sipri

BIO PLUS X

Arms Control and the Convergence of Biology and Emerging Technologies

KOLJA BROCKMANN, SIBYLLE BAUER
AND VINCENT BOULANIN

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

SIPRI is an independent international institute dedicated to research into conflict, armaments, arms control and disarmament. Established in 1966, SIPRI provides data, analysis and recommendations, based on open sources, to policymakers, researchers, media and the interested public.

The Governing Board is not responsible for the views expressed in the publications of the Institute.

GOVERNING BOARD

Ambassador Jan Eliasson, Chair (Sweden)
Dr Dewi Fortuna Anwar (Indonesia)
Dr Vladimir Baranovsky (Russia)
Ambassador Lakhdar Brahimi (Algeria)
Espen Barth Eide (Norway)
Jean-Marie Guéhenno (France)
Dr Radha Kumar (India)
Dr Patricia Lewis (Ireland/United Kingdom)
Jessica Tuchman Mathews (United States)

DIRECTOR

Dan Smith (United Kingdom)

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

Signalistgatan 9
SE-169 70 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org

BIO PLUS X

Arms Control and the Convergence of Biology and Emerging Technologies

KOLJA BROCKMANN, SIBYLLE BAUER
AND VINCENT BOULANIN

March 2019

sipri

STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE

© SIPRI 2019

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, without the prior permission in writing of SIPRI or as expressly permitted by law.

Contents

Acknowledgements

This report builds on past research by the authors on additive manufacturing, biotechnology, artificial intelligence and robotics, and on arms control, dual-use and arms trade controls, and military and security technologies. It is also based on information collected through interviews and communication with representatives of national authorities and technical experts from companies, universities and research institutes.

In putting together this research report the authors' work was greatly informed by the discussions during a breakout session on 'Bio plus X' during the 2018 Stockholm Security Conference and by three background technical briefing papers produced by Dr Elisabeth Bohm and Dr Filippa Lentzos, Dr Eleonore Pauwels, and Professor Sergey Zavriev.

The authors would like to thank the German Federal Foreign Office for providing the funding that allowed this report to be produced. They would also like to thank all those who agreed to share their expertise and particularly those who attended the Stockholm Security Conference in September 2018. Finally, the authors would like to thank their colleague Mark Bromley and the two external reviewers for their detailed comments on the report. The authors are grateful to Dr David A. Cruickshank and the SIPRI Editorial Department for their work. All errors are entirely the responsibility of the authors.

Abbreviations

AI	Artificial intelligence
AM	Additive manufacturing
BTWC	Biological and Toxin Weapons Convention
CRISPR	Clustered regularly interspaced short palindromic repeats
CWC	Chemical Weapons Convention
DIY	Do-it-yourself (biologists or community)
EU	European Union
ICT	Information and communications technology
IGSC	International Gene Synthesis Consortium
ISU	Implementation Support Unit
LOC	Laboratory on a chip
MTCR	Missile Technology Control Regime
OPCW	Organisation for the Prohibition of Chemical Weapons
R&D	Research and development
ROS	Robot Operating System
SAB	Scientific Advisory Board
UAV	Unmanned aerial vehicle
UN	United Nations
VR	Virtual reality

Executive summary

Technological advances in the biological sciences have long presented a challenge to the governance frameworks that focus on biosecurity and preventing the proliferation of biological weapons. Advances in biotechnology have, for example, made the manipulation of the genetic make-up of organisms—from bacteria to humans—faster, cheaper and easier. However, these developments often interact with or are enabled by other technologies, including by those categorized as 'emerging'. This process of convergence of recent developments in biotechnology with other emerging technologies holds tremendous promise but also increases the possibilities for misuse of biotechnology and for the proliferation of biological weapons. Specifically, the convergence of technological developments could affect the development, production or use of biological weapons and thereby challenge governance approaches that aim to prevent the proliferation of biological weapons to both states and non-state actors.

Advances in three specific emerging technologies—additive manufacturing (AM), artificial intelligence (AI) and robotics—could facilitate, each in their own way, the development or production of biological weapons and their delivery systems. This could be by enabling the automation of developmental or production steps that previously required manual manipulation or analysis by a human. They could also provide new possibilities for biological weapon use and increase the exposure of digitized biological data and operating parameters to cyberattacks. All three technologies are difficult to control, not least due to their dual-use nature, their digitization, and the fact that they are mainly developed by the civilian and private sectors. However, the impact of these technologies on the engineering of biological weapons and their delivery systems should not be exaggerated, as the expertise required to exploit these technologies for the purpose of developing and producing biological weapons remains significant and continues to pose a barrier to most actors.

The 1972 Biological and Toxin Weapons Convention (BTWC) is the central governance instrument for biological arms control. It is complemented by—or implemented through—a whole range of instruments, including export and import control measures; legislation, guidelines or standards on biosecurity and biosafety; regulations for the transportation of dangerous goods; and mechanisms to monitor relevant technological developments. However, the existing governance mechanisms provide only limited and often indirect coverage of the applications of AM, AI and robotics. The governance frameworks either have not used, or cannot fully use, their potential to explore connections between biotechnology and these emerging technologies. Treaty regimes and other governance instruments typically interact with each other much less than the respective technologies that they cover. An overarching question when viewing governance in the field of biosecurity through the lens of technological development and convergence is therefore how to better connect the relevant governance mechanisms. There is a lack of understanding of these technologies, the associated risks and their potential impact on the activities, transfers or behaviour governed by the existing frameworks. Dealing with developments in science and technology is far from a new issue. However, measures to address their impact must keep up with the dynamics of current developments. Therefore, improvements to governance instruments need to address the structural factors and new characteristics of new technologies that have a possibly significant impact through convergence with biotechnology.

The main conclusion is that, while new developments in these three emerging technologies could have an enabling effect in different steps of the development and use of biological weapons, the existing governance frameworks are ill-equipped to

comprehensively address these risks. To improve the ability to govern the convergence of biotechnology with other emerging technologies, concrete steps could be taken by national governments, regional organizations such as the European Union (EU) and international institutions, and by academia, the private sector and the DIY community.

National governments should more systematically assess technological developments, map domestic stakeholders, make use of parliamentary assessment mechanisms, increase resources for relevant authorities, and strengthen research on the detection, prevention, response and attribution of biological incidents. The EU should enhance engagement with the biotechnology industry and biosafety associations in the context of dual-use risks.

The BTWC regime should reform some of its elements, including its working practices and stakeholder engagement, and create a BTWC Scientific Advisory Board. It could also raise the issue of convergence on its agenda and better address the potential for misuse of commercial biotechnology and emerging technologies.

Academic institutions should introduce obligatory courses on ethics, law and biosafety in all natural science curriculums, encourage work on interdisciplinary technology assessments and further strengthen the collaboration between national academies of sciences, particularly on addressing risks resulting from technological convergence. The private sector should continuously strengthen its self-governance and compliance standards. The DIY community could organize workshop series on biosecurity for community laboratories and strengthen international efforts to foster responsible science and biosecurity awareness.

1. Introduction

Technological advances in the biological sciences have long presented a challenge to international and national governance frameworks, particularly those geared towards preventing the proliferation of biological and chemical weapons and other biological risks such as the accidental release of pathogens. The United Nations Secretary-General's disarmament agenda published in 2018 raises specific concerns about 'the ability of new technologies to ease barriers to the access and use of prohibited weapons, such as may be the case with synthetic biology and gene editing'.[1] Recent advances in biotechnology—such as those that make it faster, cheaper and easier to manipulate the genetic make-up of organisms, from bacteria to humans—interact with or are enabled by other technologies, including those that are often categorized as 'emerging technologies' (see box 1.1).[2] This report analyses this interactive process: the trends for convergence between biotechnology and other technologies (see box 1.2).

Discussions on the convergence between advances in biotechnology and established fields of science and technology, such as chemistry, computer science or engineering, have long informed debates on developments in science and technology, among others in the framework of the 1972 Biological and Toxin Weapons Convention (BTWC).[3] However, the existing governance architecture around the BTWC has been shown to have a limited ability to comprehensively review and appropriately address the risks and challenges arising from the speed and complexity of technological advances in particular areas.

More recently, the convergence of biotechnology with emerging technologies—including additive manufacturing (AM, often also referred to as 3D printing), artificial intelligence (AI) and robotics—has become a particular focus since these technologies hold tremendous promise but also increase the possibilities for misuse of biotechnology and the proliferation of biological weapons.[4] However, analyses and reporting by popular media, industry outlets and, to some extent, academic publications, tend to either over- or underestimate the current applications, capabilities and risks of new developments in biotechnology. These reports often cite advanced gene-editing techniques such as clustered regularly interspaced short palindromic repeats (CRISPR), but also other major emerging technologies such as AM or robotics.

This report provides a detailed and balanced analysis of the risks and challenges posed by the convergence of recent developments in biotechnology with other emerging technologies. It focuses on the impacts on arms control, non-proliferation and international security, given that the technological developments potentially have wide-ranging implications in these areas. Specifically, the report explores how the convergence of technological developments could affect the development, production or use of biological weapons and could thereby challenge the governance approaches that aim to prevent the proliferation of biological weapons to both states and non-state actors. It focuses on the convergence of biotechnology with three emerging technologies: additive manufacturing, artificial intelligence and robotics. These technologies cover a range of production-, automation- and analysis-related capabilities

[1] United Nations, Office for Disarmament Affairs, *Securing Our Common Future: An Agenda for Disarmament* (United Nations: New York, 2018), p. 52.

[2] Lentzos, F., 'Strengthen the taboo against biological and chemical weapons', *Bulletin of the Atomic Scientists*, 26 July 2018.

[3] Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (Biological and Toxin Weapons Convention, BTWC), opened for signature 10 Apr. 1972, entered into force 26 Mar. 1975, *United Nations Treaty Series*, vol. 1015 (1976).

[4] Hart, J. and Trapp, R., *Science and Technology and Their Impacts on the Biological and Toxin Weapons Convention: A Synthesis Report on Preparing for the Seventh Review Conference and Future Challenges* (SIPRI: Stockholm, Dec. 2011), pp. 24–25.

Box 1.1. Emerging technologies

Emerging technologies are usually understood to have new elements that display disruptive potential but have not yet developed their full potential.[a] The 'disruptive potential' depends on the specific technology and industry as it can mean a variety of changes. These include offering new, previously unavailable capabilities, replacing existing machines or manual labour, changing global supply chains, restructuring industries, revolutionizing or making obsolete certain classes of weapon systems. It generally represents a shift from a prevailing paradigm.[b]

Emerging technologies are rapidly developing, are usually at the centre of targeted research and development efforts, and are increasingly being adopted by economically and militarily important industries.[c] International arms control and non-proliferation frameworks have usually not developed agreed technical standards to define the qualities of emerging technologies that raise proliferation concerns but that lack a conclusive common risk assessment.[d] Technologies routinely placed in this category include additive manufacturing, artificial intelligence, biotechnology, quantum technology and robotics.[e]

Although the term 'emerging technologies' is in common usage and is used in this report, it has limitations, particularly in the arms control context. The qualification 'emerging' is commonly taken to refer to the technology as such, which by definition is always developing and not standing still, while in this report it is used to refer to emerging applications of that technology, in particular in the military and security context.

[a] On the different definitions of 'emerging technology' see Rotolo, D., Hicks, D. and Martin, B. R., 'What is an emerging technology?', *Research Policy*, vol. 44, no. 10 (Dec. 2015), pp. 1827–43, p. 1831.
[b] See e.g. Brimley, S., FitzGerald, B. and Sayler, S., *Game Changers: Disruptive Technology and U.S. Defense Strategy* (Center for a New American Security: Washington, DC, Sep. 2013), pp. 4, 11.
[c] Brockmann, K., 'Drafting, implementing, and complying with export controls: the challenge presented by emerging technologies', *Strategic Trade Review*, vol. 4, no. 6 (spring/summer 2018), pp. 5–28, pp. 7–8.
[d] Brockmann (note c).
[e] See e.g. US Department of Commerce, Bureau of Industry and Security, 'Review of controls for certain emerging technologies', *Federal Register*, vol. 83, no. 223 (29 Nov. 2018), pp. 58 201–202.

that form part of what is commonly termed the fourth industrial revolution.[5] They provide clear cases where technological advances at the interface with biology are most likely to have a significant impact on biosecurity and biological arms control, and they are generally perceived to be key emerging technology areas.

This report continues in chapter 2 by exploring the interaction of biotechnology with AM, AI and robotics, considering the current state of each technology, and identifying the developments and trends most relevant to the proliferation of biological weapons. Chapter 3 briefly introduces the existing treaties, institutions and other frameworks that govern biological arms control. It then analyses the extent to which the existing governance frameworks address the risks and challenges identified in chapter 2 and the areas where new policy approaches may be needed. Chapter 4 summarizes the key findings and conclusions and outlines policy recommendations for the most relevant stakeholders and governance frameworks.

[5] Schwab, K., *The Fourth Industrial Revolution* (Penguin: London, 2017).

Box 1.2. Convergence

There is no agreed definition of the concept of 'technological convergence'. While some definitions focus on the merging of several technologies into a new discipline, others stress the novel character of the conduct of science and the interactions of technology that transcend interdisciplinarity.[a]

For the purpose of this report, convergence describes a process with different degrees of intersection, interaction and alignment of technologies and scientific conduct that result from technologies and disciplines moving closer together. However, this neither presumes the direction of the process nor does it predict that these technologies will necessarily merge.

While chemistry and biology are commonly understood to have reached a high degree of convergence, other technologies are intertwined to lesser degrees. Partial overlaps and limited interaction only lead to convergence in specific applications of the latter technologies.

Convergence is therefore best understood as a spectrum that covers the different degrees of this process, which is bound to be continuously evolving, as are the technologies that are part of it. For example, three-dimensional printing of biological materials is aligning additive manufacturing with tissue engineering, which is increasingly referred to as bioprinting.

[a] Bajema, N. E., 'WMD in the digital age: understanding the impact of emerging technologies', Emergence & Convergence Research Paper no. 4, National Defense University, Oct. 2018, pp. 15–17; Coenen, C., *Konvergierende Technologien und Wissenschaften: Der Stand der Debatte und politischen Aktivitäten zu »Converging Technologies«* [Converging technologies and sciences: the state of the debate and political activities on "converging technologies"], Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) Background Paper no. 16 (TAB: Berlin, Mar. 2008), with English summary; and National Academies of Sciences, Engineering and Medicine, *Biodefense in the Age of Synthetic Biology* (National Academies Press: Washington, DC, 2018).

2. The convergence of advances in biology and emerging technologies

Biotechnology is generally defined as the field of study that seeks to exploit biological processes for industrial, medical or other production purposes, such as the genetic manipulation of microorganisms for the production of antibiotics.[6] Advances in biotechnology promise significant benefits to society in general, including specific biosecurity benefits in terms of supporting surveillance, detection, prevention and response to pathogens.[7] Yet they also raise significant concerns (see box 2.1).

Advances in biotechnology are expanding the techniques available to modify genes and organisms at a staggering pace, making it easier to make pathogens more dangerous. Disease-causing organisms can now be modified to, for instance, increase their virulence, expand their host range, increase their transmissibility or enhance their resistance to therapeutic interventions. Scientific advances have also made it theoretically possible to create entirely novel biological weapons in a number of ways (see box 2.2): by synthetically creating or recreating existing, extinct or entirely new pathogens; by modifying the immune system, nervous system, genome or microbiome; by weaponizing 'gene drives' that could rapidly and cheaply spread harmful genes through animal and plant populations; and by delivering pathogens and biological systems by novel means. These developments are discussed in detail elsewhere.[8]

This chapter outlines some of the key security challenges that arise where advances in biotechnology intersect with the emerging technologies of additive manufacturing, artificial intelligence and robotics. These three technologies are predominant in contemporary discussions of technologies with emerging military applications. Their impact on international security, including in relation to biological weapons, is often either underestimated or exaggerated and requires clarification. Several other technologies, including nanotechnologies, would also match these criteria, but discussing them in depth is beyond the scope of this report. The broad range of possible applications of these three technologies in the development and production of biological agents and their delivery systems illustrates the risks and challenges that governance frameworks need to address.

For each of the three emerging technologies, the following sections introduce the current state of the art, the impact on and interconnection with biology and biotechnology, and the opportunities and challenges posed for biosecurity and the proliferation of biological weapons. The final section then compares these risk profiles and provides an overview of the common types of challenge and risk that governance frameworks need to address.

[6] Oxford Dictionaries, 'Biotechnology', Oxford University Press.

[7] Watson, C. et al., *Technologies to Address Global Catastrophic Biological Risks* (Johns Hopkins Center for Health Security: Baltimore, MD, Oct. 2018).

[8] World Economic Forum (WEF), *The Global Risks Report 2019*, 14th edn (WEF: Geneva, 2019), pp. 44–53; Kirkpatrick, J. et al., *Editing Biosecurity: Needs and Strategies for Governing Genome Editing* (Institute for Philosophy and Policy et al.: Dec. 2018); National Academies of Sciences, Engineering and Medicine, *Biodefense in the Age of Synthetic Biology* (National Academies Press: Washington, DC, 2018); InterAcademy Partnership (IAP), *Assessing the Security Implications of Genome Editing Technology*, Report of an international workshop, Herrenhausen, Germany, 11–13 Oct. 2018 (IAP: Washington DC, 2018); Royal Society and National Academy of Sciences, *Sackler Forum 2015: Trends in Synthetic Biology and Gain of Function and Regulatory Implications* (Royal Society: London, Sep. 2016); and InterAcademy Partnership (IAP), *The Biological and Toxin Weapons Convention: Implications of Advances in Science and Technology* (IAP: Dec. 2015).

Box 2.1. Key trends in biotechnology and implications for security

Key trends in biotechnology

- Substantial investments required, but once discoveries are made they become reproducible almost immediately and at minimal cost
- Easier access to the knowledge, tools and components for creating living organisms
- Amateurs, DIY scientists and other new actors entering biosciences
- Rapidly evolving toolbox to modify genes and organisms (e.g. CRISPR)
- Convergence with other areas of science and technology (e.g. chemistry, engineering, computer science)
- Digitization and automation of biological experiments, production and data

Implications for security

- Novel biological weapons
- Easier for a larger range of people to misuse the science
- New misuse potential through convergence with other emerging technologies
- Larger attack surface and increased vulnerabilities that could be exploited to cause harm[a]
- Expanding grey area between permitted defensive activities and banned offensive activities
- Harder to detect and attribute use of biological weapons

[a] Kirkpatrick, J. et al., *Editing Biosecurity: Needs and Strategies for Governing Genome Editing* (Institute for Philosophy and Policy et al.: Dec. 2018).

Source: Lentzos, F., Poster presentation, '2019. Capturing Technology. Rethinking Arms Control.' conference, Berlin, 15 Mar. 2019.

Biology plus additive manufacturing

What is additive manufacturing?

Additive manufacturing, often referred to as 3D printing, is an emerging technology that has generated both positive hopes (particularly its applications in medicine) and negative publicity (e.g. regarding 3D printed guns) in recent years. It is frequently characterized as a 'disruptive technology' or as a 'game changer'.[9] AM has the potential to decentralize production capabilities, reduce the necessity for physical transportation of goods and deskill aspects of manufacturing.[10] Some of the technological developments in AM are still in their infancy, while others have already matured to the extent that they are commonly deployed in commercial settings. As such, it is necessary to consider both the current and the projected impact of the resulting risks, as well as the urgency with which they need to be addressed by the relevant governance instruments.

AM describes a broad category of advanced automated manufacturing techniques. It can produce objects of virtually any shape or form by depositing layer upon layer of material and fusing them together using a variety of techniques, such as liquefied extrusion, inkjet printing, stereolithography, sintering, and laser or electron beam melting (see figure 2.1).[11] Compared to most subtractive manufacturing technologies, which cut away excess material from a larger block, less material is lost with AM since it involves assembling material. In addition, AM promises to produce complex parts, resulting in products that are lighter and consist of fewer individual components than those built using established manufacturing processes. One of the particular

[9] Brimley, S., FitzGerald, B. and Sayler, S., *Game Changers: Disruptive Technology and U.S. Defense Strategy* (Center for a New American Security: Washington, DC, Sep. 2013), pp. 14–15.

[10] E.g. Bromley, M., Brockmann, K. and Maletta, G., 'Controls on intangible transfers of technology and additive manufacturing', *SIPRI Yearbook 2018: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2018).

[11] For a comprehensive overview of AM techniques see German Bundestag, Committee on Education, Research and Technology Assessment, 'Technikfolgenabschätzung (TA): Additive Fertigungsverfahren (3-D-Druck)' [Technology assessment (TA): additive manufacturing (3D printing)], Drucksache no. 18/13455, 29 Aug. 2017, pp. 60–70.

Box 2.2. Defining a biological weapon

In general, a biological weapon consists of a weaponized biological agent and a delivery system.

The weaponization of an agent—that is, selecting, designing, developing and manipulating an agent for a specific (usually military) purpose—should be distinguished from simply using biological materials, including pathogens or toxic agents, for malicious ends.[a] Weaponization seeks to ensure the effectiveness of a biological weapon by obtaining a suitable pathogen that can infect the target and cause illness or death after dissemination, without being affected by environmental conditions or being significantly mitigated by medical treatment and biodefence measures.

A delivery system for a biological weapon is a device that facilitates the appropriate dissemination and dispersion of the agent in a way that makes the target susceptible to its effect. Examples of dissemination include use of a spray tank on an aeroplane for area denial, injection of an agent, possibly covered in a capsule or pellet, or use of a handheld spray for targeted killings. In the case of aerosol dispersion, the effectiveness depends on ensuring that particles of the agent are of the right size to be absorbed by the target's respiratory system.

It is often more helpful to consider biological weapon capabilities—whether a state is in a position to threaten or perpetrate a biological attack—rather than actual possession and stockpiles.[b] A distinction between an actor having biological weapons and having access to weapon-related technologies that enable a biological weapon programme is therefore key to risk assessment and control efforts. These capabilities can be gained not only by operating an offensive weapon programme, but also from legitimate biodefence activities, life science research, and the industrial development and formulation of biological agents: the processes and knowledge required for each are often difficult to distinguish.

[a] Zanders, J. P., 'Assessing the risk of chemical and biological weapons proliferation to terrorists', *Nonproliferation Review*, vol. 6, no. 4 (fall 1999), pp. 17–34, pp. 18–19.
[b] Bohm, E. and Lentzos, F., 'Technical briefing note on developments in science and technology and governance in relation to biological weapons', Unpublished briefing paper, SIPRI, Nov. 2018.

advantages of AM is its ability to produce objects that are hollow or that have precise cavities or channels in an otherwise solid part. For example, the ability to build precise cooling channels has made it a particularly attractive technology for the manufacture of motors and even rocket engines.[12]

The convergence of AM and synthetic tissue production techniques into what is often referred to as bioprinting is one of the most promising techniques for regenerative medicine.[13] Bioprinting has the potential to print anything from living tissue to entire organs. In contrast to the materials used as feedstock in other AM machines, such as plastics, metals or other inanimate materials, bioprinting involves the added complexity of using living cells that are highly sensitive to environmental conditions, their growth and differentiation factors, and the particularities of the construction of tissues.[14]

In bioprinting, the biological materials, or bioinks, are deposited using, for example, small nozzles to achieve precisely layered arrangements of cells and support structures. These then grow into functional tissue based on the cells' own biological processes and the addition of growth factors.[15] A number of AM techniques that are also applied with plastics, metals and other materials have been adapted for bioprinting. For example, hydrogel bioinks can be deposited by extrusion or in droplets using an inkjet. Stereolithography—which uses photoinduced polymerization to solidify a precise pattern of a liquid resin by exposure to, for example, ultraviolet light—can be used to build precise porous scaffolds for tissue engineering.[16] The capabilities of

[12] Brockmann, K. and Bauer, S., '3D printing and missile technology controls', SIPRI Background Paper, Nov. 2017, pp. 6–8; and Aerojet Rocketdyne, 'Aerojet Rocketdyne successfully tests engine made entirely with additive manufacturing', 23 June 2014.

[13] Chowdhury, H., 'Liver success holds promise of 3D organ printing', *Financial Times*, 5 Mar. 2018.

[14] Murphy, S. V. and Atala, A., '3D bioprinting of tissues and organs', *Nature Biotechnology*, vol. 32, no. 8 (Aug. 2014), pp. 773–85, p. 773.

[15] German Bundestag (note 11), pp. 43–44.

[16] Miller, J. S. and Burdick, J. A., 'Editorial: special issue on 3D printing of biomaterials', *ACS Biomaterials Science & Engineering*, vol. 2, no. 10 (Oct. 2016), pp. 1658–61, p. 1658; and Derakhshanfar, S. et al., '3D bioprinting for biomedical devices and tissue engineering: a review of recent trends and advances', *Bioactive Materials*, vol. 3, no. 2 (June 2018), pp. 144–56, pp. 150–51.

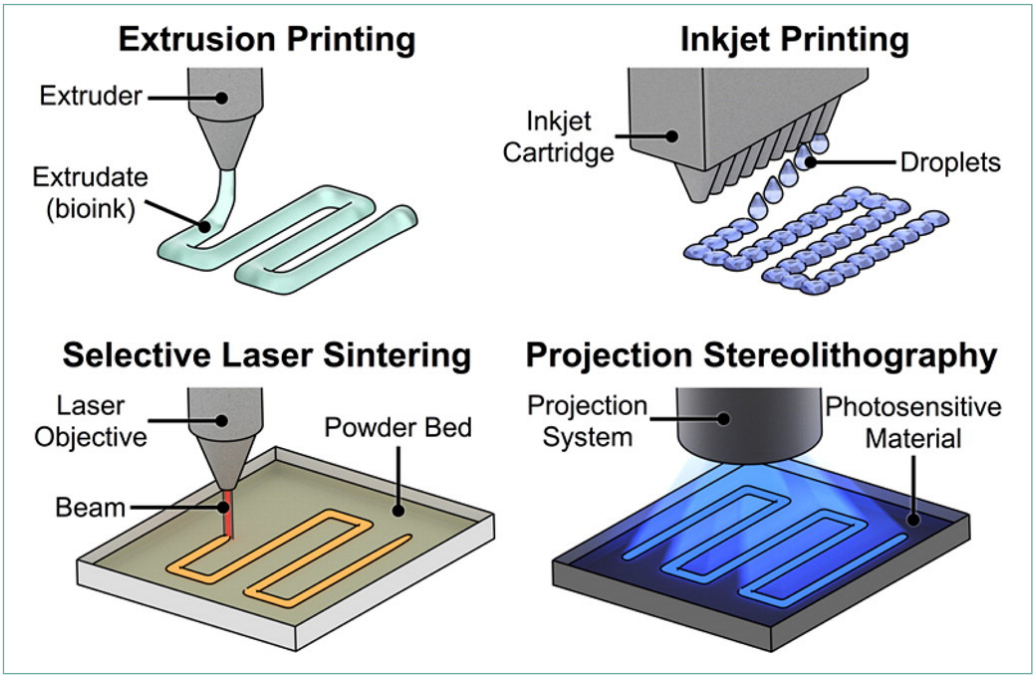

Figure 2.1. Selected additive manufacturing techniques

Source: Miller, J. S. and Burdick, J. A., 'Editorial: special issue on 3D printing of biomaterials', *ACS Biomaterials Science & Engineering*, vol. 2, no. 10 (Oct. 2016), pp. 1658–61, p. 1658.

these AM techniques vary according to their suitability for different types of tissue and the tissue-construction techniques used, particularly depending on the support structures and matrices used to simulate or scaffold cell tissue structures.

Three main components of AM are key to its capabilities and therefore also the elements considered for control: (*a*) the AM machines; (*b*) the AM feedstock materials; and (*c*) the digital build files that provide the information on the object to be printed.

AM machines are usually multipurpose machines. The image of a rather simple desktop device, as implied by the often-used term '3D printer', is somewhat misleading when used to describe the entire range of contemporary AM techniques and production machines. There are vast differences in the product range and performance characteristics, size and technical sophistication between inexpensive desktop printers using plastics, bioprinters using bioinks and the often large machine centres that house AM machines that use metal feedstock.

The materials used as feedstock in different AM techniques include polymers, metals (such as steels and alloys), high-strength carbon fibres, bioinks and a range of specialized corrosion-resistant superalloys. Commercially available bioinks can contain cells, biocompatible materials and supporting components for the production of functional living tissue.[17]

AM machines rely on digital build files, initially in the form of computer-aided design (CAD) files or similar formats, which can encode the dimensions of the desired object, and subsequently in machine-specific formats that include the operating parameters and commands that the AM machine needs to execute in order to produce the object's desired performance characteristics (see figure 2.2).[18] The digitization of the blueprints and commands—the information that is necessary for the production

[17] Murphy and Atala (note 14), p. 773.
[18] German Bundestag (note 11), pp. 57–59.

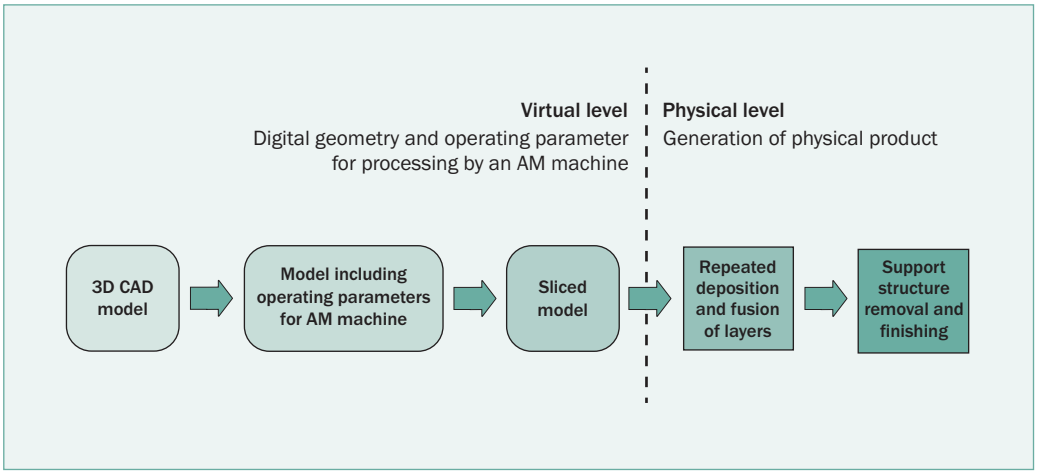

Figure 2.2. The additive manufacturing process

Notes: AM = additive manufacturing; CAD = computer-aided design.

Source: Adapted from Heil, J. E., 'Quantitative, modellbasierte Analyse der Wirkungen generativer Fertigungsver- fahren auf die Wertschöpfungskette des deutschen Maschinen- und Anlagenbaus', Master's thesis, Institute of Production Science, Karlsruhe Institute of Technology, 2014, as reproduced in German Bundestag, Committee on Education, Research and Technology Assessment, 'Technikfolgenabschätzung (TA): Additive Fertigungsverfahren (3-D-Druck)' [Technology assessment (TA): additive manufacturing (3D printing)], Drucksache no. 18/13455, 29 Aug. 2017, p. 57.

of an item—allows for easy transferability of the technology using electronic media (e.g. email) or decentralized information-sharing platforms (e.g. cloud storage).[19]

The state of the art in additive manufacturing

AM technology is rapidly developing, and only a small number of applications have matured to the extent of reaching the mainstream.[20] A number of challenges remain before AM can produce objects with the same quality, characteristics and precision that traditional manufacturing processes can achieve. The speed of production, the speed–quality relationship and the reliability of individual pieces still limit the productivity of AM. For example, many metal AM techniques that could be used to print parts or equipment for unmanned aerial vehicles (UAVs, or drones) are similar to a continuous welding process, which inherently suffers from small defects that cannot be reliably predicted, and non-destructive quality-control methods are still being developed.[21]

Despite increased automation and digitization, the exploitation of the full potential of AM technology requires a considerable amount of specific expertise and tacit knowledge. This tacit knowledge comprises information and skills that cannot be acquired simply by reading written records or instructions, such as a laboratory protocol: to develop the skills, know-how and sensory cues to execute a particular step of a procedure requires practical experience.[22]

AM does not deliver specialized high-end products 'at the touch of a button' but involves a process whose different stages require a variety of skills (see figure 2.2). While the creation of a digital three-dimensional blueprint can often be facilitated by scanning the desired shape, specialized engineering knowledge and experience

[19] Stewart, I. J., *Examining Intangible Controls*, part 2, *Case Studies*, Project Alpha, Centre for Science and Security Studies (King's College London: London, June 2016), pp. 19–21.

[20] Park, R., 'Hype, hype cycles and applying reason', *Disruptive Magazine*, 28 July 2017.

[21] Spiez Laboratory, *Spiez Convergence: Report on the Second Workshop, 5–8 September 2016* (Spiez Laboratory: Spiez, Oct. 2016), p. 19.

[22] Vogel, K. M., 'Framing biosecurity: an alternative to the biotech revolution model?', *Science and Public Policy*, vol. 35, no. 1 (Feb. 2008); and Vogel, K. M., 'Biodefense: considering the sociotechnical dimension', eds A. Lakoff and S. J. Collier, *Biosecurity Interventions: Global Health and Security in Question* (Columbia University Press: New York, 2008).

are required for the further steps before an object with the desired performance characteristics can be produced: developing a model in a specific AM machine's format, encoding the commands and process parameters, and finally processing this information to code for every single layer that is deposited and fused by the machine. Although the physical manipulation is entirely automated, the operation, handling and cleaning of advanced AM machines and the removal of necessary support structures can all affect the quality and uniformity of products. In addition, most AM techniques require the application of finishing procedures to meet precision and surface smoothness requirements. Repeatability—especially in the case of high-end metal AM—is therefore also dependent on a variety of skills and practical knowledge.

Both the range of AM technologies and the industries that produce AM machines continue to expand. The distributions of these industries vary considerably between low-end, consumer-level polymer printers, high-end metal AM machines and experimental bioprinting equipment. A major share of the market for polymer printers is held by manufacturers in the United States and China, but states from many other regions are entering this market. High-end metal AM machines and feedstock materials are mostly produced by companies based in Germany, the USA, the United Kingdom, Canada, Japan and a few other European states, which are all members of the multilateral export control regimes.[23] In contrast, research into bioprinting is much more dispersed worldwide, including in states that do not participate in the export control regimes. This is in part because it remains at the experimental stages and has not yet reached industrial scale, but also because it builds on more widely diffused technologies for production of synthetic tissue.

Opportunities arising from the convergence of biology and additive manufacturing

AM could offer increased adaptability and enhance logistics for both military operations and disaster- or crisis-response by enabling on-the-spot manufacturing during deployment. For example, the US military deploys mobile laboratories with AM machines in conflict zones for repair and the production of replacement parts.[24] While the impact on logistics is already materializing, in the future AM could potentially increase the capabilities of medical units in the field by providing on-the-spot tissue or implant production.

AM has already been adopted by the biomedical sector for a variety of applications. The main advantage that many of the applications seek to exploit is the ability of AM machines to produce individualized items without the need to produce new moulds each time, to reconfigure machine tools or to draw on extensive manual manufacturing skills. AM is established as a production technology for customized biomedical implants or prostheses, such as hip and dental implants.[25] These applications use a spectrum of AM machines, ranging from high-end metal AM machines to simpler, cheaper machines that use thermoplastics and other polymers. The price of AM production has been particularly attractive. For example, lower priced equipment and production using polymers is used to produce relatively inexpensive customized artificial limbs for children.[26] This is a significant advantage as prosthetics otherwise commonly cost thousands of dollars and require long production times by a skilled prosthetist or orthopaedic technician. The easy sharing of build files and the ability to customize or personalize products using more accessible techniques have enabled

[23] Brockmann, K. and Kelley, R., *The Challenge of Emerging Technologies to Non-proliferation Efforts: Controlling Additive Manufacturing and Intangible Transfers of Technology* (SIPRI: Stockholm, Apr. 2018), p. 8.

[24] Hallex, M., 'Digital manufacturing and missile proliferation', *Public Interest Report*, vol. 66, no. 2 (spring 2013).

[25] Ventola, C. L., 'Medical applications for 3D printing: current and projected uses', *Pharmacy and Therapeutics*, vol. 39, no. 10 (Oct. 2014), pp. 704–11, p. 708.

[26] Birrell, I., '3D-printed prosthetic limbs: the next revolution in medicine', *The Observer*, 19 Feb. 2017.

wider engagement and have built a community among doctors, engineers and affected families.

The use of bioprinting is less mature, but a variety of applications are in the developmental phase or the early stages of commercialization.[27] While the ability to print fully functional donor organs that can be implanted and sustained in a human body is probably decades away, the production of different kinds of tissue for medical research and testing is more advanced.[28]

The sophistication of AM machines and the range of marketed products continue to increase, and the biomedical AM sector is expected to grow significantly in the coming years. There are nevertheless some remaining technical hurdles and uncertainties. While most of the prosthetics applications have been certified by the appropriate medical oversight bodies, long-term clinical studies of possible side-effects and the durability of implants are still ongoing.[29] Bioprinting is not yet able to reliably produce thicker or complexly vascularized tissues, as would be required for major organs. Nevertheless, research and development (R&D) in this field of engineering and medicine continues and will probably further drive advances of the technology.

Risks and challenges arising from the convergence of biology and additive manufacturing

AM applications have caused proliferation concerns related to both conventional weapons and biological, chemical and nuclear weapons, particularly in relation to the possibility of using AM to circumvent the barriers imposed by national export control systems.[30] The UN disarmament agenda highlights AM as an example that demonstrates 'the ability of new technology to assist in the undesirable or undetected dissemination of controlled or sensitive items'—a particular challenge that needs to be addressed as part of international disarmament and non-proliferation efforts.[31]

AM technology provides a multipurpose manufacturing capability that can potentially substitute for other, controlled production equipment. In addition, the digitization in build files of much of the information required for the production of a controlled product means that it can now be more readily transferred—whether electronically, without having to pass through customs in a material form, or through the travel of a person with the necessary expertise. Advances in AM could thus have a significant impact on the effectiveness of export control as a non-proliferation tool as it could increase the reliance on transfers of data, which are assumed to be more difficult to track and control by licensing and enforcement agencies.[32] Moreover, the degree of digitization and automation also makes AM equipment and build files susceptible to cyberattack and manipulation. Experiments have shown that the manipulation of the software of an AM machine or a build file can result in material fatigue or faults that cannot be readily detected.[33]

Developments in the printing of drone components and laboratory equipment and in bioprinting continue to be driven by commercial and scientific interests and

[27] Zilinskas, R. A. and Mauger, P., *Biotechnology E-commerce: A Disruptive Challenge to Biological Arms Control*, James Martin Center for Nonproliferation Studies (CNS) Occasional Paper no. 21 (Middlebury Institute of International Studies: Monterey, CA, Mar. 2015), p. 36.

[28] Ferrari, A. et al., *Additive Bio-manufacturing: 3D Printing for Medical Recovery and Human Enhancement*, European Parliamentary Research Service, Science and Technology Options Assessment, IP/G/STOA/FWC/2013-001/LOT5/C2 (European Parliament: Brussels, July 2018), pp. 63–65

[29] Ventola (note 25), pp. 710–11.

[30] On the challenge that AM poses to export controls see Brockmann and Kelley (note 23).

[31] United Nations (note 1), p. 52.

[32] Palmer, M., 'Ship a design, not a product! Is 3D printing a threat to export controls?', *World ECR*, no. 43 (Sep. 2015), pp. 30–31; and Kroenig, M. and Volpe, T., '3D printing the bomb? The nuclear nonproliferation challenge', *Washington Quarterly*, vol. 38, no. 3 (fall 2015), pp. 7–19, pp. 11–12.

[33] Irving, D., 'Four ways 3D printing may threaten security', RAND Blog, 8 May 2018.

by the active do-it-yourself (DIY) community, rather than by the possible military applications. Thus, the interaction and convergence of biotechnology and AM currently only produce moderate risk of proliferation of biological weapons. Nonetheless, it is necessary for the arms control community to monitor these developments and consider appropriate governance measures.

Three types of AM application are of particular concern: (*a*) the printing of production or laboratory equipment; (*b*) bioprinting; and (*c*) the printing of delivery systems or their components.

AM can be used to print a range of specific parts for production and laboratory equipment and other items relevant to the production of biological weapons. In this way, AM could be used to help conceal a clandestine biological weapon development or production effort.[34] Recent studies on the capabilities of laboratory equipment produced using AM have shown promising results. However, especially when using polymers, chemical compatibility and resistance limit the range of materials that can be used. Moreover, there has been limited testing of relevant properties and therefore how printed items interact with chemicals and biomaterials.[35] Certification for safe use presents a high hurdle, especially if parts or equipment are destined for application in facilities with a high biosafety level. Indeed, much of the equipment that is of concern can already be easily acquired, often online, through channels that lack controls.[36] This means that, while AM may offer an alternative production pathway for some parts, it may involve additional hurdles—technical, knowledge-based or in process development—that would not justify the effort for most actors if there are other ways to acquire or produce these parts.[37] As the use of AM for the printing of production or laboratory equipment is still limited, it may only present advantages for making a limited set of laboratory equipment, without simplifying production significantly for any type of actor.

Among the many positive applications of bioprinting in medicine, the printing of tissue or organelles (cell compartment with specific functions) for the purpose of pharmacological testing is potentially also relevant in the context of the development of biological or chemical weapons.[38] Such synthetic tissue is already commonly used to test pharmaceutical compounds for toxicity.[39] As the technology matures, bioprinted materials may be used in this way for some of the biomedical research and specific testing that is involved in development of biological weapons.[40] For example, according to one expert, bioprinted tissue could be used to assess specific interactions between biological agents and certain tissue types under conditions that are otherwise difficult to simulate.[41] However, these techniques are not uniquely enabling; established methods, such as animal testing, are currently more accessible and require a more common set of skills.[42] While bioinks and suitable printers are commercially accessible,

[34] Bajema, N. E., 'WMD in the digital age: understanding the impact of emerging technologies', Emergence & Convergence Research Paper no. 4, National Defense University, Oct. 2018, pp. 12–14.

[35] Heikkinen, I. T. S. et al., 'Chemical compatibility of fused filament fabrication-based 3-D printed components with solutions commonly used in semiconductor wet processing', *Additive Manufacturing*, vol. 23 (Oct. 2018), pp. 99–107.

[36] Zilinskas and Mauger (note 27).

[37] Fairchild, S. et al., *Findings from the 2016 Symposium on Export Control of Emerging Biotechnologies*, James Martin Center for Nonproliferation Studies (CNS) Occasional Paper no. 26 (Middlebury Institute of International Studies: Monterey, CA, Apr. 2017), pp. 18–19.

[38] Meeting of the States Parties to the BTWC, Meeting of Experts, 'Advances in science and technology related to the Convention', 2 June 2014, BWC/MSP/2014/MX/INF.3, p. 5.

[39] Zilinskas and Mauger (note 27), p. 36.

[40] National Academies of Sciences, Engineering and Medicine (note 8), pp. 114–15.

[41] Trapp, R., Independent consultant on chemical and biological weapon issues, Author correspondence, 11 Dec. 2018.

[42] Fairchild et al. (note 37), pp.18–19.

Box 2.3. Machine learning and deep learning

Machine learning—which has been responsible for a rapid expansion in applications of artificial intelligence (AI)—is an approach to AI engineering that consists of building systems that can teach themselves to do a specific task. It differs from traditional AI programming methods, in which a human hard-codes (i.e. defines in fixed, mathematical terms) the way in which a task has to be executed by the systems.[a]

The machine learning approach has been around since the beginning of AI research but remained a marginal subfield in the 1960s and 1970s as it was of limited practical use.[b] In the 1980s and 1990s the digitization of many industries and the development of large data sets reignited interest in it and inspired the development of new machine learning techniques. These include refined versions of the 'artificial neural network' method, which draws on knowledge of the human brain, statistics and applied mathematics.

The real breakthrough for machine learning came in the early 2010s due to a successful adaptation to 'deep learning': a machine learning technique that involves large, or 'deep', artificial neural networks. The advance of deep learning was itself supported by two trends. One was the widespread commercialization of graphic processing units (GPUs), a type of computer chip that is well suited for machine learning operations. The second, and perhaps more important, trend was the development of the Internet and social media, which led to an explosion in the volumes of digital data on which machine learning algorithms can be trained.

[a] Knight, W., 'There is a big problem with AI', *MIT Technology Review*, 11 Apr. 2017.
[b] Knight (note a).

Source: Boulanin, V. and Verbruggen, M., *Mapping the Development of Autonomy in Weapon Systems* (SIPRI: Stockholm, Nov. 2017).

the advantages that methods based on AM technology may offer remain below those of more established testing approaches.

The use of AM to produce components of drones means that their designs can be adapted to increase their capabilities and make them more suitable for use as a delivery system for biological weapons. Plans and build files for printable parts of drones are commonly exchanged in the DIY community, and these may provide an attractive option for non-state actors. Simultaneously, the capabilities and customizability of off-the-shelf drones have also increased.[43] Certain sizes of spray tank and types of nozzle that are already subject to export controls may be produced using AM.[44] However, the level of sophistication of these parts is not high enough to present a major obstacle to their acquisition by either a state or a non-state actor. No state or state-sponsored actor will have a problem in producing, for example, spray tanks or nozzles, while other less technologically sophisticated production pathways are available to non-state actors.

Biology plus artificial intelligence

What is artificial intelligence?

The concept of AI was coined in the mid-1950s by John McCarthy, who defined it broadly as the 'science and engineering of making intelligent machines'.[45] Today it is used as a general term for a wide set of computational techniques that allow computers and robots to mimic capabilities that are usually associated with human intelligence, such as observing the world through vision, processing natural language and learning.[46] AI is not a definite, singular technology in the way that, for instance, nuclear weapon technology is; rather, it is a general-purpose (or 'portfolio') technology that encompasses a wide variety of enabling applications that may be used to give some form of cognitive capabilities to (i.e. 'cognify') multiple types of technology, including weapon systems.

[43] Dura, K., 'The reality of armed, commercial drones', *National Interest*, 13 Oct. 2018.
[44] Australia Group, 'Control list of dual-use biological equipment and related technology and software', May 2017.
[45] Pearl, A., 'Homage to John McCarthy, the father of artificial intelligence (AI)', Artificial Solutions, 2 June 2017. See also Dale, R., 'An introduction to artificial intelligence', ed. A. M. Din, SIPRI, *Arms and Artificial Intelligence: Weapons and Arms Control Applications of Advanced Computing* (Oxford University Press: Oxford, 1987), p. 33.
[46] International Panel on the Regulation of Autonomous Weapons (IPRAW), *Focus on Computational Methods in the Context of LAWS*, "Focus on" Report no. 2 (German Institute for International and Security Affairs: Berlin, Nov. 2017).

Since the 1950s, the field of AI has gone through several 'hype cycles': each period of major success was inevitably followed by a period of disillusion as the new and promising approach of AI eventually failed to match its early expectations.[47] These troughs in expectation typically resulted in cutbacks in the funding of research programmes and in the investment in commercial applications. Since the early 2010s the field of AI has been experiencing a new peak in expectations, due to the conjunction of several factors: (*a*) major progress in computational power; (*b*) rapid advances in machine learning, in particular 'deep learning' (see box 2.3); and (*c*) increasing availability of the digital data on which machine learning systems can be trained.

The state of the art in artificial intelligence

As in previous peaks in enthusiasm for AI, success stories about what current AI systems can achieve have channelled major interest and investment towards the most promising approach to AI engineering—which is currently machine learning. The strength of machine learning lies in its ability to abstract statistical relationships from data. It is an extremely powerful approach to AI engineering for automating tasks that require advanced pattern recognition. These tasks include (*a*) machine perception, (*b*) data classification, (*c*) prediction, (*d*) anomaly detection, (*e*) optimization and (*f*) creative data generation.[48]

The ability of computers and robots to perceive the world has been dramatically improved by advances in machine learning.[49] In the field of computer vision, the significance of deep learning was concretely measured by a tenfold decrease in the error rate of image recognition systems between 2010 and 2017—from 25 per cent to around 2 per cent.[50] Computer vision systems that are powered by deep learning can now compete with—or simply outperform—humans in object and face recognition.[51] In the health sector, deep learning is creating new possibilities for automating the analysis of medical imaging such as X-rays and magnetic resonance imaging.[52] For instance, a team at the US technology company Google uses deep learning to diagnose symptoms of blindness by reading retina scans.[53]

Machine learning methods can be used to classify any type of digital data by making sense of large and heterogenous sets of data, from images to medical records. Large Internet service providers such as Google, Facebook and YouTube use machine learning to label and organize content, from text to images and videos.[54]

The way that machine learning finds correlations in data can also be used to make statistical predictions about future behaviour. E-commerce companies such as Google, Amazon and Netflix use machine learning to generate recommendations for customers, for example by auto-filling search terms or through targeted marketing.[55] The medical field is experimenting with machine learning to process patient records to discover people at heightened risk of, for example, a heart attack or diabetes.[56]

[47] On hype cycles see Gartner, 'Gartner hype cycle', [n.d.]; and Kit, P., 'What should we learn from past AI forecasts?', Open Philanthropy Project, May 2016.

[48] As identified by Scharre, P. and Horowitz, M. C., *AI: What Every Policymaker Needs to Know* (Center for New American Security: Washington DC, June 2018).

[49] Gershgorn, D., 'See the difference one year makes in artificial intelligence research', *Popular Science*, 31 May 2016.

[50] Gershgorn, D., 'The data that transformed AI research—and possibility the world', *Quartz*, 26 July 2017.

[51] Dodge, S. and Karam, L., 'A study and comparison of human and deep learning recognition under visual distortions', May 2017.

[52] Klang, E., 'Deep learning and medical imaging', *Journal of Thoracic Disease*, vol. 10, no. 3 (Mar. 2018), pp. 458–63.

[53] Regalado, A. 'Look how far precision medicine has come', *MIT Technology Review*, 23 Oct. 2018.

[54] Marr, B., 'The amazing way Google uses deep learning AI', *Forbes*, 8 Aug. 2017.

[55] Marr (note 54).

[56] Shu, C., 'Amazon's newest service uses machine learning to extract medical data from patient record', Techcrunch, 27 Nov. 2017.

The ability of machine learning to identify patterns can also be used to detect anomalies in large data sets. For example, in order to improve cybersecurity, machine learning could be used to improve the detection of zero-day vulnerabilities in computer systems and of new malware with a signature that is not yet well known.[57]

Machine learning can be used to optimize the performance of complex systems or tasks. Machine learning is, for instance, used to improve the control of robot swarms, which are groups of identical, and generally small and low-cost, systems that operate as a coherent entity.[58]

A more recent achievement of machine learning relates to creativity. Experiments with a machine learning approach known as generative adversarial networks (GAN) have led to the creation of AI systems that create original, ultra-realistic images, sounds or written stories.[59] This breakthrough has both positive and negative implications. On the one hand, it could help a machine learning system to generate new data to train itself; on the other hand, it could create digital fakery for criminal or information warfare purposes.

Machine learning holds great promise, but like other approaches to AI engineering it has limitations. The first—and perhaps most salient—is its dependence on training data. Data is the 'fuel that powers the engine of machine learning'.[60] To be taught, machine learning systems need to be provided with large volumes of real-world examples. In order to recognize a type of object in an image (e.g. a car, a bus or a dog), a computer vision system would need to be trained with millions of pictures of that type of object. The quality of the data on which the systems are trained is equally important: systems powered by machine learning are only as good as the data on which they are trained.[61] If the training data set is not representative, the system might fail or perform poorly. Research has shown, for instance, that facial recognition systems trained with data sets that primarily include images of white-skinned men are more likely to misidentify the faces of women or people with darker skin.[62] Nonetheless, if trained with a sufficiently large and representative data set, machine learning can effectively identify errors.

Second, machine learning systems, like traditional AI systems, are brittle: that is, they are limited by the boundaries of their programming and they only work reliably for the intended tasks and operating environment. Even if they can outperform humans for many narrow tasks, they still lack what humans understand as basic common sense. That means that they can be easily fooled or that they may fail in idiotic or unpredictable ways—according to human standards. One facial recognition system, for instance, could not tell the difference between an actual person and a picture of a picture of a person.[63]

Third, machine learning remains an immature technology from a safety and security standpoint, because machine learning systems, particularly those that rely on deep neural networks, operate like black boxes—the internal workings are hidden or hard to understand. It is particularly difficult for humans to understand what such systems have learned and hence how they might react to input data that is different

[57] Polyakov, A. 'Machine learning for cybersecurity 101', Towards Data Science, 4 Oct. 2018.

[58] Hüttenrauch, M., 'Guided deep reinforcement learning for robot swarms', Master's thesis, Technische Universität Darmstadt, Aug. 2016.

[59] Condliffe, J., 'Dueling neural networks: by playing cat-and-mouse games with data, a pair of AI systems can acquire an imagination', *MIT Technology Review*, vol. 121, no. 2 (Mar./Apr. 2018).

[60] Scharre and Horowitz (note 48), p. 5.

[61] Gershgorn (note 50).

[62] Lohr, S., 'Facial recognition is accurate if you are a white guy', *New York Times*, 9 Feb. 2018.

[63] Nguyen, A., Yosinski, J. and Clune J., 'Deep neural networks are easily fooled: high confidence predictions for unrecognizable images', *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2015)*, Proceedings, 7–12 June 2015 (Institute of Electrical and Electronics Engineers (IEEE): 2015), pp. 427–36, p. 427.

from the data used during the training phase. In other words, machine learning systems are potentially unpredictable. They might fail in ways that humans could not have foreseen at the design stage.[64]

Recent advances in AI have been driven by the civilian sector. Companies with backgrounds in information and communications technology (ICT), such as Apple, Intel and Microsoft, and Internet giants, such as Google, Amazon, Baidu and Facebook, are leading innovation.[65] They have large financial resources at their disposal, which allow them to recruit the most talented AI researchers and engineers and to acquire innovating start-up companies. They also have access to gigantic data sets that allow them to train powerful machine learning algorithms. Many of these companies are based in the USA or China. However, there are also innovative companies in other countries, and important R&D is carried out around the world, including in developing countries. AI is a technology with a low barrier of entry, as it does not necessarily require large financial resources or infrastructure. An AI student could develop a game-changing algorithm from her or his bedroom.[66] The AI community is also open with regards to disseminating findings. The information to design AI tools, such as facial recognition systems, is widely available online. Only two factors limit an actor, whether a state or a non-state actor, from making advances in AI: access to AI experts and access to data. Countries that lead in AI are those that have the universities, research institutions and companies that can train and retain competent AI engineers and have a large volume of high-quality data on which systems can be trained.

Recent advances in machine learning have unlocked major possibilities in the field of biology as they can help researchers make sense of complex sets of biological data. The ability of machine learning to link, correlate and analyse data is, for instance, particularly useful for interpretation of the functions of genes and the identification of genetic markers responsible for certain diseases.[67] It is now possible to predict how likely someone is to develop diseases such as type 1 diabetes or breast cancer or to develop certain traits and capabilities—such as height or resistance to specific pathogens—that result from complex genetic influences.[68] Machine learning also unlocks many new and varied possibilities for the analysis of the vast amount of health data to which hospitals and health authorities have access. Pattern recognition capabilities can unravel how patients react to different viruses, chemicals or environments and can detect which patients are more likely to be affected by specific diseases based on genomic, physiological, health, environmental and lifestyle data. A number of hospitals have digitized their patient records for that purpose.[69] Several companies, including Apple, are also considering merging data contained in individuals' medical records with lifestyle-related data from their smartphone (e.g. data about how much they walk, exercise or sleep) to develop AI systems that improve the accuracy of health predictions. However, such efforts are being met by increasing concern from individuals, civil society organizations and states about privacy protection.[70]

[64] Righetti, L., 'Emerging technology and future autonomous systems', *Autonomous Weapon Systems: Implication of Increasing Autonomy in the Critical Functions of Weapons*, Report of expert meeting, Versoix, Switzerland, 15–16 Mar. 2016 (International Committee of the Red Cross: Geneva, Aug. 2016), pp. 36–39.

[65] Boulanin, V., *Mapping the Innovation Ecosystem Driving the Advance of Autonomy in Weapon Systems*, SIPRI Working Paper (SIPRI: Stockholm, Dec. 2016).

[66] Condliffe (note 59).

[67] Regalado, A., 'Will you be among the first to pick your kids' genes', *MIT Technology Review*, vol. 121, no 1 (Jan./Feb. 2018), pp. 16–18.

[68] Torkamani, A. and Topol, E., 'Your genome, on demand', *MIT Technology Review*, 23 Oct. 2018.

[69] Sennaar, K., 'How America's 5 top hospitals are using machine learning today', TechEmergence, 13 Apr. 2018.

[70] Bresnick, J., 'Top 10 disrupting companies to watch the healthcare space', Health IT Analytics, 5 July 2018; and Pauwels, E. and Vidyarthi, A., 'Who will own the secrets in our genes? A U.S.–China race in artificial intelligence and genomics', Wilson Briefs, Wilson Center, Nov. 2017.

The use of machine learning for biological and medical analysis could have many societal benefits. To begin with, it facilitates the earlier detection and treatment of major and complex diseases. The earlier a disease is diagnosed, the more likely it will be cured or controlled. Genomics experts hope to be able to identify genetic markers responsible for cancer or to detect cancer DNA in a simple blood test.[71] Machine learning analysis of genomic and health data could also improve the possibility of developing personalized treatments, including personalized vaccines and antibiotics, personalized treatment relying on virology and microbe research, personalized cancer treatments, and treatment involving in vivo gene editing.[72] Personalized medicine is in its early days but a number of companies, such as Tempus, IBM and Pfizer, are actively exploring the possibilities.[73] However, these efforts remain mostly focused on understanding how machine learning could help identify genetic markers or patients that should or could be targeted by personalized treatments.[74] According to two observers, there is 'still pervasive uncertainty about how accurate deep machine-learning will be in drawing useful interferences between the different datasets that make our biology'.[75] Moreover, biotechnology experts have much more work to do before they can exploit the full potential of new genetic technologies, such as gene therapies and genome-editing techniques. While both technologies have made great strides in the past five years, to develop and test them for therapeutic use in humans is still so complex that they might not benefit patients for a decade.[76]

Opportunities arising from the convergence of biology and artificial intelligence

For governments, the convergence of biology and artificial intelligence creates a wide range of opportunities.

In the military realm, it could generate new possibilities for human enhancement: 'the process of endowing an individual with an ability that goes beyond the typical level or statistically normal range of functioning for humans generally'.[77] The use of machine learning for DNA analysis and genomic prediction could help to better identify appropriate candidates for human enhancement procedures, particularly those that involve gene editing. AI could enable the military to identify what a soldier needs and then to predict how that soldier might react to enhancement. Based on genomic and health data, the military could also determine what types of personalized medical treatment (vaccine, antibiotics or other drug treatment) a soldier would require for a specific mission. The treatment could, for example, enhance the soldier's resistance to a specific pathogen and even, potentially, a specific type of biological weapon. Machine learning and traditional AI algorithm could be used to make predictive models that would help predict the impact of the enhancement on the soldier's genome and health.

Recent advances in AI also hold great promise in biosecurity. AI could help the national and international authorities in charge of preventing and managing biological incidents—be they intentional or naturally occurring—to gain better situational awareness and increase their ability to make informed decisions in critical situations. For instance, machine learning could be used to merge data from multiple sources,

[71] Dunlap, G. and Pauwels, E., 'The intelligent and connected bio-labs of the future: promise and peril in the fourth industrial revolution', Wilson Briefs, Wilson Center, Sep. 2017, p. 4.

[72] Regalado (note 53).

[73] Pauwels and Vidyarthi (note 70).

[74] Pauwels and Vidyarthi (note 70).

[75] Pauwels and Vidyarthi (note 70), p. 5.

[76] Pauwels, E., 'The new bio-citizen: how the democratization of genomics will transform our lives from epidemics management to the internet of living things', Wilson Briefs, Wilson Center, May 2017.

[77] Harrison Dinniss, H. A. and Kleffner, J. K., 'Soldier 2.0: military human enhancement and international law', *International Law Studies*, vol. 92 (2016), pp. 432–82, p. 434. See also Boulanin, V. and Verbruggen, M., *Article 36 Reviews: Dealing with the Challenges Posed by Emerging Technologies* (SIPRI: Stockholm, Dec. 2017).

including social media, in order to detect, track or forecast biological incidents.[78] A group at Carnegie Mellon University has designed a program that detects new symptoms by scanning keywords in social media sources.[79] The program assigns a significance value to new and old symptoms. If new symptoms occur repeatedly in the data, then scientists can assess whether they are significant. Machine learning could also help with the integration of data collected in a disease-affected zone by portable genomic-sequencing laboratories, such as the laboratory-in-a-box used in Guinea and Brazil to track the evolution of the Ebola and Zika viruses.[80] With regard to forecasting, machine learning could also be used to predict which diseases are likely to emerge or spread in a specific area based on the combination of historical or real-time data on disease outbreaks with variables such as climate changes, movements of people, agricultural patterns or water sources.[81]

Machine learning has great potential in investigating biological incidents. The increased digitization of pathogen data has allowed for the development of baseline data and pathogen reference data that facilitate the identification and characterization of biological incidents.[82] In that context, machine learning algorithms could be used for what cybersecurity professionals call 'outlier detection'.[83] In the same way that machine learning is used by ICT security experts to discover unknown computer viruses and suspicious online activities, a biosecurity professional could use it to detect and characterize unknown biological agents.[84] Machine learning could also support the determination of whether a biological incident is the result of deliberate action or is naturally occurring by, for example, facilitating the identification of genetically engineered biological weapons. Detecting genetically engineered organisms is already feasible, but it can take weeks using current capabilities and available resources, which is a substantial time when responding to a biological incident. Machine learning could significantly speed up the detection process. The use of AI for what the independent expert Ralf Trapp calls 'intelligent black box investigations' may, however, cause problems related to interpreting evidence and demonstrating links between an incident, any evidence and the responsible party to a political (or legal) audience.[85] The above-mentioned black box problem means that AI cannot yet be used to demonstrate culpability. In an investigation, a conclusion arrived at by AI cannot be understood easily since the process by which the conclusion was drawn is not necessarily transparent or explainable to humans. According to Trapp, the conclusions may therefore not be acceptable in international compliance-assessment forums (e.g. the UN Security Council when scrutinizing the results of a mission under the UN Secretary General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons[86]) and they may only be acceptable in national criminal proceedings subject to certain conditions.[87]

[78] Awad, M., 'Artificial intelligence for biosurveillance/real-time situational awareness/US Department of Homeland Security', Pandora Report, 3 Mar. 2018.

[79] Carnegie Mellon University, Event and Pattern Detection Laboratory (EPD Lab), 'Projects', [n.d.].

[80] Pauwels (note 76).

[81] For concrete examples see Chae, S., Kwon, S. and Lee, D., 'Predicting infectious diseases using deep learning and big data', *International Journal of Environmental Research and Public Health*, vol. 15, no. 8, article 1596 (July 2018); and Brockmann, D., Schaade, L. and Verbeek, L., '2014 Ebola outbreak: worldwide air-transportation, relative import risk and most probable spreading routes', Research on Complex Systems, Robert Koch Institute for Theoretical Biology, Humboldt University of Berlin, 4 Aug. 2014.

[82] Bohm, E. and Lentzos, F., 'Technical briefing note on developments in science and technology and governance in relation to biological weapons', Unpublished briefing paper, SIPRI, Nov. 2018.

[83] Polyakov (note 57)

[84] 'Gingko Bioworks announces biosecurity initiative using deep learning to reduce the global threat of biological weapons and infectious diseases', Cision PR Newswire, 27 June 2018.

[85] Trapp (note 41).

[86] On the mechanism see United Nations, Office for Disarmament Affairs, 'Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons', [n.d.].

[87] Trapp (note 41).

Risks and challenges arising from the convergence of biology and artificial intelligence

Applications of AI in the field of biotechnology raise multiple risks related to the development and use of biological weapons.

First, the use of AI for biological and medical analysis could open up the possibility of ultra-targeted biological warfare. In past biological weapon programmes, the targeting was simply by the geographic location of the intended victims. Advances in biotechnology may mean that a malicious actor could deploy a biological agent over a broad geographic area but only affect targeted individuals. Using the knowledge gained through AI from genomics and health data, a malicious actor could engineer biological weapons that would harm only a specific individual or group of individuals, based on their genes, prior exposure to vaccines or known vulnerabilities in their immune systems.[88] According to a recent US report on the biodefence vulnerabilities posed by synthetic biology, that possibility—which has been feared but deemed implausible for decades—may become increasingly feasible due to the widespread availability of health and genomic data and the increased sophistication of AI.[89] There are, however, some barriers that could reduce the effectiveness of such targeted biological weapons. The level of funding and expertise and the technical base required for the design of a targeted biological weapon mean that only a resourceful and motivated actor would be likely to explore this possibility.[90] If the purpose is to harm a specific individual or group, most malevolent actors would surely resort to more low-tech or direct methods, such as firearms or poison. In other words, the application of AI for ultra-targeted biological warfare may not represent an urgent or major risk.

Second, AI could make the development of advanced biological agents easier, at least theoretically. The digitization of biological data combined with the increasing accessibility of synthetic biology has already drastically reduced the barrier of entry into the development of biological weapons. A malevolent actor can already tamper with characteristics of a pathogen without having direct access to a physical laboratory. With machine learning, that malevolent actor could optimize mutations of that pathogen that would increase, for instance, the transmissibility or virulence.[91] Fortunately, there are still a number of barriers that would limit the ability of non-state actors to effectively produce highly transmissible or targeted viruses. To begin with, a laboratory or some other facility would still be needed to produce the pathogen (but see below on cloud laboratories). More importantly, developing a viable virus requires significant expertise, which most terrorist groups do not have or would have difficulties accessing. Converting DNA into a viable virus is hard, with the degree of difficulty depending on the type of virus and the process of inserting bacteria DNA into a living cell (i.e. booting). Succeeding in this and then scaling up the synthetic organism in the laboratory is even more difficult and requires a significant level of expertise.[92]

Third, the proliferation of AI applications in biotechnology increases the exposure of digitized biological data to cyberattacks. As explained by two expert observers, companies that store genomic or health data or use AI to process that data for commercial purposes could be targeted by malevolent actors who are seeking to steal raw genomic and health data or the data and algorithms arising from the data analytics.[93] This risk is aggravated by the fact that companies that gather genomic and

[88] National Academies of Sciences, Engineering and Medicine (note 8), p. 109.
[89] National Academies of Sciences, Engineering and Medicine (note 8), p. 109.
[90] National Academies of Sciences, Engineering and Medicine (note 8), p. 108.
[91] Dunlap and Pauwels (note 71).
[92] National Academies of Sciences, Engineering and Medicine (note 8), pp. 108–109.
[93] Pauwels, E. and Vidyarthi, A., 'How our unhealthy cybersecurity infrastructure is hurting biotechnology', Wilson Briefs, Wilson Center, Mar. 2016; and Pauwels and Vidyarthi (note 70).

heath data using smartphone apps often use cloud-based data storage, which might be more vulnerable to cyberattacks due to their connectivity. The stolen data could then be exploited by criminals who may seek to use it for industrial espionage or fraud (e.g. identify theft) or to extort money. Bioterrorists could use such stolen data when engineering the hypothetical ultra-targeted biological weapons described above.

Biology plus robotics

What is robotics?

Robotics is a field of science and engineering dedicated to the development of robots—that is, 'self-contained artificial machine[s] that [are] able to sense [their] environment and purposefully act within or upon that environment'.[94] As a scientific discipline, robotics is at the crossroads between mechanical engineering, electrical engineering and computer science.[95] As an industrial sector, robotics is hard to delineate as it can be applied in almost all industries, from automotive and aerospace manufacturing, via arms production to the pharmaceutical industry.

Most existing studies in the field of robotics make a distinction between industrial robots and interactive and service robots. An industrial robot is an 'automatically controlled, reprogrammable, multipurpose manipulator' that can be programmed to execute tasks in a controlled environment.[96] It has no decision-making intelligence or autonomy—it only executes scripted actions. A service or interactive robot is any other robot that is intended to assist humans in various tasks.[97] Service or interactive robots come in all shapes and sizes—from small robotic insects to large self-driving cars—and have a wide range of military and commercial applications. When they need to evolve in dynamic conditions, they usually require some level of autonomy in their functioning.

Both types of robot can be usefully applied in the field of biotechnology. Industrial robots can be programmed to execute laboratory experiments in an automated fashion, while service robots can be used to transport within or between laboratories or to disseminate biological substances in predefined areas.

The state of the art in robotics

Broadly speaking, R&D in robotics can be divided into two generic categories.[98] The first consists of efforts that focus on the development and integration of the hardware parts of robots. R&D efforts in the second category focus on the development of the hardware and software that control robot behaviour.

R&D in the first category has most impact on the actuators and the end-effectors of a robot. End-effectors are 'the physical devices that assert physical force on the environment: wheels, legs and wings for locomotion, as well as grippers and, of course, weapons', while actuators are 'the "muscles" that enable the end-effectors to exert force, and include things such as electric motors, hydraulic cylinders and pneumatic cylinders'.[99] Overall, this R&D aims to improve, among other things, the agility, endurance, flexibility, hardiness, size or velocity of robots.

[94] Winfield, A., 'What is a robot', Alan Winfield's Web Log, 31 May 2006.

[95] This introduction to robotics is based on Boulanin (note 65), pp. 19–26.

[96] International Federation of Robotics (IFR), 'Industrial robots', [n.d.]. The IFR definition is, in turn, based on the ISO definition.

[97] International Federation of Robotics (IFR), 'Service robots', [n.d.].

[98] The discussion on robotics R&D is based on Boulanin, V. and Verbruggen, M., *Mapping the Development of Autonomy in Weapon Systems* (SIPRI: Stockholm, Nov. 2017), pp. 90–92.

[99] Boulanin and Verbruggen (note 98), p. 11.

Through this research, robots have also become increasingly cheaper, smaller, softer and more connected in recent years.

1. *Cheaper*. Robots are becoming less and less expensive to produce, partly due to the boom in the smartphone industry, which has had a major impact on the availability and size of key components: batteries, computer chips and sensors, from video cameras to inertial measurement units.[100] Recreational drones that include advanced features such as GPS waypoint navigation and video-based sense-and-avoid capability can be purchased for only a few hundred dollars. The projected growth of the driverless car market is also expected to further reduce the cost of larger robotics components, such as light-detection and ranging (LIDAR) systems or large batteries.

2. *Smaller*. The development of small and miniature robots has been facilitated by the miniaturization of electronic components, which is a wider trend within the ICT industry. Moreover, progress in nanotechnology has enabled the creation of nanorobots: robots with a size of 0.1–10 micrometres that are constructed at nanoscale from molecular components.[101]

3. *Softer*. Opportunities for the development of soft robots have arisen from advances in additive manufacturing. It is now feasible to develop robots that are made entirely from soft and transformable material, such as silicone.[102]

4. *More connected*. Advances in the Internet of things and cloud computing have also unlocked many possibilities in robotics. The Internet of things allows robots to share computational power and data in real time, through machine-to-machine (M2M) and machine-to-cloud (M2C) communication. Cloud computing removes the need to build a computing device within the robotic system, which allows engineers to build cheaper and potentially more sustainable robotic platforms, as these may not need to be regularly upgraded with new and more powerful computer chips.[103] Cloud robotics has opened up new possibilities for online learning as it enables robots to directly share what they have learned with each other: when a robot learns something, all the robots that are connected to that cloud learn it too.[104]

R&D efforts in the second category—the development of hardware and software that control robot behaviour—can be further divided into two subcategories: those that seek to improve the ability of humans to remotely control the behaviour of the robot ('telerobotics') and those that seek to develop robots capable of governing their own behaviour ('AI robotics', 'cognitive robotics' or 'autonomous robots research').

Great strides have been made in the field of telerobotics in recent years, notably due to the widespread availability of virtual reality (VR) devices that give the human controller an increasingly immersive experience. VR glasses allow a user to see through a robot's cameras, while haptic control devices recreate the sense of touch by applying force, vibration or motion to the user as the robot's sensors respond to its environment. The emergence of brain–computer interfaces—devices that allow a human to control prosthetics or other devices, including drones, with his or her mind—is also notable because of their convergence with the field of biotechnology.[105] Such a device can also be used to monitor or exert control over the mental state of the

[100] Boulanin (note 65), pp. 21–26.

[101] Diamandis, P. H., 'Nanorobots: where we are today and why their future has amazing potential', Singularity Hub, 16 May 2016.

[102] Sklar, S., 'Meet the world's first completely soft robot', *MIT Technology Review*, 8 Dec. 2016.

[103] Hu, G., Tay, W. and Wen, Y., 'Cloud robotics: architecture, challenges and applications', *IEEE Network*, vol. 26, no. 3 (May/June 2012), pp. 21–27, pp. 21–23.

[104] Thielman, S., 'Man behind Darpa challenge: robots will soon learn from each other', *The Guardian*, 14 June 2015.

[105] Miranda, R. A. et al., 'DARPA-funded efforts in the development of novel brain–computer interface technologies', *Journal of Neuroscience Methods*, vol. 244 (Apr. 2014), pp. 52–67.

person that wears it. For example, extracranial interfaces—that is, electrodes placed on the outside of the skull (as opposed to intracranial interfaces inside the skull)—are used to monitor stress levels or stimulate part of the brain to increase concentration.

The field of autonomous robot research has largely benefited from the recent advances of machine learning as these have enhanced the perceptual intelligence of robots. The fact that autonomous robots are increasingly good at perceiving their environment means that they can recognize objects and people and also (simple) situations with an increasing degree of certainty.[106] Progress made in optimal control theory (a branch of engineering and mathematics that deals with the behaviour of dynamic systems) has also made autonomous robots increasingly agile.[107] Boston Dynamics, a company that develops robots with legs, regularly makes headlines when it unveils the latest achievement of its humanoid robot Atlas. Its successes include walking outdoors on an uneven terrain, jumping over obstacles, doing a backflip, and jumping upwards and sideways.[108] Combined, these achievements unlock important possibilities for the deployment of robots in unstructured environments that are difficult to access with wheeled robots.

The limited durability of batteries remains a major engineering challenge. Robots that run on a battery can rarely operate for extended periods. For instance, Atlas cannot conduct missions that last longer than an hour.[109] Small drones, such as the DJI Phantom, can only fly for half an hour.[110] For power-intensive tasks, robots need to be tethered to an energy source or use a fuel engine, which makes their use in certain environments difficult.[111]

Programming robots to do tasks autonomously is hard when the tasks to be executed are abstract and ill-defined or if the environment in which the system will operate is not highly predictable.[112] As tasks become more abstract or ill-defined, it becomes harder to formulate them in mathematical terms, and hence in programming terms. The less predictable the environment, the harder it is to model and the more perceptual and decision-making intelligence the systems need to have. In the field of biotechnology, this means that automating a task, such as manipulating an object, is much easier to achieve inside a laboratory than outside. This is the reason why the robots that are used to manipulate hazardous (chemical, biological or radiological) material in emergency operations are generally teleoperated by humans. The technology is not at the stage where autonomous robots can reliably execute complex operations in unstructured environments outdoors.

The barriers to entry in the robotics sector are increasingly low. Programming a robot has become fundamentally easier thanks to the introduction of open-source software architectures, such as Robot Operating System (ROS).[113] ROS is not operating software per se, but 'a collection of tools, libraries, and conventions that aim to simplify the task of creating complex and robust robot behavior across a wide variety of robotic platforms'.[114] It provides a basic software architecture on which researchers and companies can build their robotics applications (including proprietary applications).[115] Open-source software is popular because it allows companies to

[106] Boulanin and Verbruggen (note 98), p. 15.
[107] Boulanin and Verbruggen (note 98), p. 92.
[108] E.g. Simon, M., 'Watch Boston Dynamics humanoid robot do parkour', *Wired*, 10 Nov. 2018.
[109] Ackerman, E., 'Atlas DRC robot is 75 percent new, completely unplugged', *IEEE Spectrum*, 20 Jan. 2015
[110] DJI, 'Phantom 4 specs', [n.d.].
[111] Hern, A., 'US marines reject BigDog robotics packhorse because it's too noisy', *The Guardian,* 30 Dec. 2015.
[112] Boulanin and Verbruggen (note 98), pp. 12–16.
[113] US Department of Defense (DOD), Defense Science Board, *The Role of Autonomy in DoD Systems*, Task Force Report (DOD: Washington, DC, July 2012), p. 61.
[114] Open Source Robotics Foundation, 'About ROS', [n.d.].
[115] Poubel, L., 'The robotics revolution is open source', 4 May 2016, Scientific Computing.

focus their research efforts on the final application layer rather than the underlying software infrastructure—and hence to save cost. It also permits them to build on each other's applications.

Components are increasingly accessible because commercial off-the-shelf robotics systems are increasingly affordable.[116] This is particularly true for small robotics devices. These systems do not need a large support infrastructure and can be developed using relatively inexpensive civilian off-the-shelf components or directly acquired as pre-assembled platforms. This means that these systems are accessible to any state, but also that they are available to non-state actors and individuals. High-end robotic products, such as large military-grade UAVs or industrial robots that can manipulate material at a nanoscale, are harder to develop or acquire, given that they require more advanced programming (which itself requires human expertise), expensive components and infrastructure to operate.

Opportunities arising from the convergence of biology and robotics

Advances in robotics have already had a palpable impact on the field of biotechnology, beginning with how experiments are conducted in the laboratories of universities, research centres and biotechnology companies. An increasing number of tasks that would previously have required the physical work of a researcher (e.g. transferring miniscule volumes of DNA or separating proteins on a gel) are handed over to robots.[117] The benefits of robotization of laboratory work are manifold.

First, robots can make the laboratory increasingly automated, which in turn improves the efficiency and reproducibility of experiments.[118]

Second, it improves productivity as robots can potentially run experiments for 24 hours a day, every day of the week, without the intervention of a human worker.

Third, robotization offers researchers the possibility to decouple themselves from the laboratory. A researcher can now conduct an experiment remotely via a cloud laboratory—a robotic laboratory that can be controlled over the Internet. Cloud laboratories are a small revolution in the field of biotechnology as they open up the opportunity to conduct advanced laboratory experiments to an increasing number of actors.[119] According to Emerald Therapeutics, a US company that provides this type of service, its robots can perform over 60 different task (with a nearly equal number of tasks currently under development).[120] The only requirement is that the scientist sends samples to the company and orders online the types of task she or he would like to conduct.

Finally, robotization of laboratory work is also generating opportunities to exploit advanced AI in the biological sphere. Robotic laboratories generate massive amounts of data (e.g. through automated screening of pathogen genomic data) that can then be analysed by AI systems. In April 2018 the Defense Advanced Research Projects Agency (DARPA), an agency of the US Department of Defense, awarded a contract to two US companies, Transcriptic and Ginkgo Bioworks, to conduct a project that aims to improve the engineering of biological systems through the analysis of data produced by robotic laboratories.[121]

Advances in robotics are also important for biosecurity. Robotic systems in general can support the detection, surveillance, prevention and response to pathogens that

[116] For a detailed discussion on this see Boulanin and Verbruggen (note 98), pp. 77–80.

[117] Dunlap and Pauwels (note 71), p. 4.

[118] Check Hayden, E., 'The automated lab', *Nature*, 3 Dec. 2014, pp. 131–32.

[119] Dunlap and Pauwels (note 71).

[120] Emerald Cloud Laboratory, 'How the ECL works', [n.d.]; and Emerald Cloud Laboratory, 'Experimental capabilities', [n.d.].

[121] Haydon, I., 'DARPA awards Ginkgo Bioworks and Transcriptic $9.5M to bring AI into the lab', Synbiobeta, 12 Apr. 2018.

present biosecurity risks. They thereby enhance the global ability to detect and treat disease, whether caused by a naturally occurring pathogen or an accidental release or as the result of a malevolent act.[122]

In the detection and monitoring of biological incidents, one emerging technology holds great promises: 'laboratory on a chip' (LOC) technology.[123] LOC devices integrate laboratory functions in a single computer chip.[124] LOCs are able to handle fluid volumes less than picolitres (10^{-12} litres) and conduct automatically a wide range of tasks including detecting and monitoring pathogens. In addition to saving humans the effort of conducting the complex manipulation required, LOC technology can speed up the detection of biological incidents by enabling medical diagnostics at the point of care. By removing the need to send test samples for laboratory analysis, LOC technology permits medical doctors to detect pathogens in a patient in a matter of minutes rather than days.[125] LOC technology promises to be particularly useful when diagnostics need to be conducted in a remote or resource-poor location or in a situation that requires rapid treatment (e.g. where exposure to biological warfare agents is suspected).

Advances in robotics also provide new possibilities for the prevention and response to biological incidents. Drones can, for instance, be used to quickly deliver medicines and blood supplies to remote locations. Some companies already offer this service in the USA, Switzerland and some countries in Africa.[126] Robots can also be used to handle hazardous (chemical, biological or radiological) material in an emergency situation. Modern law enforcement agencies usually already have such systems.

Risks and challenges arising from the convergence of biology and robotics

The robotization of laboratory work has the potential to make the development of biological weapons easier, faster and possibly more accessible to a wider range of actors. A report from the US National Academies of Sciences notes that:

> Automation tools allow researchers to screen ever-larger collections of genetic sequences or physical samples for a wide variety of properties; it is now possible to produce and screen hundreds of thousands of clones and variants in a matter of weeks. Malicious actors could take advantage of these capabilities to, for example, streamline testing of agents, increase fidelity and fine-tune targeting . . .
>
> By enabling massively scaled-up experimentation and testing, these tools can significantly shorten the time frame of the Design–Build–Test cycle overall and potentially improve the likelihood of producing the desired biological functionality.[127]

Certainly, such malicious actors would still need resources to acquire this robotics technology and significant expertise to further develop the toxin into a viable biological weapon. Actors that do not have access to a laboratory could use cloud laboratory services; however, these services require a formal affiliation with a company or university and so do not permit total anonymity.[128]

[122] Meeting of the States Parties to the BTWC, Meeting of Experts on Review of Developments in the Field of Science and Technology Related to the Convention, 'Report of the Scientific Advisory Board of the Organisation for the Prohibition of Chemical Weapons 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', Note by the Implementation Support Unit, BWC/MSP/2018/MX.2/WP.7, 10 Aug. 2018.

[123] Dunlap and Pauwels (note 71).

[124] Volpatti, L. R. and Yetisen, A. K., 'Commercialization of microfluidic devices', *Trends in Biotechnology*, vol. 32, no. 7 (July 2014), pp. 347–50.

[125] Gorjikhah, F. et al., 'Improving "lab-on-a-chip" techniques using biomedical nanotechnology: a review', *Artificial Cells, Nanomedicine, and Biotechnology*, vol. 44, no. 6 (Jan. 2016), pp. 1609–14.

[126] E.g. Swiss Post, 'Drone to transport laboratory samples across Lake Zurich', Press release, 22 June 2016; and CyPhy Works, 'UPS and CyPhy Works test drone for urgent commercial delivery', 23 Sep. 2016.

[127] National Academies of Sciences, Engineering and Medicine (note 8), pp. 89–90.

[128] Dunlap and Pauwels (note 71).

Robotics also provides new and worrying possibilities for the delivery of biological weapons. Commercial off-the-shelf drones could be easily repurposed to deliver biological weapons both in a targeted way and on a large scale. It is not difficult to image that agricultural drones that are used for crop monitoring and crop dusting could be used for agroterrorism (i.e. terrorist acts targeting the agricultural industry or food supply of a population, in particular by using biological agents against livestock or crops). Recreational drones, such as the DJI Phantom, could also be fitted with spray tanks and used to spray a pathogen in public or crowded spaces. It should be stressed, however, that if drones make the delivery of biological weapons easier, the preparation of the actual delivery vector remains difficult. If the attack involves aerosol dispersal of a biological agent, which would be most likely in the case of delivery by drone, the attacker would have to make sure that the agent not only has the optimal particle size for inhalation but is also able to withstand freeze drying packaging processes, long-term storage and adverse environmental conditions such as ultraviolet sunlight or extreme temperatures. Such requirements may impose significant barriers to development of biological weapons, even with available biotechnology—especially for a non-state actor.

Miniaturized robotics systems could theoretically be used for more targeted use of biological weapons. Insect-sized drones could be used to contaminate a specific individual. Nanorobots or nanodevices that are capable of tissue diagnosis or repair could also be repurposed for the delivery of pathogenic agents.[129] Fortunately, micro- and nanorobots remain, for now, experimental systems.[130] They have not yet found large commercial application, so it would be difficult (albeit not impossible) for a terrorist group to access them. The risk of their use in biological weapons therefore remains low.[131]

The risk landscape of the convergence of biology and emerging technologies

The convergence of modern biotechnology with technologies such as additive manufacturing, artificial intelligence and robotics is bound to have an impact on the landscape of risk in biological arms control and biosecurity. While the applications and possibilities offered by the convergence of biotechnology with these other areas of technology may vary greatly, they raise a common set of risks and challenges as far as the development, production and use of biological weapons is concerned.

First, they have in common the ability to facilitate steps in the development or production of biological weapons and their delivery systems. Each emerging technology could, in its own way, enable the automation of specific operations that previously required manual manipulation or analysis by a human. AI could facilitate the analysis of genetic information that identifies the genetic markers or base pairs that need to be edited or mutated in order to alter the transmissibility of a pathogen, while a cloud laboratory could be used to automate certain laboratory tasks and thereby reduce the need for facilities and trained laboratory staff. AM could make the production of drone components for the delivery of biological weapon more accessible. Fortunately, some tacit knowledge barriers remain in place. However, the steps that can be simplified by automation could enable many of the development, production and delivery processes for biological weapons. Moreover, further technological advances in AM, AI, robotics

[129] Patra, J. K. et al., 'Nano based delivery systems: recent development and future prospects', *Journal of Nanobiotechnology*, vol. 16, no. 71 (19 Sep. 2018).

[130] Diamandis (note 101).

[131] Kosal, M. E., 'The security implication of nanotechnology', *Bulletin of the Atomic Scientists*, vol. 66, no. 4 (July/Aug. 2010), pp. 58–69.

and other emerging technologies such as nanotechnology could decisively amplify this simplification.

Second, AM, AI and robotics could enable more targeted delivery of biological weapons. Recent advances in AI could enable the design of a pathogen that would affect only specific individuals or groups of people. Meanwhile, progress in AM and robotics have made new and more advanced delivery mechanisms available to an increasing number of actors—including terrorist organizations. While these technologies may not pose an imminent risk at this stage, the gathering of and access to the necessary genomic data, for example, has already become a field of competition for some companies, which also poses ethical and privacy risks. Although this may prove to be the first step towards the development of genetically targeted weapons, such data has not yet been successfully used in this way. Meanwhile, although drones have already become more common in asymmetric warfare, there are no known cases of their use to disperse weaponized biological agents.

Third, each of these emerging technologies is vulnerable to cyberattacks due to increased digitization. This means that their systems or the data that they require could be stolen, misused or manipulated, including for activities that could facilitate the developments, production or delivery of biological weapons or cause critical malfunctions in related equipment.

Fourth, none of these emerging technologies is easy to control, notably because their development is mainly driven by the civilian and private sectors and is therefore beyond direct governmental control. Governments are trying to exert control, for instance by funding R&D directly or by controlling the funding of and foreign investment in key firms, but they may not have the influence that they previously held in strategic industries. This problem of control is further complicated by the fact that a large portion of these technologies is digital information that can be easily transferred. Traditional export and customs controls and visa screening may no longer pose sufficient barriers. Verifying and controlling digital or other types of intangible transfer of technology are more difficult than controlling traditional transfers of goods, as measures such as digital forensics, recordkeeping requirements and audit procedures are often weaker and less commonly applied. Moreover, the speed of development of most of these technologies makes the definition of long-lasting technical parameters for possible export controls or transparency measures elusive. This not only inhibits effective regulation but also creates considerable difficulties for scientists and developers when classifying and handling any risks created by transferring or making their technology available—and thus inhibits effective compliance practices.

Existing frameworks for the governance of biological weapons currently only provide limited coverage of the direct and indirect risks and challenges associated with the convergence of biotechnology with these emerging technologies. Chapter 3 discusses the governance frameworks and their efforts to address these risks in more detail. In addition to increasing understanding of ongoing developments in science and technology, each of these frameworks needs to raise awareness among a growing number of actors and develop measures to address issues that they may have only just started to consider in the biosecurity context. For example, establishing standards for genomic data security and privacy would be critical to reducing the risk of misuse of data for biological weapon development. However, companies and governments involved in collection and analysis of genomics data have barely started considering this issue for personal data protection, let alone biosecurity.

3. Governing the risks of the convergence of biology and emerging technologies

This chapter explores the extent to which the main governance frameworks for biosecurity and biological arms control are adequately equipped to deal with the risks and challenges identified in chapter 2. It starts with a brief introduction to the governance frameworks. It then explores the extent to which these governance frameworks currently cover additive manufacturing, artificial intelligence and robotics. Finally, it identifies the main challenges and limitations to the effectiveness of these governance approaches and discusses a number of good practices that could help mitigate them.

Governance frameworks for biosecurity and biological arms control

The current governance frameworks in the field of biosecurity and biological arms control include a wide range of treaty regimes and other oversight and self-regulatory instruments (see table 3.1). They include international and regional agreements; national laws and regulations and, in the case of the European Union (EU), also EU legislation; policies and guidelines; codes of conduct; terms and conditions of funding instruments; and education and awareness-raising exercises on biosafety and biosecurity.[132]

The main contemporary multilateral arms control treaty on biological weapons is the 1972 Biological and Toxin Weapons Convention. The convention, which entered into force in 1975, builds on the 1925 Geneva Protocol.[133] The BTWC prohibits the development, production, acquisition, transfer and stockpiling of 'microbial or other biological agents, or toxins . . . that have no justification for prophylactic, protective or other peaceful purposes' and 'weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict'.[134]

There are also several types of measure that states can implement at the national level to prevent the development, transfer and use of biological weapons and associated risks. These include export and import control measures; legislation, guidelines or standards on biosecurity and biosafety along with penal provisions regarding biological weapons; regulations for the transportation of dangerous goods including biological agents and materials; and mechanisms to monitor relevant technological developments, for example through parliamentary technology assessment mechanisms.[135]

Current coverage of emerging technologies by the governance frameworks

Additive manufacturing

AM is currently discussed in all the multilateral export control regimes, including the Australia Group and the Missile Technology Control Regime (MTCR), either as a possible subject of dedicated control or as part of the review of science and technology

[132] On the distinction between biosafety and biosecurity see Clevestig, P., *Handbook of Applied Biosecurity for Life Science Laboratories* (SIPRI: Stockholm, 2009).

[133] Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, signed 17 June 1925, Geneva, entered into force 8 Feb. 1928, League of Nations, *Treaty Series*, vol. 94 (1929), pp. 65–74.

[134] BTWC (note 3), Article I.

[135] On parliamentary technology assessment see Grunwald, A., Hennen, L. and Sauter, A., 'Parlamentarische Technikfolgenabschätzung in Deutschland und Europa' [Parliamentary technology assessment in Germany and Europe], *Aus Politik und Zeitgeschichte*, vol. 64, nos 6–7 (27 Jan. 2014), pp. 17–24; and European Parliamentary Technology Assessment (EPTA), 'What is technology assessment?', [n.d.].

Table 3.1. The main international and multilateral governance frameworks relevant to the production, trade and use of biological weapons

	Stated scope	No. of participants as of 1 Jan. 2019	Year initiated
Geneva Protocol	The use in war of asphyxiating, poisonous or other gases, and of bacteriological methods of warfare	143	Signed: 1925 In force: 1928
Biological and Toxin Weapons Convention	The development, production and stockpiling of bacteriological (biological) and toxin weapons and on their destruction	183[a]	Signed: 1972 In force: 1975
WHO Laboratory Biosafety Manual	Practical guidance on biosafety techniques for use in laboratories at all levels	..	1st edn: 1983 3rd edn: 2004
Australia Group	The export of materials, technology and software that could contribute to chemical and biological weapon activities	43[b]	1985
Missile Technology Control Regime	The export of unmanned aerial vehicles capable of delivering weapons of mass destruction	35	1987
UN Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons	Authorization to investigate any alleged incident at the request of a UN member state, including dispatch of a fact-finding team to the site	..	1987[c]
UN Security Council Resolution 1540	The involvement of non-state actors in nuclear, biological, chemical and radiological weapons	193[d]	2004
WHO Laboratory Biosecurity Guidance	Detailed guidance on biosecurity in a biological laboratory	..	2006
UN Security Council Resolution 2325	Keeping terrorists and other non-state actors from acquiring weapons of mass destruction	193[d]	2016
Amendment to Article 8 of the Rome Statute of the International Criminal Court	Defining as a war crime the use of weapons which use microbial or other biological agents or toxins	–	2017

UN = United Nations; WHO = World Health Organization.

[a] Five states have signed the BTWC but have yet to fully ratify it. One of these—Tanzania—having approved ratification on 14 Nov. 2018, is expected to deposit its instrument of ratification soon. Ten states have neither signed nor ratified the convention. The figure 183 includes both the People's Republic of China (China) and the Republic of China (Taiwan), which have separately deposited instruments of ratification.

[b] This includes 42 participating states and the European Union. One additional state has unilaterally declared its adherence to the Australia Group guidelines and control lists.

[c] The mechanism has been subsequently updated.

[d] As a resolution adopted under Chapter VII of the UN Charter, this is binding on all 193 member states of the UN.

in their information exchange.[136] No dedicated control or other governance tool specifically addresses the development of, use of or trade in bioprinters or AM equipment for the production of controlled equipment related to biological weapons. Export controls on technology required for the production of controlled goods (e.g. in the form of electronic build files) already apply, as do catch-all controls triggered by biological weapon end-uses. The precise legal wording and practice for list-based controls and catch-all controls differ from country to country, which may have an impact on their specific applicability to AM and bioprinting.[137]

[136] See e.g. MTCR, 'Public statement from the plenary meeting of the Missile Technology Control Regime (MTCR), Busan, 21st October 2016', 21 Oct. 2016.

[137] Brockmann and Kelley (note 23), p. 32.

Box 3.1. Governance of artificial intelligence

The conversation on the risks associated with civilian applications of artificial intelligence (AI) seems to be mainly driven by the private sector.

The largest industrial actors—including Google, Facebook, Amazon and Microsoft—joined forces in September 2016 to create the Partnership on AI, which aims to investigate societal challenges posed by AI and propose relevant principles and best practices for the design and use of AI systems.[a] The Partnership on AI now includes the participation of more than 80 companies and non-profit organizations in 13 countries. The creation of the Partnership on AI was allegedly at least in part motivated by the fear that, if companies did not take proactive steps to reduce the societal risk posed by the systems they design, then national, regional or international regulatory bodies would introduce measures that could limit the companies' ability to innovate or force them to change their product lines.[b]

In April 2016 the Institute of Electrical and Electronics Engineers (IEEE), the world's largest association of engineers, launched its Global Initiative on Ethics of Autonomous and Intelligent Systems.[c] The purpose of the initiative is to come up with recommendations for possible ethical standards for the design, use and control of AI systems, from self-driving cars to autonomous weapons. It has involved more than 850 professionals with mixed regional and disciplinary backgrounds (including computer science, electronic and mechanical engineering, and the social sciences). It has published and updated a report on feedback from a public request for information.[d]

[a] Partnership on AI, 'About us', [n.d.].
[b] Vogt, H., 'Artificial intelligence rules more of your life. Who rules AI?', *Wall Street Journal*, 13 Mar. 2018.
[c] IEEE Standards Association, 'The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems', [n.d.].
[d] IEEE Global Initiative, *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems*, version 2 (IEEE: New York, Dec. 2017).

In the BTWC framework, while no state party or observer has submitted a dedicated working paper on AM to the regular meetings of experts, the issue has been raised in side events organized by a variety of organizations. The Spiez Convergence conferences—informal review meetings of technical, academic and policy experts that have taken place biennially since 2014—have repeatedly discussed the topic and have subsequently briefed, among others, the Australia Group on AM and bioprinting, alongside other convergence topics.[138]

Codes of conduct drafted by the DIY AM community have invoked broader ethical standards, with discussion of concerns related to biological weapons being at best peripheral. This reflects the limited maturity of applications of AM that potentially pose such risks.

Artificial intelligence

The conversation on how risks posed by AI should be dealt with is still very young.[139] It is also fragmented in multiple ways.

In some areas of application (e.g. self-driving cars), the policy discussion is primarily taking place at the national level or, in the case of the EU, the regional level, while in others (e.g. autonomous weapon systems) it is coordinated by the UN directly.

The policy options that are discussed differ depending on who is leading the conversation. In areas where the conversation is led by the private sector—which is generally the case for civilian applications of AI—the focus tends to be on self-governance via the definition of shared principles and norms (see box 3.1). In areas where the discussions are driven by civil society organizations and lawmakers—which is the case for security or military applications such as autonomous weapon systems—the focus is generally on the adoption of new regulations.[140] These can be 'hard'—legally binding, top-down regulations (i.e. international treaties or government-imposed regulation)—or 'soft'—non-binding, informal, often bottom-up measures (i.e. codes

[138] Spiez Laboratory (note 21).
[139] Cath, C. et al., 'Governing artificial intelligence: ethical, legal and technical opportunities and challenges', *Philosophical Transactions of the Royal Society A*, vol. 376, no. 2133 (Nov. 2018).
[140] Boulanin, V., 'Mapping the debate on LAWS at the CCW: taking stock and moving forward', EU Non-proliferation Paper no. 49, EU Non-proliferation Consortium, Mar. 2016.

of conduct or best practices documents)—depending on the issue and national or historical regulatory preferences.

In the area where AI and biotechnology converge, the discussion on risk governance is still in its early days. Companies at the cutting edge of genomics and AI research have acknowledged that there are a number of ethical and regulatory issues that will require governance to be developed in the near future, so they have taken small steps towards the development of common principles. Questions of data privacy and data security seem to be the primary concern. Among the issues discussed by these companies are possible standards for encryption for activities related to genome sequencing and storage.[141]

The community of experts that follow issues related to biological weapons for the BTWC and the Australia Group seems increasingly aware that the convergence of AI and biotechnology will pose new risks with regard to the development and control of such weapons. At the same time, these experts also see new opportunities for increasing biosecurity and biodefence.[142]

Robotics

The discussion on the governance of risks posed by robotics resembles that for AI, mainly because AI and robotics are intertwined technologies. Both discussions are divided along several lines. Drones, autonomous weapons and care robots, for instance, each prompt their own set of concerns and discussions about regulatory requirements at the national, regional and international levels.

For the community of experts that follows issues related to biological weapons, one of the major challenges created by the convergence of robotics and biotechnology is that the traditional tools and approaches developed over many decades to prevent the design and use of biological weapons are ill-equipped to control the use of robotics for biological weapon-related purposes. For example, while the BTWC science and technology review mechanism has considered the implication of cloud laboratories and drones for the development and use of biological weapons, it has so far failed to produce concrete new guidance for the states parties.[143]

It would be difficult to limit malicious actors' access to robotic technologies using current export control mechanisms given that widely available commercial products with legitimate applications can be so easily repurposed for military or terrorist purposes. Among the export control regimes, only the MTCR currently restricts large UAV platforms, while smaller commercial off-the-shelf drones are not subject to regulation.[144] However, the problem of smaller drones with capabilities to serve as delivery systems for biological weapons has been discussed within the MTCR. In accordance with the MTCR Guidelines, there is a 'strong presumption to deny such transfers' if there is persuasive information that such drones are intended for the delivery of weapons of mass destruction, even if they are not explicitly listed on the MTCR's control list.[145] These smaller drones are thus subject to catch-all controls if they may be intended for use in connection with biological weapons.

One method to limit the misuse of commercial drones by terrorists that is currently being explored by industry is to embed specific no-fly-zones into drones at the programming phase. DJI, the Chinese company that produces the most popular

[141] Pauwels and Vidyarthi (note 93).

[142] Pauwels, E., 'The promises and perils of "bio-intelligence": rethinking the governance of emerging and converging technologies that revolutionize the engineering of life', Unpublished briefing paper, SIPRI, Nov. 2018.

[143] Pauwels (note 142).

[144] Horowitz, M. C. and Mathewson, A., 'A way to rein in drone proliferation', *Bulletin of the Atomic Scientists*, 30 Nov. 2018.

[145] Missile Technology Control Regime, 'Guidelines for sensitive missile-relevant transfers', [n.d.].

hobbyist drone on the market, the DJI Phantom, has done this to limit the use of its drones in Syria and Ukraine.[146]

Adequately equipping the governance frameworks to deal with the risk of biological weapon proliferation or use

The extent to which the existing governance frameworks can, and do, address the challenges of emerging technologies in relation to biotechnology varies. In some cases there are specific shortcomings in the arms control, export control and self-governance activities to address emerging technologies and convergence. In other cases these activities overlap. Some of the frameworks require a major rethinking of their governance structure.

Limitations of the international treaties

A key challenge for effective biological arms control is the fact that treaty structures and the institutional arrangements in ministries and government agencies do not correspond to technological realities, which are far more complex and fluid and which interact more freely with each other. This has resulted in the absence of discussions on convergence in most forums, largely due to questions of mandate. The initiative to highlight emerging technology through the UN's 2018 disarmament agenda is a step towards recognizing the need for a cross-cutting approach.[147]

The BTWC prohibitions are formulated as a general-purpose criterion in order for the convention to remain relevant despite developments in science and technology. In order to better keep up with scientific and technological developments, the BTWC states parties have been more systematically reviewing developments, starting with the intersessional meetings of 2012–15.[148] Previously, only an ad hoc group had reviewed technological developments in 1992–93, as part of a wider mandate on possible verification measures.[149] The current science and technology review activities involve states parties submitting—if they wish to do so—national working papers, which are discussed during the intersessional meetings of experts and of states parties, as well as during side events at these meetings. The official BTWC meetings allow for presentations or interventions by international organizations or technical experts at the invitation of the chair or as part of the delegation of a state party and generally allow for a joint statement by civil society organizations. However, substantial discussions with all these stakeholders, especially from industry, research and academia, is limited to the side events and poster sessions that take place during the meetings.

The three-person BTWC Implementation Support Unit (ISU) was established in 2007 to undertake certain administrative and support functions mandated by the states parties. The underfunding of the budget dedicated to the ISU and official meetings has affected the effective functioning of the BTWC. In 2018 the significant outstanding payments from states parties resulted in the shortening of the meeting of states parties as part of the intersessional programme and cast further doubts on the sustainable operation of the ISU.[150] There is a risk that discussions about biological

[146] DJI, 'Fly safe geo maps zone'; and Corfield, G., 'Drone maker DJI quietly made large chunks of Iraq and Syria no-fly zones', *The Register*, 26 Apr. 2017.

[147] United Nations (note 1).

[148] Seventh BTWC Review Conference, 'Final Document of the Seventh Review Conference', BWC/CONF.VII/7, 13 Jan. 2012, p. 21.

[149] Hart, J. and Trapp, R., 'Science, technology, and the Biological Weapons Convention', *Arms Control Today*, vol. 42, no. 8 (Oct. 2012).

[150] United Nations Secretariat, 'Status of contributions of BWC, CCW, CCM, OTW as at 30 September 2018', 30 Sep. 2018; and Meeting of BTWC States Parties, 'Biological Weapons Convention: letter from the Chairman', 8 Nov.

terrorism, biosafety and biosecurity could move from the BTWC to other forums, due to a lack of meeting time or the absence of an adequate science and technology review mechanism. The diffusion of debates and fracturing of centralization around the BTWC as the main governance framework is further demonstrated by the stark disparity between the ISU's resources and its range of tasks.[151] Moreover, the ISU's current tasks do not include specific responsibilities in the science and technology review process.[152]

While the current science and technology review process has significantly increased the discussions on technological developments under the auspices of the BTWC, it provides for a highly formalized process that suffers from the often short lead times for submissions of working papers or distribution of other information. In addition, only a small, unvarying group of states parties frequently submit working papers and are highly active in the discussions. However, if there was more participation or deeper discussion it is questionable if the time allocated for meetings would be sufficient. This issue would become even more acute if the financial problems that the BTWC currently faces were to persist and result in more shortened meetings in the future. In addition, the fact that the BTWC only prohibits development of biological weapons but is much vaguer with regard to research activities means that it is not well equipped to address the security applications of rapidly developing scientific research.[153]

Unlike the 1993 Chemical Weapons Convention (CWC), the BTWC is not supported by a scientific advisory board.[154] The Scientific Advisory Board (SAB) of the Organisation for the Prohibition of Chemical Weapons (OPCW)—the CWC's implementing body—provides regular reports on relevant developments in science and technology and gives further advice on request.[155] In addition, it prepares a larger report for the quinquennial CWC Review Conferences. The SAB is composed of 25 experts who serve in their personal capacities and it can also establish temporary working groups to bring in broader expertise. A number of experts have argued for a dedicated forum in support of the BTWC to assess treaty implications of scientific advances and a more systematic and regular review of science and technology.[156] Recent discussions under the framework of the BTWC have signalled general support among the states parties for enhancements to science and technology review processes, but a failure to agree on the practicalities continues to hamper the effectiveness of addressing scientific and technological developments.[157]

The challenges to the BTWC control framework are therefore the lack of focus, so far, on technological convergence; the lack of funding; the lack of mechanisms for monitoring science and technology; and geopolitical tensions.

Limitations of the multilateral and national export control measures

All of the main challenges in the general field of export controls are also of specific relevance in the biological field: adapting to new technologies, including their

2018.

[151] Koblentz, G. D. and Lentzos, F., 'It's time to modernize the bioweapons convention', *Bulletin of the Atomic Scientists*, 4 Nov. 2016.

[152] UN Office at Geneva, 'Role of the Implementation Support Unit', [n.d.].

[153] Koblentz and Lentzos (note 151).

[154] Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (Chemical Weapons Convention, CWC), opened for signature 13 Jan. 1993, entered into force 29 Apr. 1997.

[155] Organisation for the Prohibition of Chemical Weapons, 'Scientific Advisory Board: keeping pace with scientific and technological change', [n.d.].

[156] Koblentz and Lentzos (note 151); and Revill, J., 'Could gene editing tools such as CRISPR be used as a biological weapon?', The Conversation, 31 Aug. 2017.

[157] Revill (note 156).

cross-cutting nature; handling of intangible transfers of technology; making all stakeholders aware of controls; and limiting the negative side-effects of controls.[158]

By definition, export controls are constantly seeking to catch up with or anticipate technological developments. This was the reason behind the creation of catch-all or end-use-based controls. Moreover, the dominant cross-regime theme in recent years has been adjusting to technological developments, including the opportunities and vulnerabilities of digitization.[159] The challenge relates not only to the types of item to be made subject to control, but also to the types of transaction or means of transferring technology. It also relates to the types of actor that need to be the target of awareness-raising, preventive engagement and, potentially, control. In the biological field, these include academics and the DIY community among others.

Despite the cross-cutting and interlinked nature of technology, having joint discussions on the—clearly overlapping—control lists in the export control regimes has met resistance, primarily due to the regimes' different memberships. However, the regimes have recently explored practical and pragmatic cooperation through informal initiatives.[160]

The increase in intangible transfers of technology, including in the biological field, creates specific challenges to the enforceability of controls and a need to adjust the current prevention and enforcement toolbox.[161] This relates not only to the electronic transfer of biotechnology (e.g. digitized biological information sent to cloud laboratories, which in turn conduct experiments), but also the transfer of potentially sensitive knowledge through lectures and publications by academics, science education, scientific exchanges in all forms (e.g. research visits or collaborative projects) and development assistance in science.

Moreover, the diffusion of manufacturing centres and their (intended) closeness to end-users is expected to lead to a shift from moving materials, equipment and technologies to moving data (e.g. specifications of desired properties of products) and manufacturing tools to be at or near the site of intended use. If this development towards the fourth industrial revolution materializes, as many believe, today's export control model may require a significant transformation.[162]

A tension between security-driven controls and health has been added to the existing tension between such controls and the freedom of trade. On the one hand, export controls may delay the delivery of diagnostic equipment during health crises unless specific emergency procedures are in place. On the other hand, the regular transfer of diagnostic and reference samples between countries, regions and continents is both an element of routine global health protection activity and fundamental in scientific exchanges. In turn, these transfers contribute to safeguarding both human and animal health, but they simultaneously pose biosecurity and biosafety risks.[163] With the growing interest in global health activities in many countries, these aspects will not diminish.

Reaching out to all relevant types of stakeholder to create awareness of security risks and control requirements continues to be difficult for the governments of many, if not all, countries seeking to engage in such efforts, regardless of their size.

[158] On these general challenges see e.g. Bauer, S. et al., 'The export control regimes', *SIPRI Yearbook 2018* (note 10).

[159] Bromley et al. (note 10).

[160] Cándano, D., 'Export controls and emerging threats: a view from the Nuclear Suppliers Group', Intervention at the Export Control Forum 2018, Brussels, 13 Dec. 2018, 00:26:00–00:35:30.

[161] Bromley, M. and Maletta, G., *The Challenge of Software and Technology Transfers to Non-proliferation Efforts: Implementing and Complying with Export Controls* (SIPRI: Stockholm, Apr. 2018); Brockmann and Kelley (note 23); and Stewart (note 19), p. 34.

[162] Bromley and Maletta (note 161).

[163] SIPRI and Ecorys, *Data and Information Collection for EU Dual-Use Export Control Policy Review*, Final Report (European Commission: Brussels, 6 Nov. 2015).

While most key stakeholders in the nuclear, conventional arms, missile or even chemical fields are in the private sector, in the biological field many are also based in academia, research institutions and the health sector. This complexity and diversity of stakeholders is further reinforced through technological developments in different areas that enhance or change biological risks. The biotechnology service industries may present an additional layer of complexity as the steady decline in costs for basic and advanced biotechnological services provides both the private and public sectors with the attractive alternative of outsourcing expensive and time-consuming work.

Identifying these stakeholders and engaging with them in a tailored and targeted manner poses the practical challenge of keeping up with a moving target and requires that government agencies and licensing authorities have substantial resources and specific knowledge of a range of sectors. This difficulty is reinforced by the lack of dedicated industry and scientific associations for the emerging and converging technologies.

Alongside the tensions between export controls on the one hand and trade and health on the other, there is a tension between security interests and the freedom of science. The experience of academic scientists when publishing their work illustrates how application of export controls can vary from country to country and case to case. In a 2012 case involving research on the transmissibility of highly pathogenic avian influenza A (A/H5N1) in mammals, the Dutch licensing authority applied export control to a scientific paper deemed to be carrying sensitive information. The academic who was required to apply for an export licence unsuccessfully challenged the application of export control in court (although he did eventually apply for and obtain a licence).[164] It seems that this court case is so far unique in Europe and probably also globally. The work of US scientists who conducted similar research in parallel was also published, without the intervention of the US licensing authority but following involvement of the US National Science Advisory Board for Biosecurity (NSABB). The different approach of the US authorities may have been due to differences between the research approaches of the two teams and the substance of the publications, and not just differences in control approaches between the Netherlands and the USA.[165] Concerns may therefore not only relate to the publication of the information as such, but to the biosafety and biosecurity measures taken during the experiments. In 2013 two researchers decided to withhold some methodology information required to permit others to reproduce their research on botulinum toxins until effective treatments have been developed.[166]

The Australia Group control list states that 'Controls on "technology" do not apply to information "in the public domain" or to "basic scientific research" or the minimum necessary information for patent application', where basic scientific research is defined as 'Experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective'.[167] The EU Dual-use

[164] Clevestig, P. and Hart, J., 'Oversight of dual-purpose research in the life sciences', *SIPRI Yearbook 2013: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2013), pp. 384–88; Herfst, S. et al., 'Airborne transmission of influenza A/H5N1 virus between ferrets', *Science*, vol. 336, no. 6088 (22 June 2012), pp. 1534–41; Russell, C. A. et al., 'The potential for respiratory droplet-transmissible A/H5N1 influenza virus to evolve in a mammalian host', *Science*, vol. 336, no. 6088 (22 June 2012), pp. 1541–47; and Enserink, M., 'Dutch appeals court dodges decision on hotly debated H5N1 papers', *Science*, 16 July 2015.

[165] Imai, M. et al., 'Experimental adaptation of an influenza H5 HA confers respiratory droplet transmission to a reassortant H5 HA/H1N1 virus in ferrets', *Nature*, vol. 486 (21 June 2012), pp. 420–28. See also SIPRI and Ecorys (note 163), p. 38.

[166] Barash, J. R. and Arnon, S. S., 'A novel strain of *Clostridium botulinum* that produces Type B and Type H botulinum toxins', *Journal of Infectious Diseases*, vol. 209, no. 2 (15 Jan. 2014), pp. 183–91; and Clevestig, P. and Hart, J., 'Oversight of dual-purpose research in the life sciences', *SIPRI Yearbook 2014: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2014), pp. 414–16.

[167] Australia Group (note 44).

Regulation uses identical language.[168] In practice, the line between basic and applied research has proven difficult to draw, and this has highlighted the tension between the freedom of academia and security considerations.[169] Concerns about the impact on academic freedom relate not only to the need to publish in the academic world, but also to the ambition inherent in academia to be the first to publish a new methodology or approach.

Limitations of the self-governance frameworks

Industry self-governance. Self-governance in the biotechnology industry has increased significantly in recent years. A notable example is the screening procedures against potential misuse implemented by the International Gene Synthesis Consortium (IGSC). The IGSC was established in 2009 and currently comprises seven partners that are responsible for approximately 80 per cent of international commercial gene synthesis.[170] The companies involved in these screening measures rely on the 'know your customer' principle and a documentation system that permits questionable cases to be examined individually to confirm end-use.[171] However, such screening tools are expensive and thus less easily available to smaller companies. Moreover, increasingly complex global supply chains make it difficult to identify the ultimate end-user and to connect related orders.

In the gene-synthesis industry, the self-regulatory screening standards could be globalized beyond the IGSC.[172] Spreading such approaches to a wider field of biotechnology companies that provide goods, technology or services of potential biosecurity concern could reduce risks associated with the biotechnology industry without significantly expanding top-down regulatory measures, such as export controls. Developing standards for genomic data privacy at the international level could enable a more level playing field for companies and more ethical conduct. At the same time, they could also moderate possible future risks that could result from the exploitation of genomic data sets using machine learning and AI.

Codes of conduct and ethics training. Efforts to develop and promulgate norms of responsible conduct take different, often overlapping, forms and have different names: codes of ethics, codes of conduct, codes of practice and so on. They can govern a wide range of issues, such as responsible science, vigilance against misuse, ethics, privacy and sometimes specifically technology transfers or biological weapons. They provide an essential tool in the governance of science and technology motivated by security concerns because the scientists conducting the research, or considering doing so, are best placed to understand the implications of their work and, potentially, to impose limits.[173]

The many codes of conduct, in particular in academic institutions, have been discussed and promoted systematically as part of international and national arms control efforts (e.g. as a key agenda item of the BTWC) since at least 2005. However, outreach to and engagement with academia on security risks either do not receive enough attention and resources from governments or are still works in progress that

[168] Council Regulation (EC) no. 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, *Official Journal of the European Union*, L 134, 29 May 2009, 'General technology note'.

[169] Bauer, S. and Bromley, M., 'Dual-use export control policy review: balancing security, trade and academic freedom in a changing world', EU Non-proliferation Paper no. 48, EU Non-proliferation Consortium, Mar. 2016.

[170] Marris, C., Jefferson, C. and Lentzos, F., 'Negotiating the dynamics of uncomfortable knowledge: the case of dual use and synthetic biology', *Biosocieties*, vol. 9, no. 4 (Nov. 2014), pp. 393–420.

[171] Bauer, S. et al., *Challenges and Good Practices in the Implementation of the EU's Arms and Dual-use Export Controls: A Cross-Sector Analysis* (SIPRI: Stockholm, July 2017), pp. 22–23.

[172] International Gene Synthesis Consortium, 'About IGSC', [n.d.]; and Bauer et al. (note 171), pp. 22–23.

[173] Bohm and Lentzos (note 82).

require further improvements, in particular in finding the appropriate way to engage effectively. These efforts need to build on existing codes of conduct for research ethics, biosafety measures and so on in order to take advantage of the existing sense of ownership and to speak a language that is already understood. Indeed, the likelihood of standards and codes being effective is considerably higher if they are developed by or in conjunction with the scientific community through a continuous process of review and exchange that is able to respond to rapid scientific developments and public opinion.[174]

There currently seem to be few, if any, obligatory university courses on research ethics, biosafety and biosecurity, or international law and regulations, whether driven by university initiatives or governments. However, in order for the culture to change, awareness and acceptance of the responsibilities of scientists regarding biosecurity risks—especially in cutting-edge research at the intersection of different technologies—need to be simultaneously embraced by creative hubs, the DIY community, university institutes and company R&D programmes. Voluntary courses about responsible science that specifically consider potential misuse of biotechnology are offered by a number of institutions (e.g. Karolinska Institutet, Stockholm).[175]

The DIY community. As developments in biotechnology have lowered barriers to access, the role of the DIY community has increased. Contrary to the often-propagated image of DIY biology as an ungoverned space populated by flippant biohackers and amateurs experimenting without restraint, the DIY community has developed a range of community standards and codes of ethics. It thus actively engages with concerns over biosafety and possible misuse of biotechnology.[176] For example, in 2011 several congresses were organized in Europe and North America that brought together individuals from the community and delegates from established DIY community regional groups to collaboratively develop and ultimately agree on codes of ethics for their community.[177] One expert who was involved in convening these congresses claims that 'when it comes to thinking proactively about the safety issues thrown up by biotechnology, the global DIY-biology community is arguably ahead of the scientific establishment'.[178]

The DIY community codes include commitments to use biotechnology only for peaceful purposes. However, compliance- and norm-building effects depend on this principle being operationalized, which requires a sufficient understanding of possible security implications, beyond the more well-known safety aspects. Moreover, these communities and their codes have not paid as much attention to monitoring, forecasting and appropriately addressing relevant technological changes and their risk implications.

Conditionality for research funding and publication standards. As part of the modalities for obtaining a grant or publishing new research, momentum has grown for the introduction of specified standards that reflect concerns about the dual-use nature of some research. This reflects the increasing importance of knowledge transfer in synthetic biology. If, for example, sufficient detail is provided in a scientific article, this could help someone with malicious intentions to reconstruct an extinct pathogen,

[174] Gutmann, A. and Moreno, J. D., 'Keep CRISPR safe: regulating a genetic revolution', *Foreign Affairs*, May/June 2018.

[175] Human Brain Project, 'Research, ethics & societal impact', [n.d.]. For a list of BTWC-related e-learning courses see UN Office at Geneva, 'Resource repository', [n.d.].

[176] Skerrett, P., 'Is do-it-yourself CRISPR as scary as it sounds', STAT, 14 Mar. 2016.

[177] DIYbio, 'Codes', [n.d.]; and Kuiken, T., 'Learn from DIY biologists', *Nature*, vol. 531, no. 7593 (Mar. 2016), pp. 167–68.

[178] Kuiken (note 177), p. 167.

modify an existing pathogen to make it more lethal or transmissible, or create a dangerous new pathogen.

In February 2003 the Journal Editors and Authors Group, comprising 31 scientists and editors of leading journals, published a Statement on the Consideration of Biodefence and Biosecurity.[179] This was sparked by increased appreciation of the risks posed by terrorist attacks involving biological weapons after the 11 September 2001 attacks on the USA and the lethal incident that followed soon after involving letters sent to US media and politicians containing *Bacillus anthracis* (anthrax) spores.[180] The statement addressed the possibility that new information published in research journals might unintentionally assist malicious actors. Today, most reputable journals have some form of advisory or review board that can be called on in cases where a publication prompts potential biosecurity concerns.

In 2005 a number of British funders of life sciences research—the Wellcome Trust, the Medical Research Council (MRC) and the Biotechnology and Biological Sciences Research Council (BBSRC)—made changes to their funding application forms to take into account concerns about dual-use research. They jointly developed guidance for applicants, reviewers and funding committees and modified organizational guidelines for research.[181] Conditionality for research funding has also, more recently, been developed for specific areas within the life sciences that have been associated with new risks. One such area is gene drives, which speed up the propagation of a particular gene or group of genes through a population. In December 2017 the Wellcome Trust, along with other funders such as the Bill & Melinda Gates Foundation and the Institut Pasteur, developed the Guiding Principles for Sponsors and Supporters of Gene Drive Research.[182]

In 2014 the EU included an ethics self-assessment in the application procedure of its new Horizon 2020 funding programme. Applicants are required to declare if their research involves dual-use goods or transfers of technology that require an export authorization and to provide explanations of how they will ensure compliance with export controls and international law and avoid negative outcomes, such as misuse.[183]

Such efforts could be both more broad and systematic to cover more funding schemes in more countries, and more focused on areas of research that have not previously been a focus of attention but which carry the greatest risks.[184] While recent developments have enhanced awareness of potential misuse of scientific research, much remains to be done to introduce relevant questions into the research cycle at the point of funding and of publication globally and to strengthen other entry points, such as the teaching and doctoral supervision stages. There remains an inherent tension between the freedom of academia and security concerns, as well

[179] Atlas, R. et al., 'Statement on the consideration of biodefence and biosecurity', *Nature*, vol. 421, no. 6925 (20 Feb. 2003), p. 771.

[180] On the anthrax incident see e.g. Koblentz, G. D., *Living Weapons: Biological Warfare and International Security* (Cornell University Press: Ithaca, NY, 2009), pp. 205–12; and Zanders, J. P., Hart, J. and Kuhlau, F., 'Chemical and biological weapon developments and arms control', *SIPRI Yearbook 2002: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 2002), pp. 665–708, pp. 696–703.

[181] Biotechnology and Biological Sciences Research Council (BBSRC), Medical Research Council (MRC) and Wellcome Trust, 'BBSRC, MRC and Wellcome Trust position statement on dual use research of concern and research misuse', July 2005; Lentzos, F., 'Genetic engineering and biological risks: policy formation and regulatory response', eds R. Brownsword, E. Scotford and K. Yeung, *The Oxford Handbook of the Law and Regulation of Technology* (Oxford University Press: Oxford, 2017), pp. 1118–42; and Emerson, C. et al., 'Principles for gene drive research', *Science*, vol. 358, no. 6367 (1 Dec. 2017), pp. 1135–36.

[182] Emerson et al. (note 181); and Bohm and Lentzos (note 82).

[183] European Commission, Directorate-General for Research and Innovation, 'Horizon 2020 programme: guidance—how to complete your ethics self-assessment', version 6.0, 23 July 2018.

[184] European Commission, 'Explanatory note on the control of "export" for "dual-use items", including technology transfers, under Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items', [n.d.].

as a knowledge gap as to what could be misused. One of the questions that requires resolving relates to the common exemption of fundamental or basic research from trade control requirements, since the line between basic and applied research is not clearly defined in regulations or not sufficiently explained in accompanying guidance notes.[185]

The adequacy of the response mechanisms and implications for them

New technologies can both reinforce traditional biological risks (e.g. a disease being spread, no matter if created through synthetic biology or existing viruses) and create new risks. This includes the specific risk of agroterrorism, where an intentional incident could seriously undermine food security and health for a country or region and may even have global implications.[186] The reinforcement of traditional risks means that broader biosafety and biosecurity awareness and disease surveillance and response mechanisms are still equally, if not more, applicable. New risks require dedicated oversight and control mechanisms (e.g. for cloud laboratories).

The impact and management of a natural disease is similar to that of a non-natural disease to the extent that in both cases the public, animal or plant health systems are affected. The linkages between biosafety, disease surveillance and the global health infrastructure that are relevant to traditional biological risks remain relevant for new or reinforced risks. Natural disease outbreaks and outbreaks due to intentional release of a naturally occurring pathogen are similar in management (but probably not in impact if the release is large or in many places simultaneously). However, management of engineered pathogens can be quite different, for example if a normally foodborne disease is delivered as an aerosol.

There is a difference between the responses to natural, accidental and deliberate biological incidents. In the case of a natural disease, treatment takes place and the further spread is monitored through epidemiology and limited through research and countermeasure development (i.e. vaccines, which may be produced more rapidly due to advances in science and technology). In the case of an accidental or deliberate spread of disease caused by a safety or security failure, an additional investigation would aim to determine the origin or seek to attribute responsibility and learn to plan for any future occurrence of such an incident. However, detection of an engineered biological weapon may be delayed, making effective response more difficult. An investigation into the use of a biological weapon (e.g. using the UN Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons) would also seek to attribute blame and recommend possible prosecution or, in case of successful attribution to a state sponsor, a UN Security Council resolution with or without sanctions. Such an attribution may also be made easier through advances in microbial forensics.[187]

Several efforts are currently under way to try to strengthen the assistance and response mechanism provided for by Article VII of the BTWC. For example, a project sponsored by Canada and hosted by the ISU intends to develop an

[185] Fraunhofer-Gesellschaft and Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO, Dutch Organisation for Applied Scientific Research), 'From a practical view: the proposed Dual-use Regulation and export control challenges for research and academia', 18 Dec. 2017.

[186] Zavriev, S. K., 'Biosecurity and bioterrorism risks: agriculture and food safety—implications of technological advances', Unpublished briefing paper, Nov. 2018. See also Monke, J., *Agroterrorism: Threats and Preparedness*, Congressional Research Service (CRS) Report for Congress RL32521 (US Congress, CRS: Washington, DC: 12 Mar. 2007).

[187] National Research Council, *Science Needs for Microbial Forensics: Initial International Research Priorities* (National Academies Press: Washington, DC, 2014).

International Bio-emergency Management Plan for Deliberate Events.[188] There are further efforts to strengthen the UN Secretary-General's investigation mechanism through the expansion of the roster of experts and the network of laboratories that can be called on for impartial investigations of biological weapon use.[189]

[188] Santori, V., BTWC Implementation Support Unit, 'Strengthening global mechanisms for responding to deliberate use of disease', Presentation at the 2nd OIE Global Conference on Biological Threat Reduction, Ottawa, 31 Oct.–2 Nov. 2017.

[189] United Nations (note 86).

4. Conclusions and recommendations

This report explores the security concerns associated with the convergence of biotechnology with new developments in three emerging technologies: additive manufacturing, artificial intelligence and robotics. It also analyses the extent to which concerns arising from new technological developments can be dealt with through existing governance mechanism and identifies the limitations that persist.

The main conclusion is that, while new developments in these three emerging technologies could have an enabling effect in different steps of the development, production and use of biological weapons, the existing governance frameworks are ill-equipped to comprehensively address the resulting risks. This chapter summarizes the other key findings and presents a series of recommendations for policymakers at various levels.

Key findings

The enabling effect on the development, production and use of biological weapons

Advances in AM, AI and robotics raise a common set of issues as far as the development, production and use of biological weapons are concerned.

First, they could facilitate, each in their own way, the development or production of biological weapons and their delivery systems by enabling the automation of developmental or production steps that previously required manual manipulation or analysis by a human. AM could make the production of drone components for the delivery of biological weapon more accessible. AI could be used to find new ways to optimize the transmissibility or virulence of a biological agent. Robots in laboratories reduce the need for trained laboratory staff, while permitting major productivity gain in the design–build–test cycle of biological agents.

Second, these technologies could provide new possibilities for biological weapon use, for example through highly targeted delivery. AI could enable the design of a pathogen that would affect only specific individuals of groups of people, while nanorobots could enable the delivery of biological agents to specific cells in the human body. Meanwhile, AM could make the production of advanced delivery mechanisms available to an increasing number of actors—including terrorist organizations.

Third, these technologies increase the exposure of digitized biological data and operating parameters to cyberattacks. The data that these systems generate or rely on could be stolen, misused or manipulated, including for activities that could facilitate the development, production or delivery of biological weapons or cause critical malfunctions in related equipment.

Fourth, none of these technologies is easy to control, notably because their development is mainly driven by the civilian and private sectors and is therefore less susceptible to governmental steering and control than previous relevant technological developments. This issue is further complicated by the ease of transferring digital and digitally enabled technologies. For example, traditional export and customs controls may no longer pose sufficient barriers and adequate investigative and compliance audit measures are rare.

Fortunately, there are a number of reasons not to exaggerate the risk. The impact of these technologies on the engineering of biological weapons and their delivery systems is nuanced. The operations that can be simplified or enhanced by automation account for only a subset of the development and production processes. The expertise required to exploit these technologies for the purpose of developing and producing biological

weapons remains significant and continues to pose a barrier to most actors. With regard to the delivery of biological weapons, most of the applications of AI and nanorobotics remain experimental or hardly feasible for non-state actors. Developing genetically targeted weapons with the help of AI or developing nanorobots for biological weapon delivery would require substantial resources (i.e. data, know-how, infrastructure and time) that most non-state actors would not be able or willing to mobilize given that there are much simpler and cheaper means to target specific individuals or groups. In the case of drones, while the use of small hobby drones has already become common in asymmetric warfare, developing, stabilizing and formulating a biological agent for delivery by drone remains challenging.

It is also important to consider that, alongside the risks, these technologies provide new opportunities to prevent the development and use of biological weapons and to manage biological incidents and disease outbreaks. For example, the data-processing capabilities of AI could help national and international authorities in charge of preventing and managing biological incidents—be they intentional or naturally occurring—to gain better situational awareness and increase their ability to make informed decisions in critical situations. A number of new robotic applications, such as LOCs, could speed up the detection of biological incidents by enabling point-of-care medical diagnostics, while AM may offer increased adaptability and enhance logistics by enabling on-the-spot manufacturing in disaster or crisis response situations.

The shortcomings of existing governance frameworks

Existing governance frameworks exhibit a number of shortcomings that make them ill-equipped to comprehensively and effectively review and address the risks posed by the convergence of innovation in biotechnology and other areas of science and technology.

First, the frameworks either have not used, or cannot fully use, their potential to explore connections between biotechnology and other emerging technologies. Several governance frameworks capture, or are designed to capture, developments in science and technology, in particular the BTWC and the Australia Group. However, their mandates, political differences, working practices and levels of stakeholder engagement can affect their ability to review and ensure adequate coverage of relevant technologies. They might not be able to tackle risks deriving from the interaction with other technologies of the technology that they are meant to address. In the realm of export control, for instance, components or certain applications may be covered incidentally due to other proliferation risks (e.g. lasers used in AM machines may be subject to controls based on potential uses in conventional weapons), but their coverage in control lists may not be sufficiently informed by risks related to biological weapons or delivery systems, resulting in the possibility of inadvertent gaps in control.

Second, treaty regimes and other governance instruments typically interact with each other much less than the respective technologies that they cover. An overarching question when viewing governance in the field of biosecurity through the lens of technological development and convergence is therefore how to better connect the relevant governance mechanisms—including the BTWC, the CWC, the export control regimes and the UN investigation mechanism—where discussions on this are ongoing at different levels of intensity.

Third, governance institutions and frameworks, including the states involved in their discussions and decision-making processes, also struggle to develop a sufficient understanding of a technology, the associated risks and its potential impact on the activities, transfers or behaviour that they govern. It is therefore a significant challenge to allocate appropriate resources, leverage institutional linkages, develop novel

instruments within existing structures or identify the need for, let alone establish, entirely new governance mechanisms.

Fourth, many emerging technologies with various degrees of convergence with biotechnology that pose potential biological weapon proliferation risks are not developed through dedicated state-controlled programmes, but instead in a competitive commercial environment. It is therefore indispensable to not only maintain and strengthen norms in research and state contexts, but to broaden and build more inclusive approaches. Norm-building in the private sector and in less formalized contexts, such as the DIY community, forms a major component of such efforts.

While dealing with developments in science and technology is far from a new issue, measures to address their impact must keep up with the dynamics of these developments. Thus, improvements to governance instruments need to address the structural factors and new characteristics of new technologies that have a possibly significant impact through convergence with biotechnology. To address these limitations, the above analysis shows that efforts to improve the capability of existing governance frameworks to address technological change will require serious rethinking and have to be supported by a range of complementary measures, in particular such soft measures as codes of conduct, education and outreach. These efforts, in particular those that are bottom-up and involve the next generation of scientists and engineers, need to transcend any artificial divisions that the traditional scientific communities still impose on those working in these fields. It is thus a positive sign that multidisciplinary and transdisciplinary initiatives involving biotechnology experts are on the rise.

Recommendations

There are a number of options that could be explored to deal with these governance issues. The following recommendations propose both (*a*) ways to strengthen and amend existing governance instruments to address the identified intersection and convergence of biology with emerging technologies, and (*b*) entirely new policy options and instruments. These are addressed at national governments, regional organizations and international institutions, academia, the private sector and the DIY community.

Recommendations for national governments at the national level

1. Systematically monitor and assess developments in science and technology. For example, a national 'Biology Plus X' working group could be created composed of representatives with a relevant portfolio from the ministries of foreign affairs, economy, health, science and education (depending on national divisions of competences) and export licensing and enforcement authorities. This would strengthen their linkages and enable a continuous exchange and coordination of national monitoring, awareness-raising and governance measures. Such working groups could break down the operational barriers between government agencies and allow for more comprehensive and inclusive discussions of the implications of scientific and technological developments and convergence—and appropriate measures to address them.

2. Map relevant universities, research institutes and companies working in the fields where the convergence of biotechnology and emerging technologies is of particular concern. Such a mapping exercise would enable states to establish a baseline and understanding of the size and characteristics of relevant research efforts

and domestic industries. It would be a first step towards facilitating the effective targeting and tailoring of national outreach, engagement and control efforts (see below).

3. Task parliamentary technology assessment mechanisms with conducting studies on convergence. These studies could address both the connections between technologies and the resulting security implications, including for biological weapons, to provide policymakers with accessible scientific information on the risk landscape at the national level.

4. Increase resources for and improve approaches to outreach and engagement with the diverse field of stakeholders in academia, industry and the DIY community. That could include (*a*) working with biosafety associations to raise awareness about how technological convergence affects biological weapon proliferation and broader biological risk; (*b*) developing information material and training courses about risk-mitigation mechanisms (e.g. export control, cybersecurity and self-regulation); or (*c*) organizing or sponsoring sessions, side events and booths informing about risks, relevant legislation or contact points during related academic, DIY or industrial community events.

5. Increase resources and expertise in export licensing and enforcement authorities for dedicated company audits. These could improve the ability to verify compliance with controls on tangible and intangible technology transfers. Many states still lack the capacities to verify and enforce controls on transfers of technology. Those with more advanced capacities could consider introducing sector-specific audits, for example in the biotechnology sector or for gene synthesis providers in particular.

6. Support scientific research into strengthening the detection, prevention, response and attribution of incidents involving biological weapons or other intentionally modified biological agents. This could involve strengthening efforts to explore and harvest positive implications of developments in science and technology, such as advances in microbial forensics that could enhance the ability to discern and attribute biological incidents.

Recommendations for national governments in multilateral contexts and international institutions

1. Support the creation of a BTWC Scientific Advisory Board. This could draw on the example of the Scientific Advisory Board of the OPCW. The new board would convene experts from a broad range of fields to review on a regular basis advances in science and technology (not only those directly connected to biotechnology). It would assess how these could have an impact on the development and potential use of biological weapons. When appropriate, it could be tasked to suggest policies and practical measures to manage the associated risks and opportunities.

2. Reform elements of the BTWC. This could include developing new working practices in the BTWC that, for instance, would permit some decision-making during intersessional meetings and would enable different kinds of meeting report where consensus recommendations and proposals are prominently noted, but where those that do not achieve consensus are also clearly stated and acknowledged.[190] It could also involve increased stakeholder involvement in BTWC meetings and consultation with regard to developments in science and technology. It could further explore new mechanisms for building trust and managing perceptions of intent in biodefence. The role of the BTWC in developing guidelines on biological research with high potential for misuse could also be further strengthened.

[190] See e.g. Lentzos, F., 'Biological disarmament and non-proliferation', *SIPRI Yearbook 2019: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, forthcoming 2019).

3. Organize or sponsor events that would raise the issue of convergence and interconnectivity on the agenda of discussions on science and technology in the BTWC forums and the export control regimes. In addition to increasing awareness, these events (conference, workshops, side-events) would aim to strengthen institutional linkages between relevant international governance instruments, for instance by involving national experts. These events could bring in experts from other processes with relevant expertise (e.g. on AI, cybersecurity or robotics).

4. Initiate or support a discussion in relevant international forums on measures that could limit the misuse of commercial biotechnology. This could include discussing cybersecurity standards and customer-screening guidance for companies that provide laboratory services through the cloud.

5. At the EU level, enhance engagement with the biotechnology industry and biosafety associations in the context of dual-use risks. In addition, the requirements for self-assessment, research ethics and codes of conduct in EU funded projects could be further strengthened, including adequate guidance for their implementation. Moreover, the EU should invest in biosafety and biosecurity measures in the EU and globally through its financial instruments.

Recommendations for academic institutions

1. Introduce obligatory courses on research ethics, biosafety, international law and national regulations for all natural science disciplines. This would be driven by university initiatives, not governments, and would apply already at the undergraduate level, in more elaborate form at the master's level and then at an even more advanced level for doctoral students. Governments could support awareness-raising initiatives through funding development of specific courses or modules.

2. Encourage interdisciplinary cooperation on technology assessment, including between the social and natural sciences. Forums and other avenues for such engagement could be created, such as interdisciplinary doctoral seminars or academic workshops or by including courses from other disciplines in curriculums.

3. Further strengthen the collaboration between national academies of sciences, bilaterally, regionally and globally. This collaboration could particularly focus on codes of conduct and facilitate dialogue and the exchange of good practices. They would be well placed to consider the risks arising from the convergence of various technologies and disciplines and design the necessary self-regulatory approaches to address their impact, in particular with regard to emerging technologies such as those discussed in this report.

Recommendations for the private sector

1. Strengthen self-governance and compliance standards. For example, companies that produce commercial drones could develop international industry standards for embedding, and regularly updating, specific no-fly-zones at the programming phase to prevent the misuse of their systems in conflict zones or other sensitive areas. In another example, companies that sell automated laboratory services could create databases of orders that would enable them to develop a list of legitimate and trusted customers. They could also work together to identify cyber- and physical security standards that would limit the risks related to sabotage of robotic laboratories.

Recommendations for the DIY community

1. Organize a dedicated workshop series on biosecurity for community laboratories. This could raise awareness of regulations, biosafety and biosecurity and

of the risks of biological terrorism. It could also strengthen the understanding of how oversight functions in community laboratories can take account of these risks.

2. Strengthen international efforts to foster responsible science and biosecurity awareness. These efforts could include inclusive initiatives and competitions that emphasize responsible science, biosafety and biosecurity, as the International Genetically Engineered Machine (iGEM) competition already does for university students. They could involve schools, universities, amateur scientists, DIY communities and self-declared biohackers. Such initiatives would also support the UN Secretary-General's efforts 'to encourage responsible innovation of science and technology, to ensure its application for peaceful purposes'.[191]

[191] United Nations (note 1), p. 54.

About the authors

Kolja Brockmann (Germany) is a Researcher in SIPRI's Dual-Use and Arms Trade Control Programme. He joined SIPRI as an EU Non-Proliferation and Disarmament Consortium Intern and has been working at SIPRI since 2017. Prior to joining SIPRI, he was an Intern with the German Federal Office for Economic Affairs and Export Control (BAFA) in Frankfurt. He graduated from King's College London with an MA in Non-Proliferation and International Security.

Dr Sibylle Bauer (Germany) is SIPRI's Director of Studies, Armament and Disarmament, and the Chair of the EU Non-Proliferation and Disarmament Consortium. She has a long record of research and publication on armament and export control issues and extensive experience in managing capacity building projects, in particular in the areas of export control and governance of security relevant technology.

Dr Vincent Boulanin (France/Sweden) is a Senior Researcher at SIPRI. He joined SIPRI in 2014, where he works on issues related to the production, use and control of emerging military and security technologies, notably autonomous weapon systems and cyber-security technologies. He received his PhD in Political Science from École des Hautes en Sciences Sociales in Paris in October 2014. His dissertation looked at the diversification of the European arms industry into the security realm. His other research interests include the impact of military and security technologies on the practice of security and military professionals and the social construction of threats and risks.

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE
Signalistgatan 9
SE-169 72 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org

© SIPRI 2019