean that there are more actors that have not been included in export control outreach activities conducted by national authorities, or have not engaged with the biosecurity measures and tradition of ethics codes of conduct developed by the biology and life science community.

Security risks and possible proliferation pathways involving actors in the biotechnology ecosystem

Biotechnology has been declared an economic priority by China, the EU and the United States and is thus increasingly the subject of geopolitical competition. Companies and research organizations in the biotechnology ecosystem might therefore become the target of illicit procurement activities by state and non-state actors. One specific group of stakeholders within the biotechnology ecosystem that could be a target of illicit procurement activities is on-demand service providers, such as cloud labs and bio-foundries (see section III). A state or non-state actor that is pursuing a chemical or biological weapons programme might lack the required equipment or wish to conceal its activities by using such services rather than building up its own capabilities. Service providers that offer facilities and assistance through AI agents aimed at making development and testing more efficient are particularly attractive.[10] While accessing technology and laboratory capabilities in this way would in most cases only assist with certain specific steps in a CBW programme, limited screening procedures might not currently deter a motivated actor that is able to conceal its identity and intentions.

Relevant actors in the biotechnology ecosystem

With commercial on-demand material, equipment, products and services on the rise in the biotechnology ecosystem, it is important to unpack the evolving range

[7] European Commission, 'Commission takes action to boost biotechnology and biomanufacturing in the EU', Press release, 20 Mar. 2024.

[8] Brockmann, Bauer and Boulanin (note 3); and Zakaria, S. et al., 'Machine learning and gene editing at the helm of a societal evolution', RAND, 23 Oct. 2023.

[9] See e.g. International Federation of Biosafety Associations, 'Biosecurity & biological nonproliferation', [n.d.].

[10] Palayer, J., 'Unpacking the concerns around AI and biotechnology', UNODA blog, [n.d.].

of relevant actors in the context of export controls and CBW proliferation risks. This section explores select types of actors that could be of particular interest for export control-related outreach, beyond established major companies and other actors with mature internal compliance functions.

Start-up companies

Start-up companies have become key actors in the biotechnology ecosystem over the past two decades, making significant advances in the fields of synthetic biology, gene editing and biochemistry. For example, Ginkgo Bioworks, a US start-up that originated at the Massachusetts Institute of Technology, used genetic engineering to develop a cell programming platform and has since expanded into lab automation, genomics and the extensive use of machine learning.[11] Increasingly, AI start-ups are also entering the ecosystem, offering solutions based on combining AI-enabled tools with biology and chemistry expertise. Using precision chemistry techniques, they are able to design, synthesize and test novel molecules using generative large language models (LLMs) and to identify novel compounds for drug discovery.[12] China, the EU and the USA are leading hubs for start-ups in the biotechnology ecosystem, but many other states, from Switzerland to South Korea, are also investing in these start-ups, and there are emerging capacities in states such as Saudi Arabia.[13] Some of these start-ups have grown rapidly, partnering with traditional pharmaceutical companies to become major actors in the innovation ecosystem.[14] Start-ups often have slim organizational structures and may not yet have established appropriate regulatory compliance and risk mitigation measures or may not have enhanced them in line with their growth and expanding capabilities.

Universities, innovation hubs and research institutes

A significant share of the scientific discoveries that form the basis of the work of biotechnology companies today originated from universities and other research organizations.[15] Many start-ups emerged from universities, research institutes and their innovation hubs to support the development of applied research and commercial applications in the life sciences.[16] Therefore, these research organizations are important targets and partners in awareness-raising that can inform scientists transitioning to start-ups and other activities for the commercial market. Research in many of these fields, such as on increased transmissibility or pathogenicity in humans and animals, can pose biosecurity and CBW proliferation risks.[17] There is a history of awareness-raising on biosafety and biosecurity—both through teaching curricula and dedicated training by safety and compliance officers—and early signs that this awareness may increasingly extend to AI and biotechnology advances.[18] However, universities and research organizations have experienced long-standing challenges in applying export controls to academic and research activities.[19]

DIY biotechnology community

DIY biotechnology, or bio-hacking, describes 'unconventional experimental biotechnology, often conducted outside traditional research environments and sometimes using everyday items or recycled equipment'.[20] Advances in biotechnology have enabled the growth of this community, which uses community laboratories or its own equipment to conduct genetic engineering and molecular biology experiments outside academia or companies.[21] This includes carrying out experiments with gene editing tools such as CRISPR, which has raised a range of safety and security concerns. At the same time, DIY biologists are increasingly exchanging their experiences and know-how internationally. Approaches developed by the DIY biotechnology community are being used in some start-up or academic settings to drive innovation.

[11] Gingko Bioworks, 'Power your R&D with Gingko', [n.d.]

[12] Synsilico, 'Tomorrow's AI applications. Today', [n.d.].

[13] See US National Security Commission on Emerging Biotechnology, Section 5.3,'Attract and Retain Trusted Foreign Talent' and Section 6.1 'Promote Biotechnology with US Allies and Partners', *Charting the Future of Biotechnology: An Action Plan for American Security and Prosperity*, Apr. 2025; 'Netherlands biotech ecosystem: Inside Europe's fast-growing innovation powerhouse', PharmaSource, 24 Jan. 2025; Wamda, 'Dammam Valley launches BioTech Startups Programme', Press release, 20 Feb. 2022; and Seoul Bio Hub, 'Seoul Bio Hub', [n.d.].

[14] Recursion, 'The story of Recursion', [n.d.].

[15] Zanders, J. P. et al., 'The Australia Group and the prevention of the re-emergence of chemical and biological weapons', Foundation for Strategic Research, 9 Apr. 2024.

[16] Karolinska Institute, 'Meet the current DRIVE companies', [n.d.].

[17] Fritsch, J. and Krätzner-Ebert, A., *Scientific Freedom and Security Interests in Times of Geopoltical Polarisation*, Joint Committee of DFG and Leopoldina on the Handling of Security-Relevant Research, Nov. 2024, p. 17.

[18] Responsible AI x Biodesign, 'Community values, guiding principles, and commitments for the responsible development of AI for protein design', 8 Mar. 2024.

[19] Héau (note 2).

[20] 'Focus on: Biohacking', *The Biologist*, vol. 63, no. 6 (2016), pp. 26–29.

[21] Gruber, K., 'Biohackers', *EMBO Reports*, vol. 20, no. 6 (June 2019).

For example, the University of Ottawa has established an augmented biology lab that operates on the model of a DIY lab by using unconventional methods to innovate in regenerative medicine and synthetic biology.[22]

Bio-foundries and cloud labs

Bio-foundries and cloud labs are two types of on-demand service provider that have emerged from the convergence of biotechnology, robotics and AI. Bio-foundries use highly automated, centralized facilities to perform specific steps in the biomanufacturing processes to streamline the design and manufacturing of biological systems.[23] Cloud labs offer a wide range of experiments and laboratory processes that researchers can order and control remotely, using the integration of automated robotic lab environments, increasingly with the use of AI.[24] This allows for flexibility in experiment design while also ensuring greater standardization and replicability.[25] Bio-foundries have been established in many AG participating states, as well as in China and Singapore.[26] The number of cloud lab facilities appears to be more limited. The first cloud labs emerged in the USA and the United Kingdom, followed by China, Canada and Singapore.[27] Research on automated laboratories is also ongoing in other countries, such as the Netherlands.[28] The first university-based cloud lab was set up at Carnegie Mellon University (CMU) in 2021 by a private company, Emerald Cloud Laboratory.[29] The CMU cloud lab is based on Emerald's commercial cloud lab platform.[30] Customers include established companies, as well as start-ups and researchers, which can benefit from the lower cost of experiments and access to a wide range of equipment.[31] The defence sector has also shown an interest in these companies by funding cloud lab and bio-foundry development and by becoming a customer.[32]

Cloud labs in particular provide an important case of an emerging actor in the biotechnology ecosystem that poses challenges for the application of export controls and could thus benefit from more targeted engagement through national export control outreach.

III. CASE STUDY: APPLYING EXPORT CONTROLS TO CLOUD LABORATORIES

Increasingly rapid developments in robotics, automation, AI and computational power are changing the way chemical and biological research is conducted and experiments are performed.[33] Facilities using modular robotic laboratory set-ups can increasingly execute many of the monotonous, yet precise and consistent, steps of laboratory ('wet lab') work. In several chemical and biological research fields, AI agents are becoming essential assistance tools for collecting data, identifying scientifically relevant patterns in large data sets and suggesting experiments.[34] In addition, lab work is being progressively enabled by AI for 'automating scientific workflows, optimizing simulation codes, operating instruments, and performing repetitive experiments'.[35] The facilities that integrate automated robotic lab environments with the use of AI are commonly referred to as cloud labs or 'self-driving laboratories' (SDLs). There is no generally accepted definition of, or distinction between, either term. Some use the terms interchangeably while others distinguish SDLs from cloud labs by the extent to which the use of AI allows for closed-loop research where the AI-enabled lab plans, executes, analyses and repeats experiment

[22] 'Focus on: Biohacking' (note 20).

[23] Arias, D. S. and Taylor, R. E., 'Scientific discovery at the press of a button: Navigating emerging cloud laboratory technology', *Advanced Materials Technologies*, vol. 9, no. 16 (2024).

[24] Arias and Taylor (note 23).

[25] Arias and Taylor (note 23).

[26] Global Biofoundry Alliance, 'Members', [n.d.].

[27] See e.g. Emerald Cloud Lab, 'Transcend the lab', [n.d.]; Culture Biosciences, 'Bioprocess development without the bottlenecks', [n.d.]; Automata, 'Hardware, software and expert support that empowers automation teams to build data powerhouses', [n.d.]; Synthace, 'More robust assays. Months off discovery biology.', [n.d.]; Arctoris, 'We understand our clients needs', [n.d.]; ATLATL, 'Open lab/analysis service', [n.d.]; 'ATLATL Innovation Center launches "Cloud Biolabs" R&D assembly line', Business Wire, 4 June 2020; and Jeffrey Lee, Y. et. al., 'Documenting cloud labs and examining how remotely operated automated laboratories could enable bad actors', RAND Expert Insights, Apr. 2025.

[28] See e.g. AI4 b-io, 'AI for self-driving laboratories', [n.d.].

[29] Global Biofoundry Alliance (note 24); and Carnegie Mellon University (CMU), 'AI at CMU', [n.d.].

[30] Arias and Taylor (note 23).

[31] Arctoris (note 27).

[32] PR Newswire, 'Ginkgo Bioworks and Transcriptic selected by DARPA to leverage robotic cloud lab and foundry automation to accelerate biological design with $9.5 M award', Press release, 12 Apr. 2018.

[33] Pauwels, E. and Dunlap, G., 'The intelligent and connected bio-labs of the future: Promise and peril in the fourth Industrial Revolution', Wilson Briefs, 7 Sep. 2017.

[34] Luckey, D. et al., *Mitigating Risks at the Intersection of Artificial Intelligence and Chemical and Biological Weapons*, RAND Research Report (Homeland Security Operational Analysis Center, RAND Corporation: Arlington, VA, 28 Jan. 2025).

[35] Luckey et al. (note 34).

Box 1. What are cloud laboratories?

In simple terms, cloud labs are facilities that allow scientists to run experiments remotely in fully (or mostly) automated laboratories. Cloud labs give the user the ability to access software (via an application programming interface) to design experimental protocols that are then translated into machine-readable code. Physical samples or reagents can be sent in by the user, ordered from other companies or provided by the cloud lab provider to be placed in an otherwise fully automated robotic lab set-up, which will then run the experiment remotely according to the encoded instructions. The data generated by the experiment is then uploaded to cloud-based storage that the users can access from anywhere at any time through the software interface.[a]

Cloud labs can improve the speed, scale and reproducibility of scientific experiments through the automatic generation of standardized experimental protocols. This means that cloud labs can lower the barriers to scientific collaboration and exchange, make access to specialized equipment, instrumentation and materials easier, and lower some barriers of specific expertise and tacit knowledge.[b]

[a] Carnegie Mellon University (CMU), 'Automated science at CMU', Oct. 2021; and Krin. A. and Jeremias, G., 'Artificial intelligence: Possible risks and benefits for BWC and CWC', CBWNet Working Paper no. 5, July 2023.

[b] Arias, D. S. and Taylor, R. E., 'Scientific discovery at the press of a button: Navigating emerging cloud laboratory technology', *Advanced Materials Technologies*, vol. 9, no. 16 (2024), pp. 2–4; and Lentzos, F. and Invernizzi, C., 'Laboratories in the cloud', *Bulletin of the Atomic Scientists*, July 2019.

cycles to achieve predefined objectives.[36] This paper uses the term cloud labs to describe all labs offering modular automated lab operations as a service and discusses the extent to which they use AI where it is relevant to CBW proliferation risk or export control-related considerations. Cloud labs are poised to make significant contributions to biology and chemistry, including through advances in drug discovery and by making the ability to conduct research in these fields more accessible and, depending on the context, faster and cheaper. However, these rapidly developing applications could also pose significant security challenges since they might be misused for the development of CBWs, particularly by actors that would not otherwise have access to sophisticated equipment and specialized material.

CBW proliferation scenarios involving cloud labs

Some of the most attractive features of cloud labs—such as the ability to improve the reproducibility and pace of scientific experiments, to lower the barriers to access to specialized equipment, software, materials and knowledge, and to outsource development capabilities—risk being exploited by actors that aim to develop CBWs. Notably, the possible contribution that use of a cloud lab might make to development and testing only relates to one step in the process of obtaining a chemical or biological weapon. Weaponization and scaling-up of production will continue to provide significant hurdles and further aspects for non-proliferation measures to target.

Furthermore, there are differences in the contribution that the use of cloud labs could make to developing CBWs, depending on whether the contribution is to a weapons programme of a state or a non-state actor. A state actor without access to the advanced lab infrastructure required for a sizeable chemical or biological weapon programme and with only a small research and development team could significantly increase its development capabilities by making use of a cloud lab. A covert state programme could conceivably hide more easily behind a legitimate national university or research institute requesting to use the cloud lab. Other measures that states might take at the domestic level in order to access and make use of cloud lab technology to develop CBWs could include requiring civilian companies to make relevant technology available to them, or funding or acquiring private sector companies, for example start-ups, with a view to gaining access to the required know-how.[37] Alternatively, states might seek to exploit foreign technology by pursuing 'seemingly benign scientific cooperation' with academic institutions in other states or through theft conducted via cyberattacks.[38] Cyberattacks could also target the sensitive data generated by experiments conducted by cloud labs and stored and managed by the cloud software.[39]

[36] Mayer, T. et al., 'Workshop to Build a Vision and Strategy for Creating a National Network of Academic Cloud and Self-Driving Labs', 23–25 Oct. 2023, pp. 4–5.

[37] Blum, M., 'Artificial intelligence and chemical weapons', eds T. Reinhold et al., *Artificial Intelligence, Non-Proliferation and Disarmament: A Compendium on the State of the Art*, Non-Proliferation and Disarmament Papers, no. 92 (Jan. 2025), p. 13.

[38] Blum (note 37), p. 13.

[39] Arias and Taylor (note 23), p.8.

A non-state actor pursuing a CBW programme with limited resources and seeking to minimize the footprint of its operation in order to conceal it could make use of a cloud lab to minimize the need for qualified personnel and reduce the time required for the development and testing cycles for selecting a biological or chemical agent. Using a cloud lab to produce large quantities of, for example, a toxic agent is likely to increase the chance of detection, but small amounts could potentially be concealed among a larger number of other experimental products.

It should be noted that any actor intending to use cloud labs to develop a biological or chemical weapon faces significant obstacles, particularly if the weapon is intended to cause mass destruction rather than disruption. These obstacles include, for instance, 'access to critical materials and equipment, methods for effective dissemination of agents, programme-related costs, and importantly also, tacit knowledge'.[40] More generally, the misuse of cloud labs, especially by non-state actors, is likely to be limited by a number of factors that also apply to other AI tools that find application in the biochemical field, such as the lack of complete and accurate training data, the sparsity of data on failed experiments and the difficulty in accessing specialized data sets.[41] It is highly unlikely that a cloud lab could be used for military-scale production of CBW agents without detection. This means that the potential contribution for which malevolent actors might seek to exploit cloud labs is likely to be confined to the development and testing stages of a CBW programme.

The current status of development of cloud lab technology also presents some limitations that can act as barriers to potential misuse. While the use of cloud labs may in the longer term reduce the requirement for wet lab experience and understanding, such knowledge is currently still needed, for instance, to properly define the objectives of the experiment or to optimize the experiment and understand likely points of failure.[42] In addition, lab work experience is still necessary since cloud labs are unable to provide an alternative to live and in-person monitoring of experiments, which allow for more frequent quality checks and earlier diagnosis of possible mistakes.[43] Finally, there are still some gaps in the techniques and tasks that cloud labs can perform due to a lack of the required automated robotic systems.[44]

The application of export controls to the use of cloud labs

Given the risk scenarios explored above, and particularly the notion that cloud labs might potentially provide a state or non-state actor with a reduced footprint and decentralized CBW development capacity, it is important to consider how export controls could apply in the course of an actor using a cloud laboratory (see figure 1). This section focuses on the applicability of export controls as prescribed by the AG guidelines and the common control lists as implemented through the EU dual-use regulation.[45] Export controls may be applied to transfers of both tangible and intangible items, covering goods, software and technology, as well as cases where technology is transferred or made available by way of technical assistance. This concerns not only transfers from the cloud lab user to the provider but also transfers from the cloud lab provider to the user. The AG lists a wide array of human and animal pathogens and toxins, plant pathogens and chemical weapon precursors, as well as dual-use biological and chemical equipment and related technology and software, and chemical manufacturing facilities that participating states commit to make subject to their export controls. Licensing requirements may also apply to exports of non-listed items if it is suspected that they are destined for a CBW programme.

Cloud labs offer a wide array of different automated wet lab and analytical processes. Some of the equipment made available for use by cloud labs might be listed by the AG. Cloud labs also increasingly offer advanced software solutions for the encoding

[40] Spiez Laboratory, *Spiez Convergence: Report on the Third Workshop, 11–14 September 2018* (Spiez Laboratory: Spiez, Nov. 2018), pp. 9–10.

[41] Lentzos, F., 'Artificial intelligence and biological weapons', eds Reinhold et al. (note 37); Luckey et al. (note 34); Krin. A. and Jeremias, G., 'Artificial intelligence: Possible risks and benefits for BWC and CWC', CBWNet Working Paper no. 5, July 2023; and Moon, J. R. et al., *Impacts of Artificial Intelligence on the CBW Prohibition Regimes: Analysis, Challenges, and Futures* (Harvard Sussex Program: Brighton, 31 Mar. 2024).

[42] Luckey et al. (note 34); Krin and Jeremias (note 41); and Arias and Taylor (note 23), pp. 5–8.

[43] Arias and Taylor (note 23), pp. 5–8.

[44] Arias and Taylor (note 23), pp. 5–8; and Luckey et al. (note 34).

[45] The EU dual-use regulation combines the AG's common control lists with the controls of the other multilateral export control regimes into one list of controlled dual-use items. It has been adopted or used as a template by many states outside of the AG, particularly those that are partners in EU dual-use export control capacity-building programmes. The paper discusses notable divergences with other states' application of export controls.

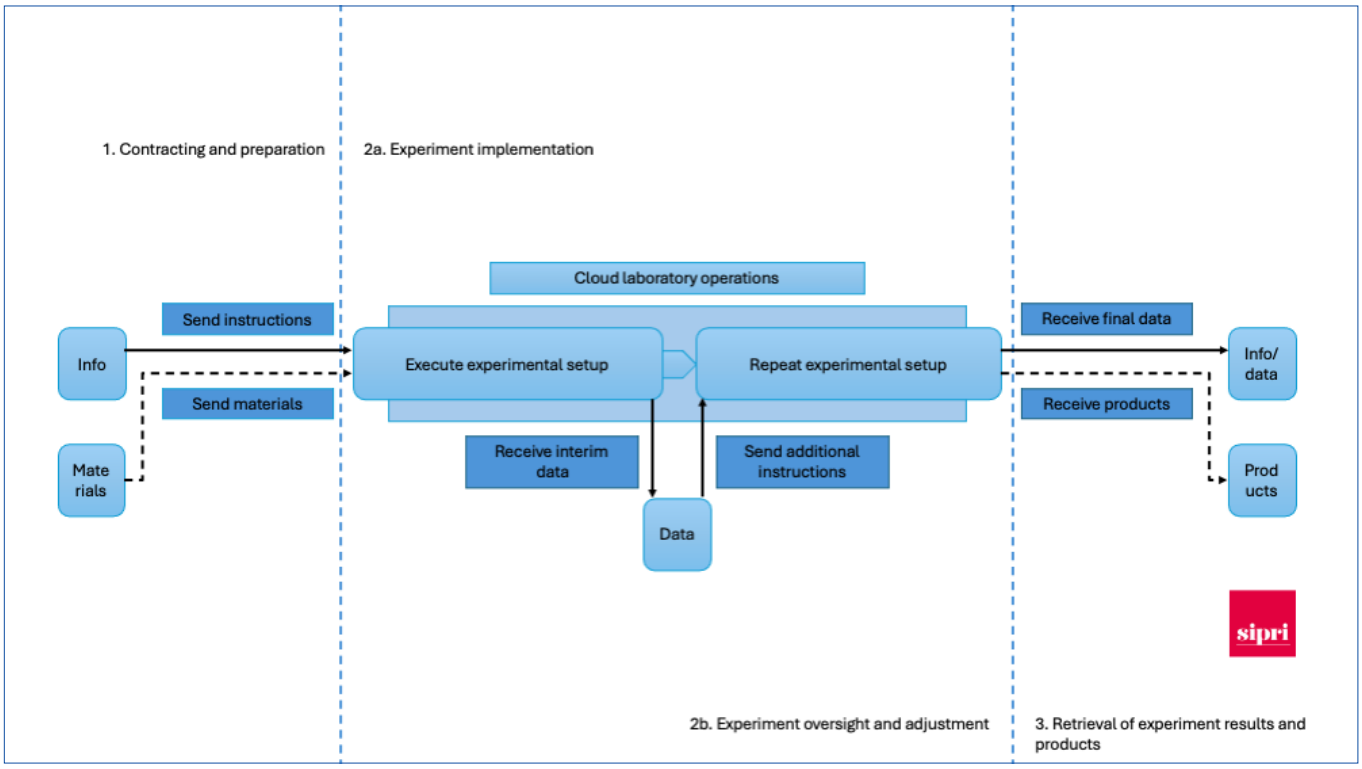

Figure 1. The cloud laboratory process

Source: Graphic created by the authors.

of experiment steps and provide analytical tools, including predictive algorithms and LLMs. Depending on the desired experiment and process, these can help to significantly reduce the number of iterations of an experimental set-up that need to be run, for example, to characterize a toxic chemical or optimize the molecular formulation of a chemical to achieve certain properties. Some of the software made available as part of these processes may also be subject to export controls.

The cloud lab process

For the purpose of considering the applicability of export controls, it is helpful to divide the process of using a cloud lab up into different steps and consider the applicability of export controls at each stage of the process. These steps are summarized below.

Step 1. Contracting and preparation

Any actor that wishes to use a cloud lab is generally required to create a profile by providing personal information, a commercial or academic affiliation and payment information. The user then commonly engages with an interface on the cloud lab provider's website to use its software to plan out in detail the experimental set-up the user wishes the cloud lab to perform and the parameters that should be observed. In advanced cloud lab set-ups, the user may also use the provider's software to add a layer of deductive or predictive analysis, for example, by using an LLM to adjust the experimental set-up or certain input parameters in iterative experimentation cycles. In addition, the user may send physical samples of the chemicals or biological materials to be used, characterized or otherwise analysed in the contracted experiments to the cloud lab. In other cases, staple biological or chemical materials provided by the cloud lab provider will be used to run the experiment.

Step 2a. Experiment implementation

Using the samples sent to the cloud lab, or samples provided by the cloud lab provider, the automated cloud lab runs the experiment as encoded by the user.

Step 2b. Experiment oversight and adjustment

Many cloud labs make the data on experiments available to the user in near-real time through the user interface or in the form of interim experiment result reports. The user is often also able to adjust the experiment or provide additional instructions.

Step 3. Retrieval of experiment results and products

Once all the contracted experiments have been concluded, the data collected from the experiments is collated into a report transmitted to, or made available for download by, the user. In certain cases, experimental products may also be shipped back to the user.

Relevant types of export

Each of the steps outlined above may involve the transfer, or making available of, tangible or intangible items subject to a licensing requirement.

Transfers of physical goods

Using the services of a cloud lab for chemical or biological lab work may involve the transfer of goods to and from the location of the lab. If the cloud lab is located in a third country, the transfer of a listed chemical precursor, plant pathogen or human or animal pathogen or toxin from the user to the cloud lab provider in step 1 could constitute an export that requires a licence. A licence may also be required if the items are unlisted but a catch-all control applies—that is, if the user is aware or has been informed by the responsible export licensing authority that the items might be destined for the development of, or use in, a CBW programme. Conversely, if the cloud lab provider transfers any products or samples back to the user in step 3, an export licence might be required if these items are listed or a catch-all control applies.

Intangible transfers of technology

The AG control lists define technology as '[s]pecific information necessary for the "development", "production" or "use" of a product'. This information can take the form of 'technical data' or 'technical assistance' (see below), where technical data is described as 'blue-prints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories'. Exemptions generally apply for a transfer of technology that is 'basic scientific research' or information 'in the public domain'.[46] In the case of cloud labs, any transfers of technology are more likely to involve intangible transfers rather than transfers of physical items. Transfers of technology that may be subject to controls take place at each step of the process. For example, transferring the collective coding for the lab tasks to be performed in step 1 could, but is unlikely to, amount to information required for the development of chemical or biological weapons. Both the transfer of intermediate data from the lab to the user and the sending of additional tasking could also be considered a transfer of technical data subject to control. Finally, this also applies to the transfer of the final data set on the experiment and any analytical assessment provided by the cloud lab, for example, through the application of machine learning- or LLM-enabled software. In most cases, the technology produced by a cloud lab, such as an optimized DNA sequence or molecular structure, will be a research product at a low technology readiness level (TRL 1–3), and could thus come under the basic scientific research exemption. It is important to note that whether information constitutes controlled technical data is highly case dependent and necessitates several checks, such as whether the information meets the threshold of 'required' for the development of CBWs.

Intangible transfers of software

The AG control lists define software as a 'collection of one or more "programmes" or "micro-programmes" fixed in any tangible medium of expression'.[47] Software for the operation of cloud labs is not explicitly listed on any of the AG chemical or biological equipment-related control lists. However, the dual-use chemical manufacturing facilities and equipment list does include 'dedicated software' related to toxic gas monitors and monitoring systems. In addition, the dual-use biological equipment list includes software designed for nucleic acid assemblers and synthesizers. Software that uses proprietary machine-learning algorithms and LLMs to optimize protein structure prediction or to perform generative design of virtual molecules with desired properties might also be subject to export controls in some states.

With regard to software, a key issue for labs and enforcement bodies to consider is whether making available (rather than transferring) controlled software is subject to export controls. Most cloud lab providers do not transmit their software to their users but rather make the software available to them through a web-based interface and run it from cloud servers where it is stored with the data collected from

[46] Australia Group, 'Common Control Lists' (note 5).

[47] Australia Group, 'Common Control Lists' (note 5).

all the experiments performed by the cloud lab. If the software is classified as controlled, granting access to it essentially means that it is being made available using the software-as-a-service (SaaS) model. States differ in their interpretation of the definition of export in ways that mean that the extent to which controls apply to making software available via the SaaS model varies.

Provision of technical assistance

The AG control lists posit that 'technical assistance' may take forms such as 'instruction, skills, training, working knowledge, consulting services', includes 'oral forms of assistance' and 'may involve transfer of technical data'.[48] The definition adopted by the EU dual-use regulation and most AG participating states is somewhat broader and refers to 'any technical support related to repairs, development, manufacture, assembly, testing, maintenance, or any other technical service', but refers to the same forms of assistance.[49] Provision of automated laboratory services does not readily fit the definitions provided. However, it is worth considering whether the provision of such services and analytical capabilities could be interpreted as providing technical support related to development or testing for the purposes of a CBW programme. Another question is whether the user only interacts with the software interface provided by the cloud lab provider or whether there is additional instruction on the use of the cloud lab or assistance with designing the experiment set-up by staff at the cloud lab provider. At least in the latter case, clarification would be needed, depending on the circumstances of the case, of whether the cloud lab provider might be providing technical assistance that requires a licence.

Challenges to using export controls to prevent cloud labs from contributing to CBW programmes

Export controls have traditionally been the main tool through which states have sought to detect and prevent transfers of goods and technologies that might enable a state or non-state actor to develop a chemical or biological weapon. However, the extent to which export controls might provide oversight and a means of intervention in cases where the use of a cloud lab would play an enabling role is limited, in particular because of the limited applicability of export controls to the types of transfer and provision of services involved in the use of a cloud lab. Even where there are applicable export controls, their effective application is constrained by divergences in states' interpretations of key provisions, such as the application of controls on intangible transfers of technology and software, and difficulties for the parties involved to exercise effective due diligence and ensure compliance.

Effective controls on intangible transfers of technology

Controls on ITT are notoriously difficult to implement. Furthermore, differences in the interpretation of key legal provisions, as well as a lack of clear guidelines on their application and on the application of the exemptions for basic scientific research and information in the public domain, mean that there is far from a level playing field, even among AG participating states. Particularly if the desired experiment set-ups do not require the transfer of any goods to the cloud lab location and no products need to be retrieved, those parts of the development and testing process can be entirely shifted to digital transfers of data, which would make preventive detection by enforcement agencies even more difficult. Another difficult aspect of compliance is classifying whether the information provided by the user to set up the experiment (or lab task) or the data sets gathered and analysed during the task runs constitute controlled technical data.

Regardless of how a state frames its controls and interprets key concepts, including what constitutes an export, it must consider whether these allow it to exercise an appropriate and sufficient level of oversight of intangible transfers, services and transactions involving cloud labs to reduce the risk of cloud labs contributing to CBW programmes.

Compliance and resilience to illicit procurement attempts

Complying with the ever-changing regulatory environment—in particular export controls and sanctions—can be difficult for companies and requires considerable resources to be assigned to building effective compliance systems. The industry standard is to set up an ICP that outlines responsibilities, procedures, staff training and regular reviews. Staff training at cloud lab providers in particular could help to raise awareness, reduce the risk of inadvertently

[48] Australia Group, 'Control List of Dual-use Chemical Manufacturing Facilities and Equipment and Related Technology and Software', 30 June 2023.

[49] Regulation 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), *Official Journal of the European Union*, L206, 11 June 2021.

assisting a procurement attempt and improve resilience. The Nuclear Suppliers Group, the Wassenaar Arrangement and the EU have each published good practice or guidance documents on ICPs, but the AG has thus far not compiled such public guidance.[50]

Media reporting and articles in professional journals on possible security concerns related to the operation of cloud labs have raised a certain level of awareness among providers and led at least some to introduce screening protocols for the types of experiments tasked.[51] However, distinguishing between an actor seeking to conduct a legitimate series of experiments using a cloud lab and an actor attempting to conduct concealed development and testing steps for a covert CBW programme is inherently difficult. Beyond the use of listed precursors and listed pathogenic or toxic agents, and particularly so where the work involves the development of novel agents with certain characteristics, there are few indicators or red flags that companies can use. This poses the question of what an appropriate level of due diligence would be for cloud lab providers to exercise and if approaches such as the know-your-customer principle can reasonably be applied. Even if customers are required to provide a commercial address and an affiliation with a university or other research organization, it is unclear to what extent this information could be verified and screened. In most cases, this would probably be more of a hurdle for a non-state actor than for a state or a state-sponsored non-state actor.

Effective application of catch-all controls

The effective use of catch-all controls to impose licensing requirements on exports of unlisted items where the national licensing authority or the exporter has knowledge of a possible CBW end-use is inherently dependent on intelligence information or information collected by the exporter, in this case the cloud lab provider. Particularly in industry sectors where there is limited awareness or understanding of proliferation risks, and where compliance functions may only be equipped with very limited resources, such as in start-up companies, it is less likely that there will be sufficiently resilient compliance functions in place that could identify an actor seeking to conceal the intended end-use of its tasked lab work. Proactive outreach to cloud labs and related service providers could raise the level of awareness of (and sensitize them to look out for) possible misuse of their services and of their potential export licensing obligations.

Enforcement

In automated laboratories, every action and analytical process applied is coded and recorded in a protocol, together with the entirety of the data generated. In cases where transfers have taken place without the required licences, this data can provide evidence for investigations using digital forensics. In many states, however, criminal liability for violations of export controls is dependent on demonstrating intent on the part of the exporter. Without human involvement in the experiment beyond the initial coding and potentially some intermediate adjustments to the set-up, proving intent to contribute to a CBW programme (and circumvent controls) when contracting a cloud lab to perform certain experiments might prove difficult. If the cloud lab provider were to provide specific assistance to optimize a lab tasking or to avoid specific controlled materials or tasks that would require additional screening, this could be construed as evidence of intent. Proactive outreach to cloud labs about their potential export control obligations would be a way to demonstrate that they are aware of these obligations and therefore cannot claim to have been unaware of the need to put compliance procedures in place.[52]

IV. NATIONAL EXPORT CONTROL OUTREACH TO CLOUD LABS AND OTHER ACTORS IN THE BIOTECHNOLOGY ECOSYSTEM

As the case of cloud labs demonstrates, new actors in the biotechnology ecosystem using new business models and practices may face significant uncertainties over the application of export controls and appropriate compliance procedures. The use of national export

[50] Wassenaar Arrangement, 'Best Practice Guidelines on Internal Compliance Programmes for Dual-use Goods and Technologies', 2011; Nuclear Suppliers Group, 'National practices', [n.d.]; and European Commission, 'Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items', *Official Journal of the European Union*, L338/1, 23 Sep. 2021.

[51] Lee, Y. J. and Del Castello, B., 'Robust biosecurity measures should be standardized at scientific cloud labs', RAND Commentary, 8 Nov. 2024.

[52] Bauer, S. and Bromley, M., *Detecting, Investigating and Prosecuting Export Control Violations: European Perspectives on Key Challenges and Good Practices* (SIPRI: Stockholm, Dec. 2019).

control outreach to better inform such actors is therefore a crucial element in reducing resulting proliferation risks. States use a range of tools to conduct export control outreach to industry, from active engagement and dialogue with relevant stakeholders to the provision of guidance materials, frequently asked questions (FAQs) webpages and dedicated communications channels, such as specific email contacts or inquiry hotlines.[53] Outreach activities aim to raise awareness of both risks and obligations and to help with the implementation of appropriate ICPs, due-diligence procedures, internal staff training and other relevant measures. National export licensing authorities are usually responsible for conducting export control-related outreach. Ministries that deal with the economy, commerce, business, trade, defence or foreign affairs—and in this case biosecurity and safety—can also play a role. Export control is only part of the wider regulatory framework, which includes biosafety, biosecurity and research security measures, that ensures states have a level of oversight over the activities carried out by actors in the biotechnology ecosystem and that these actors are aware of the security risks linked to their actions. Targeted export control outreach and awareness-raising should therefore use synergies with the practices and activities of these related instruments.

The toolbox of national outreach and awareness-raising instruments

Awareness-raising and outreach enable states to support stakeholders preventively, rather than strictly rely on the enforcement of export controls through licence denials, investigations and penalties to promote and strengthen compliance and reduce the risk of export control violations taking place. Canada's 2014 evaluation of its biosecurity system, for example, found that awareness-raising was more cost effective at achieving regulatory compliance by stakeholders.[54] Awareness-raising is most beneficial when it takes the form of a dialogue between states and relevant stakeholders in which both sides feel comfortable sharing experiences and concerns. States have therefore developed a whole toolbox of instruments that they can use to enter into a dialogue with industry and other relevant stakeholders to raise awareness.

Export control compliance conferences for industry and research organizations

Most states organize annual or more regular conferences or seminars on export controls that provide at least regulatory and policy updates from the relevant national authorities and agencies, and an opportunity to engage with the regulator. Some states organize such conferences for companies and research organizations combined, while some host a separate event for the latter. Flagship public-facing events can help raise the profile of export control compliance and demonstrate that the national authorities are seeking engagement with stakeholders. However, such events might also be perceived as exclusive and expensive and can become meetings of the larger, established companies. Major conferences organized by national licensing authorities are important engagement opportunities and have their place in a national outreach strategy, but they may need to be supplemented with more targeted outreach, particularly to reach the entirety of the diverse biotechnology ecosystem.

Export control authority engagement with industry and research organization associations

Industry associations and associations of research organizations are key interlocutors and can act as 'multipliers' in export control awareness-raising and outreach efforts. Associations can provide forums that regulatory authorities can use to interact with a large group of actors from a specific sector or ecosystem, identify and address common questions and concerns, and disseminate relevant information and guidance materials. This can help reduce the need and requests for bilateral meetings with companies and other actors while still providing an environment in which actors are more comfortable with sharing uncertainties, highlighting any unintended adverse effects of regulations, such as impacts on international competitiveness, and providing other specific feedback. Engaging with stakeholders at the level of compliance professionals and export control officers is particularly valuable as they are most likely to be the most pertinent company representatives and to have the strongest effect in terms of raising awareness and helping actors

[53] Brockmann, K. and Héau, L., 'Developing good practices in export control outreach to the NewSpace industry', SIPRI Insights on Peace and Security, no. 2023/04 (Mar. 2023).

[54] Government of Canada, Evaluation Directorate Health Canada and Public Health Agency of Canada, 'Evaluation of the Biosecurity Program 2009–10 to 2013–14', Mar. 2014.

to improve their export control compliance systems and practices.

Provision of targeted guidance materials

In guidance materials, national authorities can provide detailed information in one place on export control policies, regulatory requirements, good practices for ICPs and case studies, as well as contact information and links to relevant sources. Almost all states publish general export control guidance materials for all actors, including on ICPs, but targeted or sector-specific guidance materials are less common. Constraints on the resources required for the creation and regular updating of targeted guidance materials mean that unless the biotechnology industry plays a very significant role in a state's economy, it might not choose to develop sector-specific guidance materials. An alternative option is to provide guidance that addresses specific types of actors or characteristics of exporters that pose challenges across different sectors, or that includes cases or examples that speak specifically to common questions from actors in the ecosystem. Developing guidance on ICPs specifically for start-ups or that addresses controls on ITT, including cloud computing and SaaS, might be particularly relevant for key actors in the biotechnology ecosystem.

Assigning export control authority resources to respond to inquiries

Guidance materials are a useful resource for stakeholders but they cannot address all the questions that could arise from a particular licensing application or where companies feel that their business model is new and are uncertain about how export controls apply.[55] Both the guidance materials and the FAQs sections that are displayed on licensing authorities' websites should clarify when an individual inquiry or company visit might be appropriate, so that basic, repetitive or inadmissible inquiries can be reduced. This can also help actors in the biotechnology ecosystem to discern when their inquiries may be more appropriately directed to an authority responsible for biosecurity or where they need to engage with the export licensing authority. In other cases, direct exchanges with licensing authorities, to the extent that the limited resources available permit in terms of personnel and time, can be very useful for addressing specific queries.

[55] Brockmann and Héau (note 53).

Good practices for outreach and awareness-raising with cloud labs and other actors in the biotechnology ecosystem

Fitting the right tools for outreach to specific types of actor, including those in the biotechnology ecosystem, can depend on many factors, such as the composition, size and awareness levels of stakeholders. Identifying relevant domestic stakeholders is a first step to developing a more targeted outreach programme, which can then prioritize the actors that are of the greatest interest, for example due to the type of technology they are developing or intelligence regarding illicit procurement activities. States should use outreach to raise awareness about both the rationale underlying export controls and the role and focus of effective screening mechanisms. It can also be an opportunity to raise concerns about specific recipients, illicit procurement agents' modus operandi and the interpretation of regulations.[56] Outreach partners, in turn, can provide national authorities with valuable information about developments in biotechnology, the impact of regulations on international competitiveness, the overall development of the biotechnology sector and any suspicious inquiries or procurement attempts.[57] The following are good practices that states have identified while conducting outreach with actors in the biotechnology ecosystem or similarly innovative sectors, or general export control outreach to industry and research organizations.

Identifying relevant domestic stakeholders

If states are to select suitable awareness-raising and outreach instruments and assign the appropriate amount of resources to use them effectively, they must have an understanding of the size and nature of their domestic biotechnology ecosystem.[58] A comprehensive mapping of relevant actors should include the full range of actors mentioned above. Consulting existing or conducting new market research or industry surveys is one way to gauge the size and nature of a state's domestic biotechnology ecosystem but this may need to be supplemented with engagement with DIY biotechnology forums. The results of such mapping

[56] Viski, A. and Jones, S., 'Outreach 2.0: Emerging technologies and effective outreach practices', Strategic Trade Research Institute, Washington, DC, Feb. 2021, pp. 10–11.

[57] Viski and Jones (note 56), p. 10.

[58] Viski and Jones (note 56), p. 12.

can help a state to decide whether it would be more efficient, for example, to set up a dedicated awareness seminar for actors from the ecosystem, or that targeted individual outreach to a small number of companies might be appropriate. One option for states that do not have the resources to perform a full mapping would be to conduct compliance audits with select companies in the ecosystem, as it can help reveal other relevant parties involved in transfers.[59] If those parties have not previously engaged with the authorities, applied for licences or been audited, they can be requested by letter to provide information on their activities or lined up for future compliance audits.

Engagement with cloud labs and bio-foundries

In countries where they are already established or currently under development, cloud lab service providers and bio-foundries are two stakeholders for which more targeted outreach may be particularly beneficial. Proactive outreach to these actors could raise the level of awareness of (and sensitize them to) possible misuse of their services, and of their export licensing obligations. Cloud labs are still emerging as a new actor in many states and early engagement could be particularly impactful. This would help to ensure that as these types of services expand, the main actors also increase their level of awareness of risks and compliance with applicable regulations. For example, in the USA cloud labs have reported that collaboration with national authorities enabled them to strengthen vetting procedures for customers and security measures for experiments, to prevent the misuse of cloud lab facilities contributing to the development of CBW.[60] It would also help to establish strong compliance as an industry standard and a sign of the quality of a provider.

Incentivizing biotechnology start-ups to participate in outreach activities

Even when states or other outreach providers—sometimes including think tanks and industry associations—know which stakeholders they would like to invite to outreach events, they can struggle to reach and convince biotechnology start-ups, laboratories and other companies to bear the cost of sending representatives. It is therefore important to communicate the benefits of participation in outreach activities. Biotechnology start-ups can strengthen their awareness and understanding of compliance obligations but, perhaps more importantly, also have an opportunity to discuss specific cases and questions about their business model with regulators. They can in turn provide information to the national authorities about the way their technology works and the measures they have put in place to reduce possible risks, thereby demonstrating their credentials as responsible actors. Other benefits include the opportunity to share their experiences with other stakeholders and build a community of peers. It is important to normalize and create an environment for genuine engagement with the authorities by showing an understanding of the challenges experienced by start-ups and a willingness to work with them to improve their practices to increase the uptake of such dialogue offers. Similarly, biotechnology projects with a dual-use dimension taking place in innovation hubs transitioning into the start-up space should receive biosecurity and export control compliance training from the hosting university and be encouraged to participate in outreach events.

Building on awareness and self-regulation in the biosecurity community

Efforts to strengthen dedicated outreach and awareness-raising activities for the biotechnology ecosystem should build on the achievements of the biosecurity community in raising awareness of misuse and biological weapon proliferation risks and exercising responsible science and development. In emergent fields such as synthetic biology there have been dedicated efforts to build on the discourse in the biological arms control community, which have resulted in proactive and self-regulatory measures being initiated by industry. For example, in 2009 several gene-length synthesis companies formed the International Gene Synthesis Consortium (IGSC) to act as a focal point for discussions and the development of good practices and dedicated screening measures.[61] The consortium has since grown to comprise companies that provide up to 80 per cent of the global capacity for the supply of commercial

[59] Interviews conducted by the authors with representatives of national licensing authorities.

[60] National Academies, 'Artificial Intelligence and Automated Laboratories for Biotechnology: Leveraging Opportunities and Mitigating Risks', A workshop, 3–4 Apr. 2024, 2:09:36–2:11:30.

[61] International Gene Synthesis Consortium, 'Harmonized Screening Protocol v3.0', 3 Sep. 2024, pp. 1–2.

gene-length synthetic DNA.[62] The IGSC's harmonized screening protocol takes account of major regulatory developments affecting the gene synthesis industry and provides good practices on screening procedures, the application of the 'know your customer' principle and means for confirming end-use.[63] Notably, a major cloud lab provider and several bio-foundries are among the current members of the IGSC. Parts of the DIY-bio community have already formulated responsible practices through self-regulatory codes of conduct. Initiatives to develop and maintain such codes could be supported by national authorities through the provision of information materials, input and expertise, and help to facilitate engagement particularly with national technical experts and officials with a background in science.

Export control authority participation in national biosecurity programmes and events

Many states have national biosecurity programmes or initiatives that work to inform actors conducting research, development and other work that must comply not only with biosafety, but also with biosecurity requirements. While biosecurity does not specifically relate to export control compliance, it is an important tool that raises awareness of security and ethical concerns that might apply to much of the work in the biology, pharmaceutical and life sciences sectors. Such programmes are often much more closely connected and networked with the actors in this area than export licensing authorities. Some states assign officials working on export controls to participate in programmes organized by biosecurity offices and make periodic presentations on export controls at biosecurity events. This allows them to monitor developments in this area, identify relevant actors and be available to raise awareness and respond to export control-related questions, while also directing particularly relevant companies and other actors to more export control-focused activities.

Sensitizing biotechnology start-ups to risks linked to foreign direct investment

Targeted outreach to biotechnology start-ups should include awareness-raising of the risks associated with transfers or making available dual-use technology as part of foreign direct investment (FDI) or acquisitions. National FDI screening mechanisms and export controls are distinct but indirectly linked policy tools, as FDI screening draws on export control lists as part of selecting which cases to screen. The use of FDI screening mechanisms is growing and biotechnology has been identified as a key sector to monitor. The European Commission proposed a revision of the EU's FDI screening regulation in 2024, requiring all member states to adopt FDI screening mechanisms and extending their scope to include biotechnologies, among other 'critical technology areas'.[64] Several states have argued that coordination between, if not the involvement of, the national authorities responsible for FDI screening would improve efficiency, reduce confusion about perceived overlaps of regulatory obligations and improve awareness.[65]

Exploring synergies with research security efforts

In response to growing national security and economic security concerns related to science and innovation in critical fields, an increasing number of states, including in the EU, are adopting measures to strengthen research security.[66] Research security is particularly relevant for biotechnology, which has been identified as a critical technology field by the EU and others.[67] There are clear synergies between research security and export controls that states could take advantage of when conducting outreach on both sets of issues, and related tools to leverage the limited resources available. For example, strengthening the application of controls on ITT among research organizations is also likely to be beneficial for the key aims of research security.

[62] International Gene Synthesis Consortium, 'About', [n.d.]; and PR Newswire, 'International Gene Synthesis Consortium updates screening protocols for synthetic DNA products and services', Press release, 3 Jan. 2018.

[63] International Gene Synthesis Consortium (note 63), pp. 5–18.

[64] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the screening of foreign investments in the Union and repealing Regulation (EU) 2019/452 of the European Parliament and of the Council, COM(2024) 23 final', 24 Jan. 2024; and European Commission, 'Commission Recommendation of 3 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States', 2 Oct. 2023.

[65] Interviews conducted by the authors with representatives of national licensing authorities.

[66] Héau (note 2); and Council of the European Union, 'Council recommendation on enhancing research security', 9097/1/24, 14 May 2024.

[67] Australian Government, Department of Industry, Science and Resources, 'List of Critical Technologies in the National Interest', 19 May 2023; and European Commission, 'Annex to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with member states', C(2023) 6689 final, 3 Oct. 2023.

V. CONCLUSIONS AND RECOMMENDATIONS

The expanding and diverse set of actors that is the biotechnology ecosystem is engaged in highly innovative and promising technological development but it also poses a range of CBW proliferation risks and export control challenges. Cloud labs, in particular, raise cross-cutting concerns related to the proliferation of CBW, automation and AI, and increasingly pose risks and challenges for export controls. In response to the changing make-up of the biotechnology ecosystem and specific uncertainties over the application of export controls in cases like cloud labs, states should seek to strengthen outreach activities and practices to relevant actors to more effectively raise awareness and strengthen their compliance with export controls and related governance mechanisms. The EU and the AG provide important forums in which the EU and its member states, as well as the other AG participating states, could assess and seek to address these risks and challenges.

Recommendations for strengthening the application of export controls to cloud labs and strengthening outreach to the biotechnology ecosystem

Recommendations for the EU and its member states

- Initiate discussions on—including a risk assessment of—cloud labs and the associated export control challenges in the EU's Emerging Technology Expert Group.
- Conduct a study to map new actors in the biotechnology ecosystem relevant for export control outreach to industry and research organizations in all EU member states. Such a study could focus on mapping bio-foundries, cloud labs and start-ups, including those operated or supported by universities and other research organizations.
- Continue work on developing guidelines for controls on ITT, to create more clarity on their implementation, including through the ongoing process towards the creation of EU guidelines on ITT controls. Such guidelines should include examples and case studies that represent scenarios familiar to actors in the biotechnology ecosystem.
- Raise the topic of cloud labs in AG meetings to continue collective monitoring of the risk as the technological capabilities offered by cloud labs expand and the number of providers increases.
- Deepen dialogue and coordination among EU member states through the Working Party on Dual-Use Goods on good practices when conducting targeted outreach and engaging with specific ecosystems of actors in wider export control outreach efforts, with a specific focus on outreach to actors in the biotechnology ecosystem.
- Develop a detailed good practices document for EU member states—but useful for all states—on outreach to industry, including to start-ups, and research organizations, with dedicated sections on targeted outreach to specific sectors and actor ecosystems, using cloud lab providers and developers of AI-enabled software as an example.
- Conduct joint workshops with actors from the biotechnology ecosystem to discuss how to strengthen compliance with the controls imposed by the dual-use regulation and referenced in the EU research security initiative and proposed update to the FDI screening regulation.

Recommendations for the AG

- Initiate discussions in the implementation and enforcement experts groups on the application of licensing requirements to the different transfers and provisions via SaaS that are part of the interaction between cloud lab providers and users.
- Initiate or continue New and Emerging Technologies Technical Experts Meeting discussions on the capabilities that roboticized laboratories and AI-enabled analysis and experiment design offer and how these affect CBW proliferation risks—and whether any specific items should be included in future AG control lists.
- Discuss laboratory security standards applicable to cloud labs and explore connections between the AG and BWC-related initiatives in order to have a wider discussion about safety and security issues and the prevention of illicit transfers.
- Foster dialogue across the multilateral export control regimes on national outreach to start-ups and emerging enabling technologies companies, in particular AI companies, that are increasingly impactful across the areas of CBW, conventional weapons, and missile and other delivery systems.

- Engage with international efforts to strengthen the global implementation of dual-use export controls through UN Security Council Resolution 1540 and the associated Wiesbaden Process (on industry) and Erlangen Initiative (on research and academia).[68] This could help to develop a two-pronged approach to engaging with start-ups and other new actors in the science and research context, from where many originate, and from the perspective of industry, to which most desire to progress and succeed.

[68] See 'Wiesbaden Process' and 'Erlangen Initiative' at German Federal Office for Economic Affairs and Export Control (BAFA), 'Outreach', [n.d.]; and United Nations, 1540 Committee, 'Information note', 7th International Wiesbaden Conference, 8–9 Feb. 2023.

ABBREVIATIONS

AG	Australia Group
AI	Artificial intelligence
BWC	1972 Biological and Toxin Weapons Convention
CBW	Chemical and biological weapon
Cloud lab	Cloud laboratory
CMU	Carnegie Mellon University
DIY	Do-it-yourself
EU	European Union
FAQ	Frequently asked questions
FDI	Foreign direct investment
ICP	Internal compliance programme
IGSC	International Gene Synthesis Consortium
ITT	Intangible transfers of technology
LLM	Large language model
SaaS	Software-as-a-service
SDL	Self-driving laboratory

LIST OF RECENT NON-PROLIFERATION AND DISARMAMENT PAPERS

Non-proliferation, Nuclear Technology and Peaceful Uses: Examining the Role and Impact of Export Controls
Non-Proliferation and Disarmament Paper no. 95
Giovanna Maletta, Dr Mark Bromley and Kolja Brockmann
April 2025

The EU Research Security Initiative: Implications for the Application of Export Controls in Academia and Research Institutes
Non-Proliferation and Disarmament Paper no. 94
Lauriane Héau
March 2025

Subregional Arms Control and Conflict Prevention in the Western Balkans
Non-Proliferation and Disarmament Paper no. 93
Katarina Djokic
January 2025

Artificial Intelligence, Non-proliferation and Disarmament: A Compendium on the State of the Art
Non-Proliferation and Disarmament Paper no. 92
Dr Thomas Reinhold, Dr Elisabeth Hoffberger-Pippan, Dr Alexander Blanchard, Marc-Michael Blum, Dr Filippa Lentzos and Alice Saltini
January 2025

The Potentially Revolutionary Impact of Emerging and Disruptive Technologies and Strategic Conventional Weapons on the Nuclear Deterrence Debate
Non-Proliferation and Disarmament Paper no. 91
Tom Sauer
December 2024

The Nexus of Non-traditional Security and Nuclear Risk: Implications for EU Foreign Policy in the Indo–Pacific
Non-Proliferation and Disarmament Paper no. 90
Elin Bergner, Sarah Laderman and Marcy R. Fowler
November 2024

Arms Supplies to Ukraine: Does the European Arms Export Control System Need Revision?
Non-Proliferation and Disarmament Paper no. 89
Ester Sabatino
May 2024

What Happened To Demand? Getting Small Arms Control Back on Track
Non-Proliferation and Disarmament Paper no. 88
Callum Watson and Aline Shaban
March 2024

The Chemical Weapons Convention After its Fifth Review Conference: Key Issues for the European Union
Non-Proliferation and Disarmament Paper no. 87
Alexander Ghionis and Alexander Kelle
February 2024

Feminist Foreign Policy and Nuclear Weapons: Contributions and Implications
Non-Proliferation and Disarmament Paper no. 86
Laura Rose Brown
November 2023

The Biological and Toxin Weapons Convention Confronting False Allegations and Disinformation
Non-Proliferation and Disarmament Paper no. 85
Jean Pascal Zanders
October 2023

Weaponizing Innovation? Mapping Artificial Intelligence-enabled Security and Defence in the EU
Non-Proliferation and Disarmament Paper no. 84
Dr Raluca Csernatoni
July 2023

The EU Space Strategy for Security and Defence: Towards Strategic Autonomy?
Non-Proliferation and Disarmament Paper no. 83
Dr Clara Portela and Dr Raúl González Muñoz
June 2023

Armed Conflict and Nuclear Security: Implications for Europe
Non-Proliferation and Disarmament Paper no. 82
Muhammed Ali Alkiş
April 2023

This document has been produced with the financial assistance of the EU. The contents are the sole responsibility of the EU Non-Proliferation and Disarmament Consortium and can under no circumstances be regarded as reflecting the position of the EU.

A EUROPEAN NETWORK

In July 2010 the Council of the European Union decided to support the creation of a network bringing together foreign policy institutions and research centers from across the EU to encourage political and security-related dialogue and the long-term discussion of measures to combat the proliferation of weapons of mass destruction (WMD) and their delivery systems. The Council of the European Union entrusted the technical implementation of this Decision to the EU Non-Proliferation Consortium. In 2018, in line with the recommendations formulated by the European Parliament the names and the mandate of the network and the Consortium have been adjusted to include the word 'disarmament'.

STRUCTURE

The EU Non-Proliferation and Disarmament Consortium is managed jointly by six institutes: La Fondation pour la recherche stratégique (FRS), the Peace Research Institute Frankfurt (HSFK/ PRIF), the International Affairs Institute in Rome (IAI), the International Institute for Strategic Studies (IISS–Europe), the Stockholm International Peace Research Institute (SIPRI) and the Vienna Center for Disarmament and Non-Proliferation (VCDNP). The Consortium, originally comprised of four institutes, began its work in January 2011 and forms the core of a wider network of European non-proliferation and disarmament think tanks and research centers which are closely associated with the activities of the Consortium.

MISSION

The main aim of the network of independent non-proliferation and disarmament think tanks is to encourage discussion of measures to combat the proliferation of weapons of mass destruction and their delivery systems within civil society, particularly among experts, researchers and academics in the EU and third countries. The scope of activities shall also cover issues related to conventional weapons, including small arms and light weapons (SALW).

www.nonproliferation.eu

EU Non-Proliferation and Disarmament Consortium

Promoting the European network of independent non-proliferation and disarmament think tanks

FONDATION pour la RECHERCHE STRATÉGIQUE

FOUNDATION FOR STRATEGIC RESEARCH

www.frstrategie.org

PRIF Peace Research Institute Frankfurt — HSFK Hessische Stiftung Friedens- und Konfliktforschung

PEACE RESEARCH INSTITUTE FRANKFURT

www.hsfk.de

iai Istituto Affari Internazionali

INTERNATIONAL AFFAIRS INSTITUTE

www.iai.it/en

IISS

INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES

www.iiss.org/en/iiss-europe

sipri

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

www.sipri.org

VCDNP Vienna Center for Disarmament and Non-Proliferation

VIENNA CENTER FOR DISARMAMENT AND NON-PROLIFERATION

www.vcdnp.org