sipri

# BIOSECURITY RISK ASSESSMENT IN THE LIFE SCIENCES

## Towards a Toolkit for Individual Practitioners

MIRKO HIMMEL

**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.





**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

# BIOSECURITY RISK ASSESSMENT IN THE LIFE SCIENCES

Towards a Toolkit for Individual Practitioners

MIRKO HIMMEL

sipri

STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE

March 2023

# Contents

# Acknowledgements

The author is grateful to participants attending the expert workshop on risk at the intersection of biological science and technological developments held at SIPRI in Janaury 2023 for their feedback on an earlier draft of this paper. The author would also like to graciously acknowledge the editorial work of the SIPRI Editorial Department, particularly the efforts of Dr Linda Nix. The example biosecurity risk assessment in section 4 was based on an unpublished background briefing nanobiotechnology provided by Dr Margaret E. Kosal. Daria Dretvić provided assistance in generating the figures.

This publication was produced by SIPRI with the financial support provided by the UK Foreign, Commonwealth and Development Office.

# Introduction

The prospects of research in biological sciences and emerging technologies for beneficial uses in biomedicine, biotechnology and environmental protection go hand in hand with the risk of unintended consequences of the research and its misuse for malicious purposes. While a number of established, discrete risk management approaches exist, there are significant gaps in managing the specific risk of misuse. For example, biological risk (biorisk) assessment procedures are often implemented in biosafety management routines, but these mechanisms do not necessarily cover biosecurity risks, and those that do tend to focus on biological weapons development. Another gap arises from the fact that while biosecurity governance systems such as treaties, regulations, codes of ethics and funding guidelines cover research in the public sector and academia reasonably well, they do not fully cover the private sector; moreover, compliance and enforcement mechanisms vary from state to state and institution to institution. There is also a knowledge gap: many individual scientists and technicians whose first-hand knowledge of their research is essential for assessing and managing the associated biorisks may lack access to biosecurity-related guidance documents or be unfamiliar with the technical concepts and terminology.

The lack of a universally implemented biorisk management framework is an opportunity for the global scientific community to further foster and support a culture of biosafety and biosecurity and to continue developing the understanding among scientists of the risks associated with their work and how to manage them.[1] This involves finding ways to motivate individual practitioners to proactively take responsibility for managing the biorisks associated with their work. For many practitioners, professional pride in being a responsible scientist and concern for the safety of people, society and the environment, and understanding of and interest in the need to establish and maintain public trust in science—the general public's belief that scientists follow basic ethical principles and the public's high confidence in the accuracy of scientific findings—will be sufficient motivation. But there is also a particular need to close the knowledge gap and equip scientists with the appropriate tools to take responsibility for making their work safer and more secure, including tools that (*a*) enhance awareness about biosecurity risks beyond biological weapons development, and (*b*) facilitate the implementation of a comprehensive biorisk mitigation strategy at the practical level. Ideally such tools would be used universally by individuals in the life sciences or be easily adapted to suit local conditions.

For while responsibility for ethical and legally compliant conduct in the biological sciences lies in the hands of the individual scientist, it cannot be separated from the political and societal context in which the research is performed. The 'Decision Framework' proposed by Jonathan Tucker in 2012 more deeply analyses the roles that government, non-government and civil society should play to mitigate biorisk. This instrument is characterized by a flexible, three-level approach—group, institutional and regional or national levels—to the assessment of threats posed by emerging technologies and includes recommendations for policy makers to implement effective regulatory procedures informed by the assessment.[2] This paper constitutes an explicit

[1] In particular, credit to advance these efforts should be given to the World Health Organization (WHO) to create a 'global biorisk management framework'. See WHO, 'Responsible life sciences research for global health security: A guidance document', WHO, 2010. See also, inter alia, Mancini, G. and Revill, J., Fostering the Biosecurity Norm: Biosecurity Education for the Next Generation of Life Scientists (Landau Network-Centro Volta/ Bradford Disarmament Research Centre: 2008); and Perkins, D. et al., 'The culture of biosafety, biosecurity, and responsible conduct in the life sciences: A comprehensive literature review', *Applied Biosafety*, vol. 24, no. 1 (Mar 2019), pp. 34–45.

[2] Tucker, J. B., *Security: Managing the Risks of Emerging Biological and Chemical Technologies* (MIT Press: Cambridge, MA, 2012).

attempt to add the individual as a fourth level to the existing three-level approach. In so doing, it focuses on the first practical steps that could be taken by individual practitioners directly involved in the research activities and conceptualizes what a toolkit for these individuals might involve.

The first part of the paper lays the foundation for the proposed toolkit. Section 1 outlines the broader landscape in which biorisk assessments are carried out. It identifies key concepts and maps the relevant existing mechanisms and instruments for managing biorisk. Section 2 situates biosecurity risk assessments within a wider biosecurity management system, looking at the role of the individual in this context and the specific questions individuals must consider in identifying whether any aspect of their research poses a potential risk. The second half of the paper sketches what a toolkit might look like and then gives it a trial run. Section 3 focuses specifically on how life scientists might go about conducting a risk assessment and identifying strategies to manage the aspects of their project they have identified as having the potential for misuse. Its approach is centred on a series of steps grouped under three 'pillars' that adopt parts of Tucker's proposed Decision Support Framework. Section 4 concludes by deploying the sample approach, using one potential application from nanobiotechnology for demonstration purposes. The conclusions consider next steps.

# 1. Understanding the biorisk landscape

## Key concepts used in biorisk management frameworks

### *Biorisk, biosafety and biosecurity*

'**Biorisk**' is short for 'biological risk' and refers to risk that arises in relation to **biological agents**.[3] The two main technical concepts in the biorisk context are **biosafety** and **biosecurity**.[4] The World Health Organization (WHO) defines **biosafety** as the containment principles, technologies, measures and practices that can be used to prevent unintentional exposure to, or inadvertent release of, biological agents. It defines **biosecurity** as the principles, technologies, measures and practices that are implemented for the protection, control and accountability of biological agents, data or equipment, biotechnologies, skills and information related to their handling. Biosecurity aims to prevent their unauthorized access, loss, theft, misuse, diversion or release.[5] In general, life science practitioners are familiar with biosafety as a standard part of their socialization into the field; many are less familiar with biosecurity both as a concept and as something to be applied directly to their work.

### *Contextualizing biorisk*

Given the different definitions of biosafety and biosecurity, biorisk can express itself in different ways depending on the context.

In the context of biosafety, biorisk is an expression of the probability of harm caused by biological hazards. A particular biorisk is determined by the type of biological hazard (e.g. a biological agent such as a virus), the likelihood of an undesirable event involving the biological hazard (e.g. accidental human contact with the virus) and the consequences of the event (e.g. a life-threatening infection).

In the context of biosecurity, biorisk is an expression of the probability of harm as the result of *unintended consequences* of research or *intentional misuse* of biological agents, data or equipment, biotechnologies, and skills and information related to their handling.

Importantly, for the purpose of a proposed toolkit, both contexts necessitate biorisk assessments. Biosafety management requires biorisk assessments along a rather technical definition, whereas biosecurity management requires biorisk assessments along a broader definition.

### *Dual-use and misuse potential*

Biological materials, products, technologies, software, information, know-how and research results are generally used for legitimate purposes for ultimately beneficial outcomes. However, risk arises from an item's dual-use or misuse potential. Biosecurity risk management is about preventing the use for harmful outcomes.

The terms 'dual-use' and 'misuse' potential are sometimes used interchangeably or with slightly different interpretations within the literature. This paper proposes that any provisional toolkit takes the definitions outlined here.

**Dual-use** refers to those materials, products, technologies, information, methods and knowledge generated by legitimate research that can be used for both beneficial

[3] A biological agent is microorganism, virus, biological toxin, particle or otherwise infectious material, either naturally occurring or genetically modified, which may have the potential to cause infection, allergy, toxicity or otherwise create a hazard to humans, nonhuman animals or plants.

[4] With the development of a universal toolkit in mind, it should be noted that the difference between biosafety and biosecurity can be blurry, and the terms do not always translate equally in different languages.

[5] World Health Organization (WHO), *Global Guidance Framework for the Responsible Use of the Life Sciences: Mitigating Biorisks and Governing Dual-use Research* (WHO: Geneva, 2022), pp. xviii–xix, fig. 1.

**Table 1.1.** International instruments relevant to biosafety and biosecurity

| Instrument title in full | Short title | Entry into force | Relevance to biosafety and biosecurity |
|---|---|---|---|
| Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare | Geneva Protocol of 1925 | 8 February 1928 | • Prohibits chemical and biological warfare<br>• Perceived as customary international law which is binding on all states |
| Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction | Biological Weapons Convention, BWC | 26 March 1975 | • Prohibits non-peaceful uses of biological agents and toxins independent of their origin and their means of delivery (general purpose criterion) |
| Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques | ENMOD | 5 October 1978 | • Prohibits misuse of environmental modification techniques having widespread, long-lasting, or severe effects as the means of destruction, damage or injury to another state party |
| Convention on Biological Diversity | Convention on Biodiversity, CBD | 29 December 1993 | • Promotes the conservation of biological diversity, the sustainable use of its components, and the fair and equitable sharing of the benefits arising out of the use of genetic resources |
| Cartagena Protocol on Biosafety to the Convention on Biological Diversity | Cartagena Protocol | 11 September 2003 | • Aims to ensure the safe handling, transport and use of genetically modified organisms |
| Nagoya Protocol on Access to Genetic Resources and the Fair and Equitable Sharing of Benefits Arising from their Utilization to the Convention on Biological Diversity | Nagoya Protocol | 12 October 2014 | • Aims to ensure the benefits arising from the use of genetic resources are shared in a fair and equitable way |
| Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction | Chemical Weapons Convention, CWC | 29 April 1997 | • Prohibits non-peaceful use of highly toxic chemicals and their means of delivery (general purpose criterion)<br>• Explicitly regulates two toxins (ricin and saxitoxin) |

| Instrument title in full | Short title | Entry into force | Relevance to biosafety and biosecurity |
|---|---|---|---|
| United Nations Security Council Resolution 1540 (2004) | Resolution 1540 | 28 April 2004 | • Prohibits UN member states 'from providing any form of support to non-State actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery'<br>• Requires states to 'adopt and enforce appropriate effective laws' and domestic controls to support this prohibition |

and harmful purposes. **Dual-use potential** is the mere existence of dual uses of a given item or the feasibility of an item's use for harm as well as good, as determined by the item's technical features and its usability.

**Misuse** refers to the use of biological materials, products, technologies, information, methods and knowledge for malicious purposes, with the intent to cause harm. **Misuse potential** is the feasibility of misusing a given dual-use item for malicious purposes, as determined by the accessibility of the dual-use item, the ease of misuse (e.g. feasibility of malevolent applications), and the level of harm-causing consequences. There are three main categories of biological misuse: bioweapons, bioterrorism and biocrime.[6]

## Mapping the existing mechanisms and instruments for managing biorisk

There are a number of legal instruments and frameworks at the international and national levels that seek to mitigate the potential harm caused by life sciences research. Additionally, there is a range of voluntary, institutional and field-wide standards and codes in circulation that seek to inform research practice. However, as the mapping below illustrates, biorisk assessment—as it relates to both biosafety and biosecurity—is neither mandated (as a required practice) nor mainstreamed (as a norm) as a standard activity assigned to individuals.

### *Legal obligations and controls*

Legal obligations and controls at the international, national, institutional and group or laboratory levels are woven together in specific ways, and can range from more to less restricting depending on where a practitioner works or lives. Thus, efforts to codify and control the potential dangers of life sciences research may leave gaps of various kinds and at different levels. Establishing and mainstreaming a universal biorisk assessment toolkit at the level of individual scientists would work to close these gaps and increase both biosafety and biosecurity.

**International treaties.** Most states have ratified multilateral treaties aimed at preventing biological harms, such as the Biological and Toxin Weapons Convention (BWC) or the Convention on Biological Diversity (see table 1.1). States that are parties to the BWC have called for synchronized political actions towards improving awareness among scientists about biosafety and biosecurity. Individual scientists should be

[6] Katona, P. and Carus S., 'The history of bioterrorism, biowarfare, and biocrimes', eds P. Katona, J. P. Sullivan and M. D. Intriligator, *Global Biosecurity: Threats and Responses*, 1st edn (Routledge: Abingdon, 2010).

aware of the relevant treaties that apply to the country in which they work, and of international perspectives on their work.

**National and regional laws.** States parties to international conventions will have introduced, at national and regional levels, laws to comply with their treaty obligations, as well as other laws regulating biological science practices and use of biological agents. Examples include laws and regulations around genetic engineering, export controls (see below), and weapons non-proliferation measures. Individual scientists must understand the legal framework in which they work.

**Export controls.** A number of export control regimes are in place to manage risks arising from cross-border transfers of prohibited or dangerous goods. One of these is the Australia Group (AG), an informal forum of countries that seeks to ensure that exports do not contribute to the development of chemical or biological weapons, which assists states to comply with their BWC obligations. One of the mechanisms the AG uses is harmonization of regulations around exports. Export control regimes rely in part on lists of dual-use items such as selected biological agents (certain pathogens and toxins) and devices (e.g. biofermenters), to which controls—such as an export licence—apply. The AG maintains five such lists, two relating to chemical weapons and three relating to biological agents: dual-use biological equipment and related technology and software; human and animal pathogens and toxins; and plant pathogens.[7] In addition to specified controls, 'catch-all' controls apply to any export item where there is reasonable doubt about its use for legitimate or peaceful purposes. In countries where export control regulations are in place, it is mandatory for an individual scientist or exporter of a controlled item to assess risks associated with certain types of technologies, materials, knowledge and dedicated dual-use items, in order to obtain an export licence. This means that individual scientists must understand which aspects of their work are subject to export controls, and which might be exempt as being a certain type of scientific or technological activity. For example, 'basic' or 'fundamental' research is generally not subject to export controls, but scientists cannot assume that all research projects classified as basic research or that every aspect of a basic research project will be exempt.[8] Ideally, a scientist's institution will have compliance experts to provide support for this process.

### *Voluntary standards and codes*

Many laboratories that handle biological agents choose to implement voluntary international, regional and national standards and codes. Practitioners are generally required to comply with the measures set out in such standards and codes as are implemented at their laboratory.

**International standard IS35001: Biorisk management for laboratories and other related organizations.** This standard provides a framework for implementing biorisk management processes in laboratories and other places that use, store, transport or dispose of hazardous biological materials.

**Laboratory Biorisk Management Standard CWA 15793:2011.** This voluntary standard developed by the European Committee for Standardization (CEN) is applicable to all institutions, industries and organizations handling biological agents and toxins. It includes both biosafety and biosecurity measures as the basis for a biorisk management system.

[7] Australia Group, 'Australia Group Common Control Lists', [n.d.].

[8] For examples of guidance documents in the United States and the European Union see, respectively, US Department of Commerce, Bureau of Industry and Security, 'Deemed exports and fundamental research for biological items', [n.d.]; and European Commission, 'Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items', *Official Journal of the European Union*, L338, pp. 3–52 (Annex).

**Codes of conduct and guidelines.** The scientific community has itself considered the risks and benefits of science and technology, and developed a number of voluntary codes of conduct and guidelines. Those that apply to biorisk management are listed among the tools and resources included at the end of this section.

**Journal editorial policies.** Publishers of scientific articles and editors responsible for journal policies recognize their 'vital role in ensuring that effective safeguards exist to cope with the risks of publishing scientific research with dual-use implications'.[9] While studies in 2011 and 2012 found that very few journals had policies in place to review submissions for dual-use potential, and a lack of consensus on standards for appropriate review procedures, in 2023 it is increasingly likely that journals will require some form of biorisk assessment to be undertaken before publication.[10]

### *Institutional and funding requirements*

**Workplace rules.** Many workplaces where biological agents are used—research institutes, universities, private laboratories, and so on—have their own biosafety and biosecurity rules and systems, often so that the workplace complies with national laws and passes safety inspections. The workplace may also have decided to implement particular standards or codes. Many workplaces will have a dedicated compliance and risk department or manager responsible for overseeing legal and standards compliance, and for providing relevant training to staff. It will usually be a condition of employment or contract that the science practitioner complies with the workplace rules, including by attending the training.

**Funding agencies.** Some funding agencies already require applicants for research grants to provide assessments on the dual-use potential of the planned research work. Examples include Horizon Europe in the European Union (EU), the German Research Foundation and the National Institutes of Health (NIH) in the United States.

### *Other tools and resources*

**International and general.** Although not exhaustive, the selective list below illustrates that there is a range of resources targeted at an international or general audience that seek to improve biorisk management.

- The Biosecurity Central website provides 'a curated set of resources and tools applicable across the spectrum of biosecurity'.[11]
- The WHO provides a *Global Guidance Framework for the Responsible Use of the Life Sciences: Mitigating Biorisks and Governing Dual-use Research* that contains a helpful glossary, checklists and other tools for use at all levels and stakeholders, including governments and funding bodies.[12] See also the WHO's *Laboratory Biosecurity Guidance: Biorisk Management*.[13]
- The International Working Group on Strengthening the Culture of Biosafety, Biosecurity, and Responsible Conduct in the Life Sciences provides a guide that includes extensive training materials for use by laboratory managers at research institutes.[14]

[9] Patrone, D., Resnik, D. and Chin, L., 'Biosecurity and the review and publication of dual-use research of concern', *Biosecurity and Bioterrorism*, vol. 10, no. 3 (2012), p. 290.

[10] Patrone, Resnik and Chin (note 9); and Resnik, D. B., Barner, D. D. and Dinse, G. E, 'Dual-use review policies of biomedical research journals', *Biosecurity and Bioterrorism*, vol. 9, no. 1 (2011).

[11] Biosecurity Central, 'Our project and the biosecurity community', [n.d.].

[12] WHO, *Global Guidance Framework for the Responsible Use of the Life Sciences* (note 5).

[13] WHO, *Laboratory Biosecurity Guidance: Biorisk Management* (WHO: Geneva, 2006).

[14] International Working Group on Strengthening the Culture of Biosafety, Biosecurity, and Responsible Conduct in the Life Sciences, *A Guide to Training and Information Resources on the Culture of Biosafety, Biosecurity, and Responsible Conduct in the Life Sciences* (2021).

- The SIPRI *Handbook of Applied Biosecurity for Life Science Laboratories* provides practical advice to people who work with infectious pathogens and toxins.[15]
- The most recent and comprehensive biosecurity code of conduct is the 'Tianjin Biosecurity Guidelines for Code of Conduct for Scientists', produced under the umbrella of the InterAcademy Partnership.[16]
- To raise awareness about dual-use potential and the need for biorisk mitigation on a global level, the International Genetically Engineered Machine (iGEM) competition requires participating teams (mostly students who work on projects in synthetic biology) to perform biosafety and biosecurity assessments following instructions provided by the organizers.[17] The iGEM website contains a number of tools, policies, quizzes and other resources that explore safety and security practices, with a focus on responsible project design.[18]

**National.** A number of countries provide guidelines to life science practitioners. While the guidelines are not legally binding as such, they seek to raise biorisk awareness and increase biorisk management practices. However, some are mandatory for funding applications and recipients. The examples below are from Germany, the Netherlands, the United Kingdom and the USA. Individual scientists should check with the national authorities and funding bodies that govern their laboratories as to guidelines that are available or that may be mandatory.

In Germany, the Federal Office for Economic Affairs and Export Control provides a toolkit for researchers in Germany to better understand EU export control legislation. The toolkit, which is published in both German and English, provides workflows and selected study cases to guide users through legally required assessment of the dual-use potential of results, materials and technologies, with an emphasis on export control licensing procedures.[19] The Max Planck Society has published guidelines and rules on responsible practice of science for German research institutes.[20] The German Research Foundation and German National Academy of Sciences Leopoldina used this as a basis for a set of recommendations for handling security-relevant research.[21]

In the Netherlands, the *Guidelines for Researchers on Dual Use and Misuse of Research* assist EU practitioners in understanding their legal obligations and other relevant regulations in all scientific disciplines, including biological sciences. The guidelines contain background information and workflows for identifying dual-use potential and export license requirements.[22] The Biosecurity Working Group of the Royal Netherlands Academy of Arts and Sciences has also published *A Code of Conduct for Biosecurity* that aims 'to prevent life sciences research or its application from directly or indirectly contributing to the development, production or stock- piling

[15] Clevestin, P., *Handbook of Applied Biosecurity for Life Science Laboratories* (SIPRI: Stockholm, 2009).

[16] Tianjin University Center for Biosafety Research and Strategy, Johns Hopkins Bloomberg School of Public Health Center for Health Security and InterAcademy Partnership, 'Tianjin Biosecurity Code of Conduct', 7 July 2021.

[17] iGEM, 'What is iGEM?', [n.d.]. See also Millett, P. et al., 'The synthetic-biology challenges for biosecurity: examples from iGEM', *Nonproliferation Review*, vol. 27, nos. 4–6 (2020).

[18] iGEM, 'Responsible design', [n.d.].

[19] German Federal Office for Economic Affairs and Export Control (BAFA), *Export Control and Academia Manual* (BAFA: Eschborn, Feb. 2019).

[20] Max Planck Society), 'Guidelines and rules of the Max Planck Society on a responsible approach to freedom of research and research risks', 2010.

[21] German Research Foundation (DFG) and German National Academy of Sciences Leopoldina (Leopoldina), *Scientific Freedom and Scientific Responsibility: Recommendations for Handling Security-Relevant Research*, 2nd edn (DFG and Leopoldina: Halle, 2022).

[22] Flanders Institute for Biotechnology, imec, and the Flemish Interuniversity Council, *Guidelines for Researchers on Dual Use and Misuse of Research* (Oct. 2017).

of biological weapons' as described in the BWC, 'or to any other misuse of biological agents and toxins'.[23] The code includes valuable background information, case studies, and six main rules of conduct: raising awareness, research and publication policy, accountability and oversight, internal and external communication, accessibility, shipment and transport. It also gives examples for identifying dual-use potential in infection biology.

In the UK, the national biological and medical research councils and the Wellcome Trust released a joint policy statement in 2016 on managing the risks of research misuse. The statement refers to criteria for identifying dual-use potential and highlights two important additional areas of dual-use research: 'new technologies or tools with generic applications—such as in the areas of bio-processing or bio-fermentation scale-up—which could, for example, make it easier to synthesise or produce harmful agents'; and 'projects that carry very little potential for misuse, but where the risk would be greatly increased by emerging data or methodologies from other disciplines'.[24]

In the USA, the NIH provides a guide to government policies for oversight of dual-use research in the life sciences.[25] The guide incorporates risk assessment strategies proposed by the US National Science Advisory Board for Biosecurity.[26] It also contains valuable tips for assessing dual-use potential, including 'ease of misuse'.[27] In Canada, the Canadian Biosafety Guideline: Conducting a Biosecurity Risk Assessment provides guidance for practitioners in the life sciences working with pathogenic microorganisms how to perform a biosecurity risk assessment of the own work. Quantitative and qualitative approaches are used to assess the likelihood of biosecurity events, severity of consequences, and risk level evaluation.[28]

[23] Royal Netherlands Academy of Arts and Sciences (RNAAS), Biosecurity Working Group, *A Code of Conduct for Biosecurity* (RNAAS: Amsterdam, Aug. 2008), p. 11.

[24] British Biotechnology and Biological Sciences Research Council, Medical Research Council and Wellcome Trust, 'Managing risks of research misuse', Joint policy statement, 8 Jan. 2016, p. 4.

[25] National Institutes for Health (NIH), *Tools for the Identification, Assessment, Management, and Responsible Communication of Dual Use Research of Concern: A Companion Guide to the United States Government Policies for Oversight of Life Sciences Dual Use Research of Concern* (NIH: Bethesda, MD, Sep. 2014).

[26] National Science Advisory Board for Biosecurity (NSABB), *Proposed Framework for the Oversight of Dual Use Life Sciences Research: Strategies for Minimizing the Potential Misuse of Research Information* (NSABB: Washington, DC, June 2007).

[27] NIH (note 25), pp. 26–28.

[28] Canadian Government, *Canadian Biosafety Guideline: Conducting a Biosecurity Risk Assessment* (Public Health Agency of Canada: Ottawa, 25 Jan. 2018).

# 2. Biosecurity risk assessment in practice

## Biorisk assessments within a wider biosecurity management system

The proposed toolkit presented in section 3 of this paper is designed to supplement other guidance documents and tools, to provide individual scientists and practitioners in the life sciences with a universal approach to conducting their own biorisk assessments as part of a wider biosecurity management system. Such a system generally follows the six-step approach developed by the WHO:

1. Identify and assess risks and benefits
2. Describe values, principles and goals
3. Undertake stakeholder analysis
4. Identify tools and mechanisms
5. Implement the identified tools and mechanisms
6. Review performance and modify (adapt) as needed.[29]

The proposed toolkit focuses on steps 1 and 4—identifying and assessing biorisks, and the tools and mechanisms to mitigate those risks. It aims to provide questions that guide the user through the assessment of risks associated with their own scientific activities. Carefully conducted, the risk assessment could potentially allow the user to improve their laboratory or organization's planning of risk mitigation strategies and support them in establishing a 'biosafety and biosecurity culture' in their workplace as well as globally. The proposed toolkit could also enable the user (and their laboratory or organization) to demonstrate that their work is conducted in a responsible manner.

## When to undertake biosecurity risk assessment

Biosecurity risk assessment is a continuous process. Ideally an individual scientist will assess the biosecurity risks at the planning stage of each specific research project—even if there is no legal obligation to do so—then review the assessment periodically and adapt the risk mitigation measures as needed. But if a project is already underway without having been comprehensively assessed for biorisk, the project's lead scientist should prioritize conducting a biosecurity risk assessment as soon as possible.

## Identifying goals and participants

The scientist must understand their task: why they are conducting the risk assessment. There are likely to be several primary goals, including to meet a specific compliance requirement, such as a grant application; to take responsibility not only for the beneficial consequences of their work, but also the potential negative consequences; and to assist their workplace, regulatory authorities and the wider science community in preventing their work from being misused. There are also likely to be some secondary outcomes that they want to pursue, such as improved planning of the research project; fostering a shared view of the project among all participants; and identifying who has responsibility for specific risk management strategies.

Understanding their specific goals will help them identify who else needs to be involved in the process. The risk assessment should involve, at a minimum: anyone

[29] WHO (note 5), p. 78, fig. 1.

who will be directly involved with the (planned) work; the principal investigator or laboratory head supervising the work; and relevant actors at the workplace such as compliance officers and safety supervisors. In most projects there will be several participants with various roles at different levels.

**Individuals.** Biosecurity risk assessment must start at the lab bench by the people best able to conduct rather technical risk assessments.

**Group.** Individual scientists might act as drivers for biosecurity risk assessments but should engage their colleagues in their research team, group or laboratory in discussion of potential risks and appropriate mitigation strategies. In many cases the discussion should also encompass colleagues and experts outside the immediate workplace and field of expertise, as biorisks may require multidisciplinary risk assessment strategies.

**Institutional.** Biosecurity risk mitigation strategies will need institutional support to achieve engagement of individual scientist, research teams, principal investigators and decision makers.

**Regional and national.** Depending on domestic requirements, the assessment process may need to involve regulatory authorities and other review bodies on biosafety and biosecurity, who will have a broader awareness about identified research risks.

## Identifying dual-use and misuse potential of scientific work

One of the first questions a scientist must ask is whether any aspect of their project has potential for dual use. Almost all biological material, technology, information, skills, knowledge and research results has dual-use potential. Because infection biology and toxicology have historically formed the basis of offensive biological and toxin weapons development, biosecurity risk assessments often focus on understanding dual-use potential of biological threat agents. The approach to biosecurity risk assessment of microbial pathogens and toxins fell into three types: (*a*) *agent-based*: the risk that a biological agent is inherently harmful; (*b*) *method-oriented*: the risk that a biological experiments or methods will cause harm; and (*c*) *results-based*: the risk that the results of biological research will cause harm if used for a harmful purpose. This historical approach to microbial pathogens and toxins can be applied to other life sciences and related disciplines, including neurophysiology, epigenetics, synthetic biology, nanobiotechnology.

For each life sciences project, the individual scientist should consider:

- What *agents* will be used in the project? Are any of these inherently harmful to people, animals or the environment—for example, pathogens and toxins?
- What *methods* will be used in the project? Do any of these have the potential to cause harm to people, animals or the environment—for example, inhalation experiments, targeted drug delivery, genetic manipulation of animal populations?
- Can the intended *results* of the research be misused? If misused, could the results cause harm to people, animals or the environment? Examples might be research into the relationship between particle sizes of pathogen-loaded bioaerosols and infection rates, drug delivery across the blood–brain barrier, or elimination of pathogen-transmitting animal species in nature.

**Box 2.1.** Questions to identify potential misuse of research funded by the European Union

- Could the materials/methods/technologies or knowledge concerned physically or in any other way harm people, animals or the environment, by themselves or if modified or enhanced?
- Could the materials/methods/technologies or knowledge concerned, physically or in any other way, have direct negative impacts on the security of individuals, groups or states?
- Could the unauthorised disclosure of the materials/methods/technologies or knowledge concerned prejudice the interests of the European Union or of its Member States?
- Does the activity involve the development of surveillance technologies?
- What would happen if they ended up in the wrong hands?
- Could they serve any purposes other than the intended ones? If so, would that be unethical?
- Does the activity involve minorities or vulnerable groups or activities involving the development of social, behavioural or genetic profiling technologies?
- Does the activity generate knowledge, materials and technologies that could be used for criminal or terrorist purposes?
- Could the activity result in the development of chemical, biological, radiological or nuclear (CBRN) weapons or any method for their delivery?

*Source*: European Commission, Directorates-General for Migration and Home Affairs and for Research and Innovation, 'Guidance note: Potential misuse of research', version 2.0, 14 Sep. 2021, p. 2.

Another way to identify whether a project has dual-use potential is to use one or both of the tools described below. These tools use guiding questions for identifying dual-use or misuse potential in any research project proposal.

### *European Commission questions on misuse potential*

The first example is a set of guiding questions provided by the European Commission, which provides guidance for applicants preparing EU research grant proposals.[30] The guideline asks researchers to consider the research project's immediate aims and intended applications; whether the research could serve 'unethical or malevolent purposes'; and any risks that could outlast the project's duration.[31] It then poses a series of questions about the project (box 2.1). This example was taken to highlight that funders already acknowledge the importance of biosecurity risk assessments, and to demonstrate that development of a 'gold standard' for tackling dual-use issues in research is underway, with the EU as one of the key players. Even if scientists are not seeking EU funding and so are not required to assess misuse potential of their planned research work, they should still find this set of questions useful for identifying the misuse potential of their work.

The European Commission's questions are very general, being designed to apply to all research projects, not just those in the life sciences. Although they are useful for raising awareness about the kinds of malicious purposes to which research can be applied, some of which might not occur to scientists about their work—for example, its application to vulnerable groups—the specific threat potential of research using biological agents requires a more targeted set of questions.

[30] European Commission, Directorates-General for Migration and Home Affairs and for Research and Innovation, 'Guidance note: Potential misuse of research', version 2.0, 14 Sep. 2021.
[31] European Commission (note 30), p. 2.

**Box 2.2.** Questions to identify dual-use potential of aspects of research

- Are you working with a biological agent, or parts of it, that can be considered a high-risk pathogen?
- Is the host range or tropisma of the biological agent likely to be altered?
- Could your research increase the virulence of the biological agent?
- Do you expected the stability of the biological agent outside the host to increase as a result of your research?
- Is it likely that the transmissibility or ability for dispersion or dissemination of the biological agent will increase?
- Do you expect the absorption of the biological agent to be facilitated or an increased toxicokinetic effect?
- Is it likely that your research will increase the resistance of the biological agent to clinical or agricultural prophylactic or therapeutic interventions, including antimicrobial resistance?
- Does the biological agent possibly have a negative effect on the immunity of humans, animals or plants?
- Could your research impact the detection methods, diagnostics or clinical diagnosis of the biological agent?
- Does your research contribute to the reconstruction of an eradicated or extinct biological agent?
- Could changes to the biological agent possibly generate or enhance harmful consequences that could involve 'improved weaponization'?
- Is it likely that the knowledge you obtain and technologies you develop in your research could allow others to use them for malicious purposes?
- Could your research contribute to possible harmful ecological consequences due to misuse of the modified biological agent or the knowledge thereof?
- Could your research contribute to possible harmful economic consequences due to misuse of the modified biological agent or the knowledge thereof?
- Could your research contribute to possible harmful consequences for society due to misuse of the modified biological agent or the knowledge thereof?

*Source:* Netherlands Biosecurity Office, 'Questionnaire', Dual-Use Quickscan, [n.d.].

### *Dual-Use Quickscan tool*

The second example presents a set of guiding questions that focus on biosecurity risks associated with pathogens and toxins for human, animal, and plant health. The Dual-Use Quickscan tool developed by the Dutch Biosecurity Office is an interactive web-based tool that guides the user through 15 questions about different aspects of research that may contribute to its dual-use character: 11 questions on the characteristics of the biological agent; 1 question on knowledge, methods and technologies; and 3 questions on possible consequences of misuse for ecology, the economy and society (box 2.2).[32] Answering 'yes' to one or more of these 15 questions means the project has dual-use potential, and is the trigger for proceeding to a comprehensive risk assessment.

Again, these questions are useful for raising awareness of biosecurity risks that the researcher may not have thought of, such as ecological and economic impacts of their project if misused. However, they are too specific to be of universal application.

[32] Netherlands Biosecurity Office, 'How do I fill in the Dual-Use Quickscan?', *Dual-Use Quickscan*, [n.d.]. See also Vennis, I. M. et al., 'Dual-Use Quickscan: a web-based tool to assess the dual-use potential of life science research', *Frontiers in Bioengineering and Biotechnology*, vol. 9 (2021).

### *An alternative approach*

The above examples of guiding questions demonstrate that some approaches are very broad while others are very narrow. They also tend to apply to the project as a whole rather than individual aspects. These dual-use assessments might reveal that there are certain research activities that have a rather remote dual-use potential and others that could be directly misapplied for causing great harm. The latter is termed 'dual-use research of concern', a technical term used for example in the USA to allow for tailored regulation of a subset of research activities in the life sciences.[33] There is an ongoing debate as to the usefulness of this term, but any instrument which helps the individual practitioners in the life sciences to identify misuse potential and severe research risks is most welcome.[34]

The next section presents an approach in this vein. It underlines the agency of the scientist, providing them with a readily implementable means to assess biorisk in their own research. The approach also avoids downplaying the severity of any misuse potential of the research activity under examination, because this has its own risks. For example, neglecting biosecurity risk assessment of work with potential pandemic pathogens is conflict with research ethics and might even pose a violation of legal obligations. Rather, this paper recommends a proactive and stringent approach to clearly identify any dual-use or misuse potential of each aspect of a life sciences project and to identify strategies for risk mitigation.

[33] See US Government, 'United States Government policy for institutional oversight of life sciences dual use research of concern', 24 Sep. 2014.

[34] Casadevall, A. et al., 'Dual-use research of concern (DURC) review at American Society for Microbiology Journals', *mBio*, vol. 6, no. 4 (2015).

# 3. Proposed approach for a practical biorisk assessment toolkit

Active engagement by the life science community can help complement the component parts of the landscape discussed in the previous section. After all, there remains no global harmonization of mandatory biosafety and biosecurity standards, even if the recent WHO *Global Guidance Framework* represents a step in this direction. Follow-on activities should centre on the development of practical tools that can facilitate assessment of dual-use and misuse potential and the development of adequate risk mitigation strategies.

While numerous approaches are possible, the provisional toolkit presented in this section presents a more readily implementable approach for the individual practitioner that centres on the following three pillars:

- Pillar 1. Scientific–technical assessment of biological risks
- Pillar 2. Evaluation of potential misuse scenarios
- Pillar 3. Identification of appropriate measures for mitigating risks of misuse.

These pillars adopt parts of the Decision Support Framework proposed by Jonathan Tucker.[35] The starting point is the list of items in a science project that have been identified as having dual-use or misuse potential (see section 2). Under pillar 1, each of these items is then analyzed for risk in detailed scientific–technical terms. The individual scientist who planned the project is best placed to undertake this analysis, along with any colleagues working directly on specific aspects, as they know the science and technology involved and the expected results. The results of the analysis are recorded and, in pillar 2, evaluated for their misuse potential according to risk scales and other metrics. The result is a number representing a risk level in terms of likelihood and severity of impact. Under pillar 3, the number guides the scientist in identifying the appropriate measures and priorities in mitigating the risks.

All analyses and recommendations are recorded. The scientist is then able to take these detailed records of their risk assessments to the group, institution and national or regional levels for a number of purposes, including implementation of the measures, providing evidence of undertaking the assessment (e.g. for funders or for safety compliance), and contributing to the group or institutional knowledge base. For these reasons, and because proactively taking measures to prevent or mitigate the risk of misuse will allow individual scientists to do their work safely, securely and responsibly, it is highly recommended that scientists perform the steps in this proposed biosecurity risk assessment even where such assessments are not mandatory under legal, funding or institutional procedures.

## Pillar 1. Scientific–technical risk analysis

### *Defining the potential harm in detailed scientific–technical terms*

For each aspect of a life sciences project identified with dual-use or misuse potential, the individual practitioner working on the project should define the specific harm that might be caused if the potential is realized. The recommended approach is to use the following five parameters: (*a*) general level and type of harm; (*b*) mechanisms by

[35] See Tucker (note 2), p. 2.

**Box 3.1.** Some practical tips for performing the scientific–technical risk analysis

- Allow plenty of time to perform the assessment during the first phases—don't try to squeeze the task into a heavy workload.
- Start with a few thoughts about your concerns and write them down in short sentences, before going deeper.
- When obtaining feedback, invite others to extend your initial views in a collaborative manner.
- Avoid generating a substantial body of 'blueprints for misuse' or sharing your concerns and findings about misuse potential in forums you cannot control, such as social media.
- Remember to check for inhouse knowledge about biosecurity-relevant issues that might already be in place.

which the harm is effected, down to molecular levels if appropriate; (*c*) who or what might be harmed and at what scale—individuals, populations, species or ecosystems; (*d*) the extent to which the harm is reversible (e.g. illness) or irreversible (e.g. death); and (*e*) general applicability of the technology/knowledge for other misuse cases (e.g. development of platform approach to synthesise any RNA virus including highly virulent strains).

It is important that the scientist is both honest and realistic in assessing the potential harm that each aspect of their project could cause if misused. That means paying attention not just to obvious and likely scenarios but also worst-case scenarios, however unlikely or impractical they may seem. However, the scientist must take care not to include too much detail and inadvertently create a list of ideas and ways in which to misuse their work. This provisional toolkit suggests structuring the risk assessment along a few select, not very detailed, scenarios for the misuse of the research work to inform the next step of the risk assessment. Scientists might need some practical advice in conducting the risk analysis. An example of the kind of tips that could be provided in a toolkit are shown in box 3.1.

### *Documenting the analysis*

Although documenting the initial analysis can begin in short notes , the scientific–technical basis for any concerns needs elaboration in a detailed record. The record should set out the specific harm under each of the above five parameters, and also include the evidence base for the concerns (see table 3.1).

Keeping a record of the analysis should (*a*) make follow-up evaluations of identified biorisks much easier; (*b*) allow the scientist to demonstrate that they take their scientific responsibilities seriously; and (*c*) enable sharing of the analysis to obtain feedback—the next step recommended in the process. Once created, the record will need to be kept in a secure location, protected from unauthorized access or dissemination, with a level of security appropriate to the threat level shown in the analysis and the inherent sensitivity of the information. This might require establishing strategies to manage 'information hazards', if these are not already in place.[36]

### *Obtaining feedback*

The next step is for the scientist to obtain feedback on their risk analysis from other experts in their field, including : (*a*) selected colleagues at their institution; (*b*) persons with institutional oversight (e.g. department head, a biosafety and biosecurity steering committee); and (*c*) experts in their scientific–technical domain as well as in biosecurity.

Potential aims of the feedback process are: identifying missing information to complete the risk analysis; defining possible countermeasures against misuse of the

[36] Lewis, G. et al., 'Information hazards in biotechnology', *Risk Analysis*, vol. 39, no. 5 (2019).

**Table 3.1.** Example way to record a scientific–technical risk analysis of an aspect of a research project identified as having dual-use or misuse potential

| Risk parameter | [Name or description of research activity, material, technology etc. with dual-use or misuse potential] |
|---|---|
| Level / type of harm | [e.g. specify disease] |
| Mechanism of harm | [e.g. infection, contamination] |
| Subject(s) affected | [e.g. individuals, species, populations, ecosystems] |
| Extent of reversibility | [detailed description] |
| General applicability | [list of other misuse cases] |
| Evidence base | [scientific–technical basis for concern, including citations] |

(planned) scientific work; and generating a common understanding about risks and benefits of the scientific work conducted at the research facility.

## Pillar 2. The estimation of risk of misuse

The first steps in this proposed toolkit are identifying the aspects of the research project with dual-use potential, analyzing the risk and detailing their specific harm potential (pillar 1). Pillar 2 in the process is for the individual scientist to explore the *likelihood* of the harm being realized. This involves several steps to assess four risk attributes: (*a*) how accessible the risk item is to malicious actors; (*b*) how easy it is to use once accessed; (*c*) the magnitude of the potential harm if it is used; and (*d*) the likelihood of its use for specific harmful purposes such as bioweapons, bioterrorism or biocrime. While conducting these assessments will be challenging for the individual scientist, going through the process in this manner will at the very least enhance their awareness of relevant risk scenarios.

### *Describing the accessibility for malicious actors*

The first step is for the individual scientist to consider whether and how a broad range of malicious actors might try to get access to each risk item of their project. Access can mean actual theft, where biological material or equipment is physically removed from the laboratory, or copying of information such as data, methods and results. Classes of potentially malicious actors include both insiders and outsiders. Insiders might be scientists, students and other people working at the facility (e.g. executives, office staff, safety officers), as well as contractors hired by the facility (e.g. cleaners, maintenance workers, security guards). Outsiders might be visitors to the facility (including visiting scientists granted special access); criminals either working alone or as part of a gang or syndicate; terrorists (as part of domestic or international terrorist groups, or radicalized individuals); state-sponsored infiltrators (e.g. hackers, agents of intelligence services or the military, government officials); and non-state infiltrators such as competitor organizations, activists or militant groups.[37]

Preventing access involves assessing current levels of security measures at the scientist's facility: how easy it is for different types of actors to access the laboratory, storage facilities and information systems. It also involves assessing whether, and which, aspects of the risk item are: (*a*) already in the public domain; (*b*) published in closed forums (and how secure those forums are); (*c*) commonly available in most laboratory settings; or (*d*) readily available for purchase.

[37] Canadian Government, 'Appendix D: Adversaries', *Canadian Biosafety Guideline: Conducting a Biosecurity Risk Assessment* (Public Health Agency of Canada: Ottawa, 25 Jan. 2018).

One way individual scientists could approach this task might be to think of accessibility as generally comparable to planning the transfer of each risk item from one laboratory to another (which occurs frequently in the sciences and of course with good intentions), which involves considering both security and availability. It would be expected that the recipient laboratory would already have or could easily gain access to a publicly available or ubiquitous item, but not certain materials, methods, technology and knowledge that is novel, dangerous, expensive or has other barriers to access.

### *Estimating how easy the misuse would be*

The next step proposed is for the individual scientist to assume that a malicious actor has gained access to the risk item, whether through theft or copying, and to consider whether that item is ready for use or if the actor needs to take further steps, and if so, how easy or difficult it will be to get the item ready for use. That is, how much time and effort might be required for a malicious actor to successfully establish the dual-use aspect of the project?

The individual practitioner's scientific–technical expertise is key to considering whether the dual-use item is in a finished state, or if it needs something additional before it can cause harm. Examples of additional steps or processes include: (*a*) modification; (*b*) further testing (e.g. animal tests, feasibility tests); and (*c*) special dissemination technologies or mechanisms. If the answer is yes to something additional being needed, the scientist must then consider the levels of sophistication, expertise and resources required to perform the modification, testing or dissemination. In other words, the scientist needs to assess the risk item's maturation level. In principle, this is very similar to the application of a new method or technology in the laboratory, but on the assumption there are bad intentions behind the use of the item.

In this respect, the other aspect of ease of use is considering which kinds of malicious actors might have the knowledge, training and resources to use the risk item and, where something additional is needed, to take those extra steps to get the item ready for misuse.

For example, CRISPR/Cas9 genome editing is now feasible for a broad range of actors because of the availability of commercial CRISPR/Cas9 kits. However, targeted and successful modification of genomes other than the ones intended by the vendor require specific knowledge of how to reprogramme the CRISPR/Cas9 machinery, how to synthesize new molecular components, and methods for testing the genome manipulation and delivery to the target individuals or species. For malicious actors who have or can readily acquire the resources and expertise, ease of use may be relatively straightforward. For other actors, such as individuals who lack either the knowledge or the resources or both, using the item will be very difficult.

### *Estimating the magnitude of potential harm*

The next step is for the scientist to assume a malicious actor has accessed the risk item and found a way to use it for a harmful purpose, and to consider the scale of the potential harm. This is a matter of considering, first, the direct effects of potential harm: the kinds of victims or targets that would be directly affected; the mechanisms, likelihood and speed at which the harm could spread (i.e. directly affect new victims or targets); the potential number of directly affected victims or targets; and the level of the harm, which could vary for different types of victims or targets. The second consideration is the types and extents of secondary effects. That is, if the harm were realized, how might this affect, for example, human well-being, societal structures, ecosystems, economies, trust in governmental institutions.

For instance, if genome editing targeting a specific plant or animal species were used by a malicious actor to sterilize that species, what might be the effect on ecosystems relying on that species, and would there be further consequences for food production and economies? Answering these questions involves a certain amount of hypothetical scenarios, but the practitioner could bring their scientific–technical expertise to access relevant research, obtain relevant data and make evidence-based estimations. For example, in infection biology, if the risk item is a pathogen, data on recent infectious disease outbreaks caused by the relevant pathogen could be used to inform this estimation. In the absence of relevant data, the scientists should make the most robust estimation possible with the knowledge they have. The aim is not to deliver a definitive answer to this question but rather to promote thinking about unwanted consequences of misuse of risk item under review.

### *Estimating the likelihood of misuse*

Even more than the other attributes in this pillar, this is quite difficult to estimate because it involves exploring intent behind the misuse. The task of estimating the 'likelihood of misuse' can be seen as similar to the common task in grant proposals of assessing 'potential future applications' of the proposed research. Here the individual scientist could identify the potential misuse and consider why a malicious actor would select the particular dual-use item of their project to cause the intended harm. Of course, scientists are unlikely to be able to provide definitive answers, but this step should help them to envision at least some abstract misuse scenarios of their work. Scientists do not need to consult experts or obtain access to sensitive background information in this respect; general reporting in the public domain and some general knowledge of the context in which they work—including the national and international security landscape—should suffice. Most scientists will know, for example, whether their state is currently in armed conflict with another, or whether they are collaborating with scientists in another state that is subject to political sanction, or whether there are ongoing pandemics or natural disasters that their project may have relevance for.

Classifying the nature of potential misuse as biocrime, bioterrorism or bioweapons may further help in this process. For example, a state actor developing a bioweapon with an indiscriminate dispersal method might consider the risk of harm to its own population too great to justify using it against another state, so the likelihood of this misuse scenario is low. But an activist wanting to use a toxin that requires immediate delivery to the target (e.g. direct injection) on a small number of specific people identified as obstacles to the activist's cause, or a state-sponsored agent aiming to use the toxin against people identified as enemies of the state, is much more likely to use the toxin for this purpose. Interrelated, the scientist needs to consider why a malicious actor might select the dual-use aspect under review to cause the harm. In the examples above, the state actor might consider other types of weapons easier to access, more effective and less risky than the bioweapon; and the activist and agent might consider it easier to cause the harm by using a method that does not require close contact with their targets (e.g. using a gun or a bomb).

### *Quantifying the estimates to estimate the level of misuse potential*

The result of these estimates is not merely an exercise in thought experiments for hypothetical scenarios but to quantify them to deliver a value for the level of misuse potential. For each scenario of misuse, the individual scientist should award a score of 0, 1 or 2 to each of the four risk attributes for each of the three different categories of biological misuse—bioweapons, bioterrorism and biocrime—as set out in table 3.2. For example, a toxin requiring direct injection to an individual will have different

**Table 3.2.** Quantification of misuse potential

| Risk attributes (point value) | Bioweapons | Bioterrorism | Biocrime |
|---|---|---|---|
| 1. *Accessibility* [a] | | | |
| Difficult (0) | | | |
| Limited (1) | | | |
| Simple (2) | | | |
| 2. *Ease of misuse*[b] | | | |
| Low (0) | | | |
| Medium (1) | | | |
| High (2) | | | |
| 3. *Magnitude of harm*[c] | | | |
| Low (0) | | | |
| Medium (1) | | | |
| High (2) | | | |
| 4. *Likelihood of misuse*[d] | | | |
| Low (0) | | | |
| Medium (1) | | | |
| High (2) | | | |
| **SUM** | | | |

[a] Accessibility scale: low = there are no or few barriers to accessing the dual-use item; medium = there are some barriers to accessing the item; there are many barriers, or the barrier is very high, to accessing the item.

[b] Ease of misuse scale: low = barriers for misuse are assumed to be high; medium = additional effort is required prior to harmful use; high = no or very low barriers preventing misuse.

[c] Magnitude of harm scale: low = the harm will be minor or localized; medium = the harm will be serious or over a large area; high = the harm will be severe or catastrophic, or widespread, or both severe and widespread.

[d] Likelihood of misuse scale: low = the purpose, risks and alternative means make the use unlikely; medium = the purpose, risks and alternative means make the use quite likely; high = the purpose, risks and alternative means make the use very likely.

scores for its use as a bioweapon (where it might score high on accessibility and ease of misuse, medium on magnitude of harm, and low on likelihood of misuse) than it will for bioterrorism and biocrime (where it might score medium or high on ease and likelihood of misuse but low on accessibility or magnitude, depending on the characteristics of the toxin). These scores are added together give a total between 0 and 8 corresponding to three levels of misuse potential—low (0–2), medium (3–5) and high (6–8) (figure 3.1)—for each category. An example of how this works for a specific dual-use item is shown in section 4.

This quantification step is important because practical steps in prevention of misuse will likely differ, and will have different levels of priority, depending on the threat in each case. Identification of appropriate strategies is the third pillar of the proposed toolkit.

## Pillar 3. Strategies for minimizing misuse potential

The quantification of a dual-use item's misuse potential to provide a value of 'low', 'medium' or 'high' influences the selection of measures for preventing or mitigating misuse of that item. For example, an item that has **low** misuse potential might only need continuous monitoring of the research activity to detect any change in status, such as

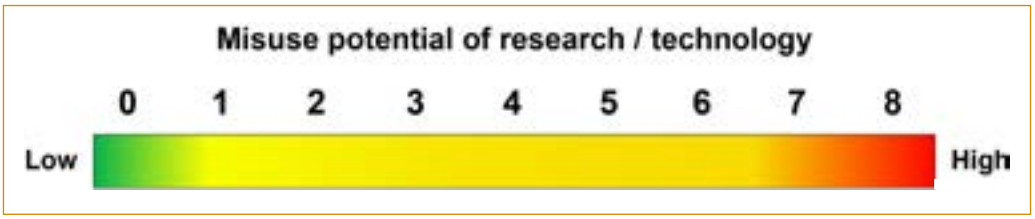


**Figure 3.1.** Numerical scale quantifying misuse potential

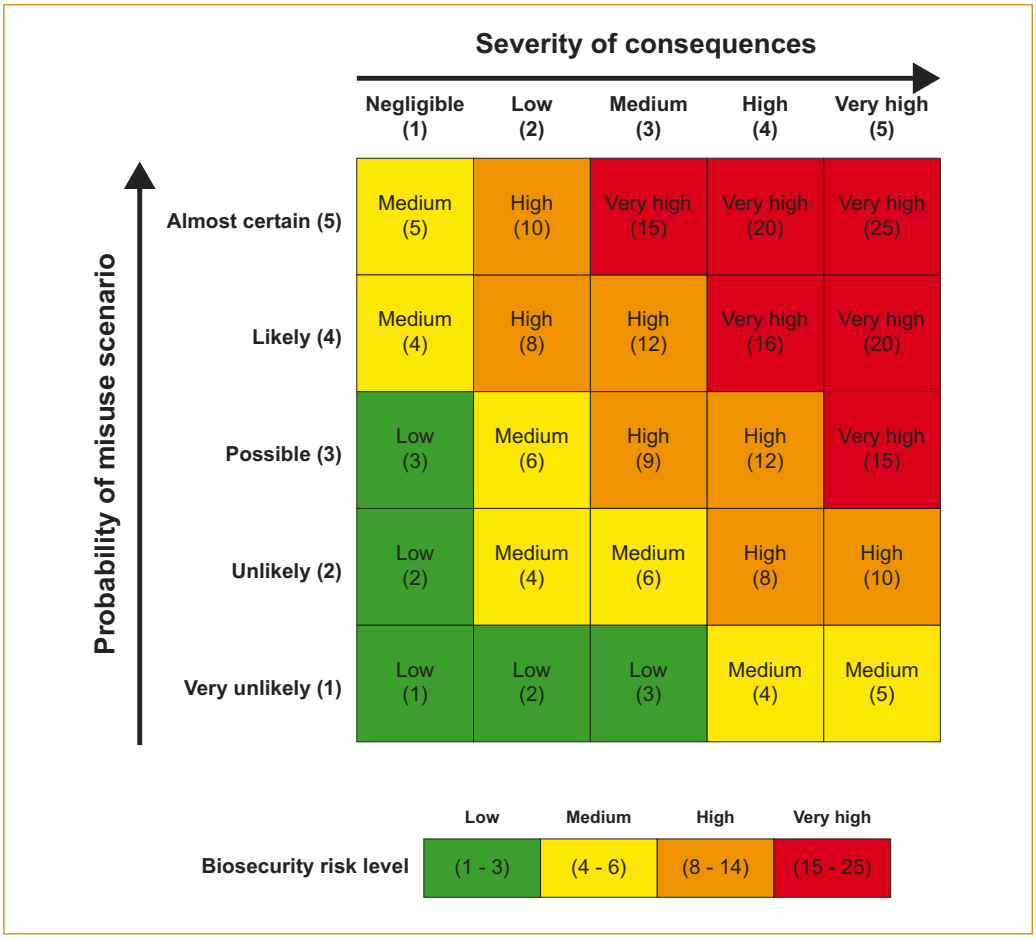


**Figure 3.2.** Probability–impact risk matrix

emerging biosecurity risks and misuse potential, as well as compliance with existing biosafety and biosecurity instructions at the institution. An item that has **medium** misuse potential might require the planned research to be reorganized, for example by using one or more of the following measures: using an alternative biological agent or experimental method that has a lower misuse potential; enhancing the biosafety and biosecurity measures around the project; communicating within the research team and the institution to enhance awareness about the identified misuse potential; and of course continuous monitoring of the research activity to detect emerging biorisks and misuse potential. And any item that has **high** misuse potential will need more stringent measures in place, such as not using the item at all—for example, by reorganizing the planned research to use a different, lower-risk item, or cancelling that part of the project using the risk item, or even, as a last resort, cancelling the planned research in entirety. If those measures are not feasible, alternative strategies for items with high misuse potential include enhancing biosafety and biosecurity measures; continuous monitoring of the research activity to detect emerging risks and misuse potential; and

**Box 3.2.** Example list of questions an individual scientist can use to initiate discussions about biosecurity risk management strategies at different levels

**Individual level**

- What are my individual responsibilities in keeping my work safe from misuse?
- How can the other individuals working on my project—e.g. scientist colleagues, research assistants, laboratory technicians—contribute in this respect

**Group level**

- Are additional or enhanced physical protection measures required at the laboratory?
- Are additional or enhanced information security measures required at the laboratory?
- Will an informal training session be required to inform co-workers within the group about the identified research risks?
- Are sufficient instruments in place for continuous biorisk monitoring within the laboratory? Do those responsible for the instruments and the monitoring work within the group or are they external?
- Which measures will the group leader take responsibility for and which will remain at the individual level?

**Institutional level**

- Are additional or enhanced physical protection measures required at the institution ?
- Is any sensitive information stored centrally or externally rather than at the laboratory? If so, are additional or enhanced information security measures required at the institution, especially?
- Does the project involve transfer of dual-use items to or from another laboratory or storage facility? If so, are additional or enhanced security measures required for such transfers?
- Will an informal training session be required to inform others at the institution about the identified research risks?
- Are sufficient instruments in place for continuous biorisk monitoring within the institution? Who is responsible for the instruments and the monitoring?
- Are there any potential duties regarding export control regulations? If so, who oversees compliance within the institution?
- Regional and national level:
- Should regulatory authorities be approached to obtain a better understanding of misuse potential from a different perspective? If so, who is best placed to make the approach?
- Should regulatory authorities provide background information about security-related questions in scientific collaborations? If so, is this information readily available now?

involving other stakeholders (e.g. regulatory authorities) to further define appropriate biorisk prevention and mitigation strategies.

However, the level of misuse potential for a project's identified risk items is not the only factor in identifying a suitable risk management strategy for the project. Two other factors are (*a*) the type and scale of victim or target the measures are aimed at protecting (discussed near the end of this section); and (*b*) priority—determining how the level of misuse potential relates to the potential consequences of the misuse, to identify which identified risk items have the highest urgency.

### *Relating likelihood of misuse to severity of consequences: the probability–impact risk matrix*

Before an individual scientist can recommend the best evidence-based risk mitigation approach to prevent their work from being misused, they should input the estimates of potential misuse and potential consequences into a probability–impact risk matrix (figure 3.2) for each misuse scenario. For example, a scenario that has low probability but high impact (i.e. severe or widespread harm such as a deadly pandemic or ecological

collapse) might need a similar level of biosecurity risk management as a scenario with higher probability but low impact. Such cases should follow the precautionary principle which aims to minimize risks and unintended consequences.

The biosecurity risk assessment matrix in figure 3.2 shows the severity of harmful consequences of misuse of research on the x-axis on a scale of 1 (negligible) to 5 (very high), and estimated probability of a given misuse scenario on the y-axis also on a scale of 1 (very unlikely) to 5 (almost certain). The 'biosecurity risk level' is the product of probability of the misuse scenario and severity of consequences. For example, a scenario that has a severity value of 2 (low) and a likelihood value of 2 (unlikely) gives a product of 4, which is a 'medium' level of biosecurity risk; but a scenario that is just as unlikely has a very high severity of 5, the product is 10, which is a 'high' level of biosecurity risk. The higher the level of biosecurity risk, the more urgent and stringent the risk mitigation strategies need to be.

### *Considering specific measures to mitigate biosecurity risks*

Once the individual scientist has estimated the level of biosecurity risk associated with their project and the urgency of implementing strategies appropriate to that level, they should then consider specific measures to protect the research from being misused. The best biosecurity risk mitigation strategies for the project will strongly depend on local requirements and circumstances. A few of the possible strategies include: physical access control; information control; data protection; biological control measures (e.g. kill-switch; auxotrophy); change of experimental procedures; and change of biological agent under study.

Even though individual scientists will not (and cannot) be responsible for implementing all of the measures, they can take responsibility for those that are within their control and initiate discussions at the group, institutional and regional/national levels. A possible list of questions the scientist can consider is shown in box 3.2. The scientist could summarize their answers to these questions so that they can take the process further in group discussions and decision making in their laboratory and institution.

### *Prevention of primary negative impacts*

The individual biosecurity risk mitigation strategy will further depend on the type and scale of victim or target of the harmful or other negative consequences of misuse of the dual-use aspect of the project—that is, whether the strategy is for protection of humans, animals or plants (level: individuals, populations), or of ecosystems (level: populations, species; biotic and abiotic factors of ecosystem).

Potential biosecurity risk mitigation measures to prevent primary negative impacts include physical protection, replacement of material or method, minimizing potential exposure, the precautionary principle, and training and education. Generally a combination of multiple measures will be needed to protect the different types and scale of potential victims or targets. That is, if the victims of the harm are humans, some measures should be designed to protect the individual humans working directly with the risk item in the laboratory, while others should be designed to prevent the item from harming humans more generally or indeed whole populations, if that is a possible consequence. The examples that follow are not intended to be an exhaustive list. Physical protection measures include confirming that required biosafety measures are both in place and effective. Examples of such measures are the use of personal protective equipment and biosafety cabinets; disinfection of work spaces; decontamination of solid and liquid waste; and prevention of uncontrolled release of hazardous biological agents and materials.

Replacement and minimization measures include replacing the biological agent, material, technology or method identified as showing a high misuse potential with variants of no or low concern, or reducing the amount of work it is used for to a minimum. For example, the scientist could consider replacing a pathogenic bacterial or viral species with a non-pathogenic species that has comparable biological features reducing the number of experiments; restricting work to specialized facilities (if not already required by law); and reducing the number of people involved in or with access to the project.

A measure that applies the precautionary principle is to avoid release of any biological agent to nature unless biological control measures have been proved to be effective and strategies for reversing unintended consequences of the release are in place.

Finally, all strategies and measures require everyone involved in the project to receive an appropriate level of training and education in the application of biosecurity risk mitigation measures.

# 4. Biosecurity risk assessment of emerging technologies

## The challenge for biosecurity risk assessment in the life sciences

The rapid growth of scientific and technical knowledge within the various subdisciplines of the life sciences and the biotechnology industry makes assessment of misuse potential even more challenging. For example, biosecurity risk management in the life sciences needs to take into consideration potential threats posed by emerging dual-use technologies.[38] Convergence between technologies such as gene editing, artificial intelligence (AI), and additive manufacturing open possibilities to generate novel biological materials not occurring in nature. Revolutionary developments (and not necessarily evolutional steps) are anticipated at exactly these disciplinary boundaries. Existing biorisk governance frameworks are thought to be inadequately adapted for the assessment of emerging technologies in the life sciences.[39]

This section provides an example of how the proposed toolkit's approach to biosecurity risk assessment could be applied to of these emerging technologies—nanobiotechnology. This case alone highlights the need for multidisciplinary work to better mitigate biorisks on a broader level that includes both biosafety and biosecurity measures.

## Nanobiotechnology example[40]

In this example, all information and analysis are provided for demonstration purposes only, based on a hypothetical misuse scenario. The users of any upcoming biosecurity risk assessment toolkit would need to perform their own analyses, estimates, quantification and strategy selection based on their scientific–technical knowledge about the particular research project, current state of art in the field of nanobiotechnology, and security-relevant context information.

Similarly, any risk levels calculated are abstract examples and do not reflect risks associated with potential misuse of nanobiotechnology. This is not an actual assessment of medical or environmental safety of nanobiotechnology applications.

### *Definition and dual-use character*

Nanobiotechnology refers to research, development and application in biotechnology involving the use of nanomaterials (size dimensions between ~1 and 100 nanometers), as well as effects at the nanoscale on biological materials. It is an emerging technology with a broad spectrum of uses in both basic and applied research, including generation of new biological agents and modification of existing biological agents. Applications can be used for both beneficial and malicious purposes.

Interestingly, this dual-use potential creates uncertainties about various possible applications that contribute to geopolitical rhetoric. For example, peaceful innovations in nanobiotechnology might be declared as irresponsible and in violation of existing international weapons ban treaties. However, the misuse potential is high: research

[38] Himmel, M., 'Emerging dual-use technologies in the life sciences: challenges and policy recommendations on export control', EU Non-Proliferation and Disarmament Paper no. 64, Sep. 2019.

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

[40] The example used in this section is based on an unpublished background briefing by Margaret E. Kosal written specifically for the research supporting the development of the toolkit outlined in this publication. See also Kosal, M. E, *Nanotechnology for Chemical and Biological Defense* (Springer Academic Publishers: New York, June 2009).

**Table 4.1.** Record of scientific–technical risk analysis of the example scenario

| Aspect under review | Toxin-loaded nanocarriers |
|---|---|
| Level / type of damage | Mass poisoning of people in the course of an attack / the toxin leads to severe damage to the nervous system |
| Mechanism of damage | Encapsulation of the toxin in nanocarriers designed for targeted drug delivery to the human body |
| Subject(s) affected | Humans who take the drug(s) containing the toxin-loaded nanocarriers |
| Extent of reversibility | No antidote or treatment available; most victims surviving the attack will recover in a couple of weeks although some may have lingering health effects |
| Evidence base | [List citations of research on] Assessment of dual-use potential of nanocarrier based on drug delivery technologies; effects of toxins |

and development in nanobiotechnology could inadvertently lead to the development of novel nanobiotechnology-enabled biological or chemical weapons.

### *Aspect under review for misuse potential*

One scenario for misuse of nanobiotechnology is a clandestine attack by a physiologically active material, such as a toxin, on a person's internal biological systems.

### *Scientific–technical analysis of an attack using a toxin-loaded nanocarrier*

The harm-causing mechanism could be encapsulation of the toxin in nanocarriers designed for targeted drug delivery to the human body. Detection of these loaded nanoparticles in biomedical samples by standard techniques might be difficult if not impossible. The harm to a person so attacked would be illness, possibly severe and possibly leading to death, depending on the toxin used. The scale of the attack would depend on the actual delivery mechanism chosen—it could be limited to a small number of people in a specific clinical trial of a new drug or it could be widespread in a common, over-the-counter drug.

This assessment assumes the worst-case scenario of a mass dissemination of nanoparticles containing a toxin for which there is no treatment, but the victims recover after a few weeks. Table 4.1 shows how this analysis might be recorded.

### *Estimation of misuse potential of toxin-loaded nanocarriers*

**Accessibility.** The high level of sophistication of nanobiotechnology means that access is assumed to be extremely difficult for anyone but state actors and experienced scientists already working in the field with full access to an equipped laboratory and relevant materials. States are the most concerning actors in the context of risks from misuse of a toxin-loaded nanocarrier for a malicious purpose, for example, as a bioweapon. However, there is also a risk of misuse, albeit less likely, of a well-resourced terrorist or criminal organization gaining access to the technology for the purposes of bioterrorism or biocrime (e.g. an attack by way of demonstration in the context of extortion).

**Ease of misuse.** Application of toxin-loaded nanocarriers requires advanced production and preparation techniques as well as a sophisticated means of delivery which are not fully developed yet. This is because the maturation level of this technology is still rather low.[41] An attacker would also need to conduct testing for harmful effects of the generated nano-devices, which is less likely to be feasible on

[41] Mitchell, M. J., Billingsley, M. M., Haley, R. M., Wechsler, M. E., Peppas, N. A., and Langer, R. (2021). Engineering precision nanoparticles for drug delivery. Nat Rev Drug Discov, 20(2):101–124.

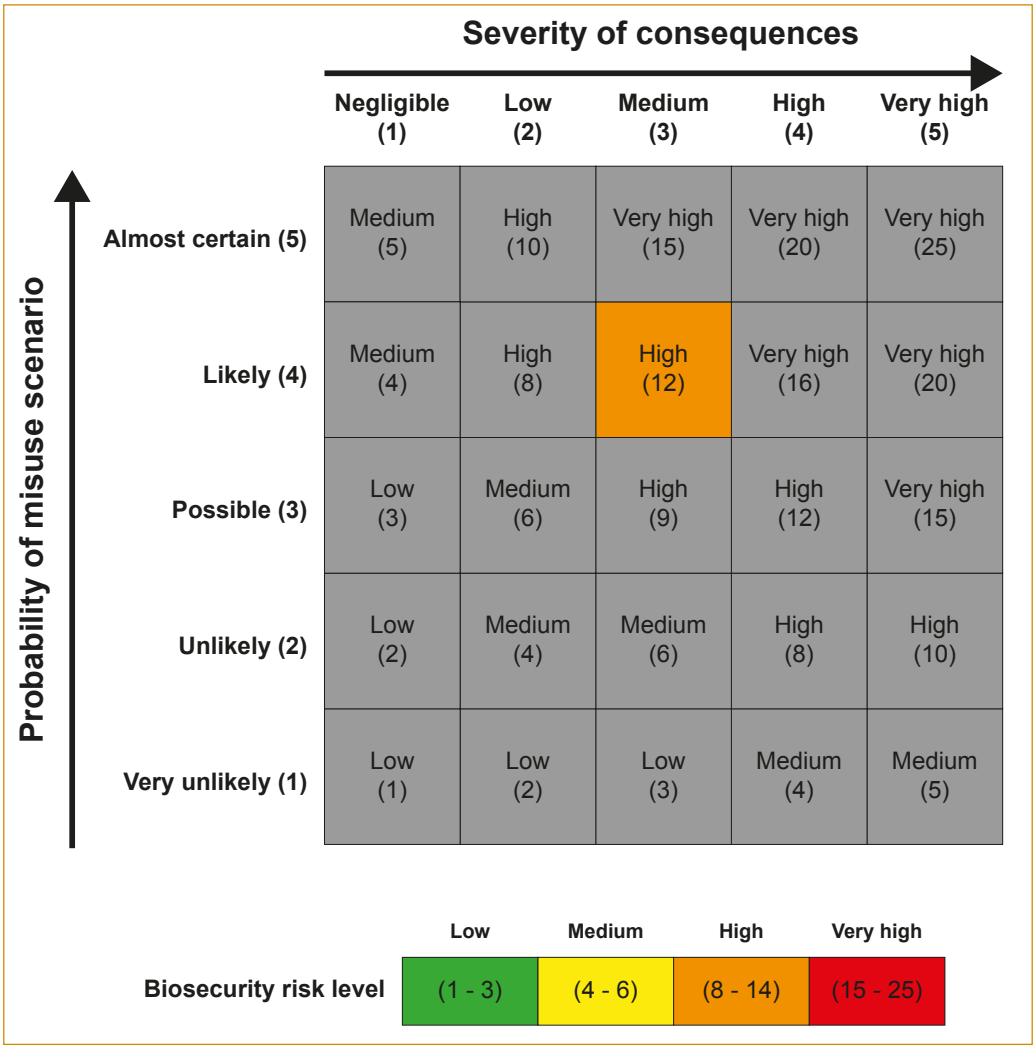


**Figure 4.1.** Example of a probability–impact matrix for estimating the biosecurity risk level in the case of misuse of toxin-loaded nanocarriers by a malicious state actor

the human test subjects required, to be sure that this novel technology will cause the intended harmful effect. Therefore, ease of misuse is assessed to be rather low for most categories of actor.

**Magnitude of harm-causing effects.** Harmful consequences of a well-prepared malicious application of toxin-loaded nanocarriers might be a high number of casualties. Despite the fact that most victims will likely recover in a few weeks, the attack could be sustained for a longer time, leading to ongoing mass hospitalizations, collapse of health systems, and widespread fear and distrust in the community. These secondary effects could lead to further negative impacts on the economy and society. The extent of the potential harm means the application has potential for misuse as a bioweapon and for bioterrorism, as well as for biocrime. Because the harm is reversible and relatively temporary, however, the severity is 'medium' rather than 'high' or 'very high'.

**Likelihood of misuse.** Currently, other biological and chemical threat agents seem to be more easily available and applicable for malicious actors. States that have the means to use the technology as a bioweapon must also be willing to breach the BWC and face international sanctions, among other consequences. Likelihood of misuse is therefore assessed to be rather low, as there are few such states. However, if the project

**Table 4.2.** Example quantification of misuse potential of toxin-loaded nanocarriers

| Risk attributes (point value) | Bioweapons | Bioterrorism | Biocrime |
|---|---|---|---|
| 1. *Accessibility* | | | |
| Difficult (0) | | | 0 |
| Limited (1) | | 1 | |
| Simple (2) | 2 | | |
| 2. *Ease of misuse* | | | |
| Low (0) | 0 | 0 | 0 |
| Medium (1) | | | |
| High (2) | | | |
| 3. *Magnitude of harm* | | | |
| Low (0) | | | |
| Medium (1) | | | 1 |
| High (2) | 2 | 2 | |
| 4. *Likelihood of misuse* | | | |
| Low (0) | | 0 | 0 |
| Medium (1) | | | |
| High (2) | 2 | | |
| **SUM** | 6 | 3 | 1 |

can be accessed and used by a malicious state that considers the potential effects outweigh any adverse consequences to itself, the likelihood of misuse is high.

An example of how the estimates for these four attributes might be quantified is shown in table 4.2. In this example, the misuse potential is quantified as low for actors intending to use the technology for biocrime, medium for actors such as bioterrorist organizations, and high for state actors willing to use it as a bioweapon.

### *Development of biosecurity risk mitigation strategies*

The analysis here focuses on risk mitigation strategies appropriate to prevent a state from using toxin-loaded nanocarriers for a malicious purpose, such as a bioweapon or state-sponsored terrorism. The overall misuse potential was estimated as medium, but for state actors the likelihood of misuse is 'high' while the severity is still 'medium'. These values (4, 3) are input into the probability–impact matrix shown in figure 4.1, to give a biosecurity risk level for this particular scenario of 'high' (12).

The above scientific–technical analysis and estimation of risk of misuse has resulted in identification of a particular scenario of misuse as having a high level of biosecurity risk. In other words, toxin-loaded nanocarriers can be understood as high-risk technology, which means that measures for preventing their misuse must be implemented immediately. The key strategies for prevention of misuse are access control and information control. The key countermeasures are developing capabilities for detection of toxin-loaded nanocarriers, and elimination or inactivation once detected.

Table 4.3 sets out some possible measures for preventing or mitigating the risk of misuse of toxin-loaded nanocarriers which could be implemented at the individual, group and institutional levels. In practice, the user of a proposed toolkit should add two additional columns designating the level of implementation for each measure (individual, group or institution) and assigning responsibilities for the implementation, based on discussions as set out under pillar 3 in section 3 above.

**Table 4.3.** Example strategies and measures for preventing or mitigating the risk of misuse of nanocarriers designed for targeted drug delivery

| Strategy | Possible measures |
|---|---|
| Access control | Restrict access to nanocarriers designed for targeted drug delivery to authorized users only.<br>Log each instance of access to a nanocarrier—including (as a minimum) the access time and date, the person's name, and the reason for the access—using a method that cannot be falsified or tampered with.<br>Review logs frequently to detect attempts at unauthorized access as well as any authorized access for an unauthorized or unnecessary purpose. |
| Information control | Classify as 'sensitive' any information about synthesis, preparation and packing of nanocarriers designed for targeted drug delivery.<br>Restrict access to sensitive information to only the working group and external collaboration partners; in both cases, only grant access to as few members of these groups as possible.<br>Log all instances of access to sensitive information—including (as a minimum) the access time and date, the person's name, and the reason for the access—using a method that cannot be falsified or tampered with, and review the logs frequently.<br>Ensure that dissemination of information via scientific conferences, publications and social media reflects the sensitivity of the information. |
| Data control | Restrict access to data that could be misused (e.g. chemical nature of the nanocarriers, precursors, intermediates). |
| Change of experimental procedures | Avoid improving loading capacities of nanocarriers for a broad range of biological components such as toxins.<br>Avoid development of uncontrollable targeting of organs/body compartments by not using methods that enhance dependence of drug delivery on a set of triggers for targeted drug delivery or release in situ. |
| Countermeasures | Develop analytical capabilities for detection of toxin-loaded nanocarriers in biomedical samples<br>Develop mechanisms for elimination or inactivation of unwanted nanocarriers.<br>Enhance dependency of nanocarriers on sophisticated method of application to the human body. |
| Change of experimental design | Change nanomaterial or method of packing to minimize risk for loading nanocarriers with toxins.<br>Modify physico-chemical properties to diminish accumulation of nanocarriers by enhanced clearance from the body. |

## 5. Next steps

The role of the individual scientist in biosecurity risk assessment is to start the process and provide the scientific–technical basis and solutions for risk management strategies. This provisional approach for a proposed toolkit has outlined one way to go about this. This approach needs, at the very least, critical reflection from practitioners working in different areas of the life sciences and in different regions of the world. Moreover, it represents only one approach to scientific–technical risk assessment, which itself constitutes only one part of a comprehensive biosecurity risk assessment. Regardless, implementing the proposed three-pillar approach on the ground will be necessary to see its applicability for selected study cases across different institutions and fields of research, and for further conceptual refinement. This field testing can also include use of historical cases, with practitioners assessing known experiments of concern based on the level of knowledge at the time the research was undertaken. Would deploying the toolkit have raised an alarm?

The focus on the proposed three pillars approach for a biosecurity risk assessment means the proposed toolkit does not address a number of other questions, which are beyond the scope of this paper. For example, in the absence of legal or other obligations, how can individual scientists be incentivized to conduct biosecurity risk assessments for their projects? What specific knowledge is needed to assess misuse potential, and is that knowledge base accessible to scientists worldwide? How can individual scientists estimate the 'likelihood of misuse' when even well-equipped intelligence services might fail to do so? Where misuse potential has been identified, what thresholds trigger either completely redesigning or stopping the research activity? And what are the legal and ethical implications if scientists differ significantly in their risk assessments of similar activities?

Assuming these questions are addressed, and the necessary development, testing and conceptual refinement work yields a practical, universal toolkit, for individual scientists to use in conducting biosecurity risk assessments, that toolkit will only go part way in ensuring life sciences research is conducted both safely and securely. It starts with the individual scientist but that scientist needs support at the group and institutional levels, which must implement the necessary administrative controls to ensure that biosafety and biosecurity is taken seriously at the institution. The level of individual activities is crossed when it comes to the prevention of secondary negative impacts on economics or society or the environment, both nationally and internationally. Biosecurity risk management strategies covering those broader scales are beyond the scope of this document but could be based on the results obtained by the risk assessment approaches provided for this proposed toolkit.

# About the author

**Dr Mirko Himmel** (Germany) is an Associate Senior Researcher within the SIPRI Armament and Disarmament research area. He works on research topics related to non-proliferation and preventive arms control of biological weapons. He is a principal scientist working in the Department for Microbiology and Biotechnology at the University of Hamburg. His teaching activities include lectures in molecular infection biology and biomedical ethics. Furthermore, he frequently provides biosecurity advice for students and researchers at the university. Dr Himmel is biochemist by training and has a long-standing work experience in basic research in the life sciences. In 2005, he started his junior postdoc career at the University of Leipzig and moved in 2009 as senior postdoc to the University Medical Centre Hamburg-Eppendorf. From 2014-2022 he was with the Centre for Science and Peace Research at the University of Hamburg. He is sharing his scientific and biosecurity expertise with governmental and non-governmental organizations.


**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