Established in 1871

Swiss Medical Weekly

Formerly: Schweizerische Medizinische Wochenschrift

An open access, online journal • www.smw.ch

Review article: Biomedical intelligence | Published 02 December 2018 | doi:10.4414/smw.2018.14688
Cite this as: Swiss Med Wkly. 2018;148:w14688

Dual use in the 21st century: emerging risks and global governance

Ienca Marcello, Vayena Effy

Health Ethics and Policy Lab, Department of Health Sciences and Technology, ETH Zurich, Switzerland

Summary

Dual use research of concern (DURC) is defined by the World Health Organization as "life sciences research that is intended for benefit, but which might easily be misapplied to do harm." Ethical and policy discussions on DURC span the past three decades. Today, however, new and emerging technologies and associated sociocultural transformations within the scientific community are reshaping the current risk scenario. This paper identifies three major trends that are likely to characterise dual use dilemmas in the near future: the diversification of dual use domains, the digitalisation of potential threats and the proliferation of actors. This analysis illustrates an increasingly heterogeneous and fragmented risk scenario, which can hardly be effectively governed top-down from a centralised authority. We propose that in order to meet the critical challenges of dual use in the 21st century, a global and distributed governance is needed. In contrast to globally binding sets of legal mechanisms administered by a central and hierarchical authority supported by leading powers, we suggest a global and decentralised governance architecture encompassing multilevel, multipolar and bottom-up strategies that can stretch across a spectrum of stakeholders and scientific domains in an agile, proactive and adaptive manner. Finally, we discuss how Switzerland can take a leading role in the promotion and development of this global governance architecture.

Keywords: *dual use*, *biomedical research*, *bioethics*, *governance*, *biohackers*, *bioterrorism*, *biosecurity*, *decentralised*, *digitalisation*, *risk management*

Introduction

The history of science and technology attests that nearly any information or technology holds the risk of being co-opted for nefarious purposes. Examples include the utilisation of nuclear reactions for the development of nuclear weapons [1] and the mailings of *Bacillus anthracis* spores to deliberately cause fatal inhalational anthrax infections for bioterroristic aims [2]. Since the late 1990s this "deviation of intent" [3] of beneficial scientific knowledge and technology has become the object of scientific investigation, ethical concern and policy intervention.

In 2004, the US National Research Council introduced the term "dual use dilemma" to demarcate ethical dilemmas related to "beneficial life sciences research whose results could be misused by those wishing to cause harm" [4]. The United States government subsequently introduced the oversight label "dual use research of concern" (DURC) and emphasised the importance of minimising the risk that beneficial research findings could be re-purposed for the development of threats to public health and national security. Today, the DURC label is often criticised by researchers because of its conceptual ambiguity and lack of analytic rigor [4]. Nonetheless, it is widely established as a regulatory framework among national and international organisations including the US National Institutes of Health (NIH) and the World Health Organization (WHO) [5].

One major conceptual controversy related to the definition of DURC pertains to the problem of intentionality. Traditional definitions of DURC, including the one provided by the WHO, encompass both intentional and accidental misuse. In contrast, recent reports for the British Royal Society and the Dutch Research Council have provided a narrower definition and distinguished "intentional misuse" from the general domain of biosecurity accidents or other activities resulting in unintended harmful consequences. Malevolent agents responsible for intentional misuse of scientific research and technology may differ in composition (individual agents vs organised groups), purpose (political, military, personal motive, etc.) and type of organisation (state vs non-state).

For over two decades the debate on dual use has focused primarily, if not entirely, on those subdivisions of the life sciences involving research on pathogens such as virology and bacteriology. In the early 2010s, dual use dilemmas sparked a heated debate in the scientific community after two research articles, published in *Science* and *Nature,* respectively [6, 7], reported the experimental creation of influenza A virus subtype H5N1, which can cause illness in humans and many other animal species. The dilemma resulted in a year-long self-imposed moratorium, during which scientists, ethicists, policy experts and international organisations debated whether research on pathogens such as avian influenza should be conducted and published [8]. This debate focused primarily on the notion of gain-of-function (GOF) [9] research, namely research capable of

Correspondence:
Marcello Ienca PhD, Health Ethics and Policy Lab, Department of Health Sciences and Technology, ETH Zurich, Auf der Mauer 17, CH-8092 Zurich, marcello.ienca[at]hest.ethz.ch

conferring a new or enhanced activity on a biological agent such as a cell or a protein, especially when this enhances "the pathogenicity or transmissibility of potential pandemic pathogens" [10]. Proponents highlighted the scientific importance of GOF experiments to demonstrate causality between genes or mutations and specific characteristics of pathogens. In contrast, other researchers have argued that certain GOF experiments, such as those involving potentially pandemic pathogens, are often low-throughput, poorly generalisable and exceptional in their level of risk, and therefore should be replaced with safer approaches [9].

In this paper, we review the common emerging features of dual use threats in the life sciences. Additionally, we outline the principles of a possible framework for global governance designed to minimise misuse risks without hampering scientific freedom and innovation. Finally, we conclude by discussing Switzerland's position in the global dual use landscape.

Dual use in the 21st century

Compared with their historical antecedents, dual use risks in the second decade of the 21st century are characterised by three main features: the diversification of dual use domains, the digitalisation of potential threats and the proliferation of actors (see fig. 1). We argue that these three features are likely to persist and even escalate in the upcoming decade.

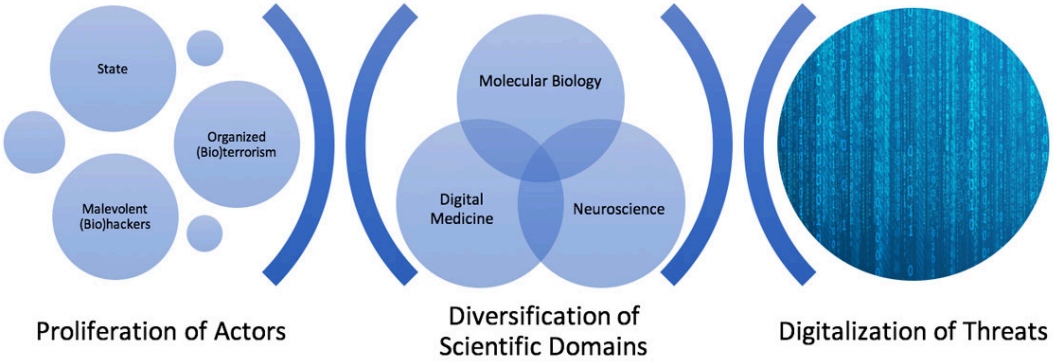
Diversification of dual use domains

Although microbiology research involving human pathogens is still at core of dual use debates, the last decade has shown that several other areas of the life sciences and medicine are sensitive to dual use dilemmas. These include, among others, synthetic biology [3, 11], neuroscience [12, 13], bioinformatics [14], implant medicine [15], and teleoperated surgery [16]. This diversification of focus originates from the fact that not only biological pathogens but many other tools, methods and scientific findings have been observed to provide informational or technical resources for the development of threats. These include methods for genome editing such as CRISP/Cas9 [3], brain-computer interfaces [17], medical implants [15], and computer code [14]. The proliferation of dual use risks across multiple scientific and healthcare domains jeopardises regulatory frameworks and harm-minimisation measures.

At least three main technological trends appear to be particularly exposed to dual use risks in the coming years: gene editing via CRISPR/Cas9, biomedical robotics and medical implants. CRISPR/Cas9 is a relatively simple technology for editing genomes which allows genes within organisms to be effectively and specifically changed. *In-vitro* and animal studies have shown that this technology can potentially correct genetic disorders in humans, such as cystic fibrosis and Fanconi anaemia [18]. In addition, it can be used to enable gene drives that reprogramme mosquito genomes with the aim of controlling –possibly eliminating – the spread of infectious diseases such as malaria [19]. However, CRISPR/Cas9 can be misused for nefarious purposes such as producing pathogenic bioagents that pose threats to public safety [3]. These include enhanced neurotoxins and infectious agents [20]. Due to the relative performative simplicity of CRISPR/Cas9 programming [21] and the estimated velocity of propagation of contagious airborne pathogens in the current interconnected world [22], this technique might result in pandemics and mass destruction should it fall into the wrong hands. This risk has been emphasised by a global threat assessment released in 2016 by James Clapper, the former US Director of National Intelligence, which placed CRISPR and other genome editing techniques among six threats listed in the section on weapons of mass destruction, alongside North Korean nuclear tests and Syrian chemical weapons.

Unlike gene editing technology, biomedical robotics is less likely to result in exponential propagation and global destruction. However, the dual use potential of this technology relies in its widespread application in military settings. Wearable robotic machines such as power exoskeletons are being increasingly used as an assistive technology for improving quality of life and partially restoring motor functions in patients suffering from traumatic injury or neuromuscular disorders [23]. In addition, they can be used to ease or enhance the work of professional caregivers [24]. At the same time, powered exoskeletons are being increasingly used in the military setting to reduce fatigue in

Figure 1: The evolving dual use scenario in the 21st century.



operating war-fighters, increase productivity, and enhance activities such as loading/unloading supplies, running or climbing [25]. The widespread and hard-to-reverse availability of biomedical robotic applications in the military sector raises complex ethical dilemmas for biomedical researchers active in this domain, given the high probability that their research findings will be repurposed for non-civilian aims.

Finally, medical implants and other digital medical devices may become targets of intent-deviating misuse by malevolent actors. The prodromal signs of this trend are already observable. In August 2017, the US Food and Drug Administration (FDA) issued a safety communication regarding potential cybersecurity vulnerabilities of several widely used cardiac pacemakers. These vulnerabilities included the risk that adversarial parties could intentionally misuse the device to drain its battery or insert malicious programming commands into the device. Given that patients with arrhythmia and heart failure depend on cardiac pacemakers, these vulnerabilities could result in severe harm to the affected patient [15]. Furthermore, since the devices at risk were used by over 450,000 patients, cybersecurity concerns arise not only in terms of severity but also amplitude. Similar vulnerabilities have been identified also in drug-infusion pumps [26], brain implants such as deep brain stimulation [27] and noninvasive brain-computer interfaces (BCIs) [17]. It is worth considering that harmful misuse of medical implants does not necessarily require computationally sophisticated methods for hijacking the full operational functions of the device. Rudimentary attacks that can disrupt the device's energy supply or cause battery drain are sufficient to cause significant harm to the victim [17].

Digitalisation of potential threats

As the hacking of medical implants attests, malicious software or other malevolent exploitation of computers can result in significant harm to life science research, healthcare institutions and individual patients. This risk scenario is enabled by the digitalisation of the life sciences and the increasing pervasiveness of computing tools in biomedicine research and clinical medicine. In 2016, a computer code originally developed by the US National Security Agency (NSA) was repurposed to perform cyberattacks against various industry actors including the pharmaceutical company Merck. In the same year, the perpetrators of the large-scale WannaCry ransomware attack used data encryption techniques to deny access to patient data across various healthcare institutions of the UK National Health Services and demanded ransoms to be paid in cryptocurrencies, hence selectively turning the dual use potential of cryptography and distributed ledger computing against healthcare services.

Cyberweapons can be used not only to sabotage biomedical research and capture biomedical data, but also to create the tools and infrastructures for biological warfare purposes. State and non-state actors can use advances in bioinformatics to enhance the magnitude and proliferation of biological weapons. As Microsoft co-founder Bill Gates stated during the Munich Security Conference 2017, "the next epidemic has a good chance of originating on a computer screen" [28]. The combination of malicious programming and synthetic biology expands the bandwidth and complexity of this risk scenario. As Gates himself has argued in a subsequent perspective article in the *New England Journal of Medicine*, "every year, advances in science make it easier for somebody to create a biologic weapon of mass destruction" [22]. Advances in artificial intelligence (AI) could aggravate the bandwidth and complexity of this global risk landscape. In fact, AI techniques could increase the speed, precision and disruption of both cyber-attacks and responses, and ultimately lead to a cyber arms race [29]. The use of cyberweapons against patients, hospitals and research institutions can be seen as the digital counterpart of using highly contagious and pathogenic bioweapons, since both threat models are characterised by fast propagation, difficult prevention and high potential for harm.

It is important to consider that, while the digitalisation of the biosciences and medicine is opening new opportunities for offence, it is thereby also producing new tools for deterrence and prevention. Examples include the use of social media to track and measure current activity of contagious disease [30], retroactively predict disease outbreaks [31] and promptly notify patients who are victim of disasters [32], as well as the use of web search signals to detect neurodegenerative disorders [33].

Proliferation of actors

Following increasing internet penetration, open access, open development and the broader trend of democratisation of science, scientific-technological knowledge is becoming more evenly distributed and fairly accessible across societies. These trends have undoubted scientific (e.g., insightful findings emerging from citizen science projects [34, 35]), social (e.g., increase in scientific literacy [35, 36]) and ethical [37] benefit, but they also increase the probability *ceteris paribus* that people with malicious intentions might get their hands on such scientific-technological knowledge. Participant-led biomedical research studies such as those initiated by online patient communities, such as PatientsLikeMe and uBiome, have raised ethical concern given their elusiveness to conventional ethical oversight such as review by an institutional review board [38]. In parallel, do-it-yourself (DIY) biology and biohacking communities represent a growing socioscientific movement in which individuals or groups actively engage in scientific research in extra-academic settings and often in absence of formal scientific training [39, 40]. DIY biologists and neuroscientists often operate in unmonitored garage laboratories through self-experimentation and by open-source equipment such as recreated polymerase chain-reaction (PCR) machines. A frequent feature of DIY research is self-experimentation: in the absence of an available patient population and without certified safety standards, biohackers often conduct experiments on themselves. Reported self-experiments include self-injection with the gene-editing tools [41] and self-administration of transcranial direct current stimulation [42, 43].

The unmonitored, decentralised and noninstitutional nature of biohacking research has raised institutional concern. Since 2010, the US Federal Bureau of Investigation (FBI) has begun sending representatives to DIY biology conferences [44] and has collaborated with the American Asso-

ciation for the Advancement of Science's National Science Advisory Board for Biosecurity to convene meetings on biosecurity and risk management. Other countries are taking more repressive regulatory approaches. In 2017, the German Federal Office of Consumer Protection and Food Safety, an agency of the German Government, issued a statement warning that whoever practices genetic engineering outside of a licensed facility would be punished with a fine of €50,000 or up to 3 years in prison. The statement was based on existing federal regulation, in particular the "Gesetz zur Regelung der Gentechnik (GenTG)", a 1990 regulation on genetic engineering that prohibits unlicensed experiments. This regulation has been perceived by many as a crackdown on DIY research. In fact, although obtaining a license is not impossible for biohackers, it may be difficult for a DIY experimenter to fully comply with GenTG. Although taking a position in the regulatory debate over DIY biology is beyond the scope of this paper, it is important to consider that the increasing number of DIY experiments will cause a fragmentation of actors in the dual use landscape. It should be noted that several DIY and bio-hacking communities have produced their own standards and codes of practice; however whether and how these codes are enforceable remains to be seen. As DIY biology grows in number and variety, risk-assessment strategies should have on the radar not only institutions, organised groups (including terroristic groups) and other state or non-state actors, but also isolated individuals who could conceivably do harm if sufficiently skilled and motivated.

Given the substantial heterogeneity of the misuse risks described above, one-size-fits-all solutions are unlikely to be efficacious and traditional regulatory mechanisms might lack the necessary bandwidth, agility and adaptiveness for guaranteeing effective oversight.

A double-edged sword

Dual use problems are usually portrayed as dilemmas since they involve a regulatory decision to be made between *prima facie* equally undesirable alternatives. For example, the influenza A/H5N1 case involved an editorial choice between the following alternatives: (i) publishing the manuscripts and thereby releasing information that could be potentially used by malevolent agents to cause human illness; (ii) declining publication and thereby censoring the diffusion of scientific knowledge. This dilemma entails a conflict between different normative principles such as scientific freedom and transparency on the one hand, and the promotion of public safety and security on the other hand. The DIY examples entail a similar conflict between public safety and security and the human right to science [45] or even to citizen science [37].

The task of adequate governance is to address the complexity of the problem by identifying (and promoting) a preferable, or at least, less undesirable course of action. This requires a proactive risk-benefit analysis, which, ideally, should be conducted prior to commencing DURC projects. However, authors have observed that risk-benefit assessments, even though very important, are difficult to perform in light of the high uncertainty that characterises values and variables before the actual research is conducted [4]. This methodological quandary is known as the Collingridge dilemma and it involves a double-blind problem that is a function of two conflicting constrains: (i) the impact of a technology cannot be easily predicted until the technology is extensively developed and widely used; (ii) controlling or modifying a technology via regulation is more difficult when the technology has become socially entrenched. To aggravate the problem, risk-benefit evaluations based on proxy information such as practical use and history might be unsatisfactory because they risk penalising basic research with little short-term application (whose direct social benefits are difficult to quantify) [46] and might neglect the evolution of methods and safeguards over time. Finally, the proliferation of dual use issues across multiple scientific domains exacerbates the uncertainty of risk-benefit analyses.

Global governance

Given the diversification of dual use domains, the digitalisation of potential threats and the proliferation of actors, governance models are increasingly required to expand their bandwidth, agility and adaptiveness for guaranteeing effective oversight. In light of these challenges, DURC dilemmas in the 21st century will require enhanced governance frameworks. In the following, we sketch some salient features which, in our view, should characterize such framework. These are global bandwidth, multilevel and multipolar organisation, proactivity and adaptivity. We suggest that these normative principles could help researchers and policy makers establish an agenda for DURC governance in the next decade. It is beyond the scope of this review to discuss how these principles can be effectively enforced under national and international law, or how the resulting governance strategies can (and should) be implemented. These are important areas for further deliberation and research.

First of all, effective governance for dual use research and technology in the 21st century requires a global governance architecture. The reason for this stems from the fact that the diversification of potential threats and proliferation of actors make dual use risks elusive or even immune to centralised governance mechanisms. As the number of domains and potential actors multiplies and fragments, it becomes increasingly unlikely – and possibly counterproductive – to concentrate oversight efforts under a single regulatory authority. Additionally, given the inherent heterogeneity of dual use threats across different domains (e.g., synthetic biology vs medical implants) and actors (e.g., individual malevolent biohacker vs national government agencies), it is improbable that effective governance can be delivered through the same one-fits-all procedure, set of norms or regulation.

In contrast, a global governance architecture should encompass an "overarching system of public governance and private institutions, principles, norms, regulations, decision-making procedures and organizations" [47] that are applicable at various levels of policy making. As observed by other authors [47], a global governance architecture is characterised by both vertical and horizontal directionality. Vertical directionality entails multilevel governance, i.e., governance executed simultaneously at the subnational (e.g., research institution or organisation), national (state), international (e.g., United Nations) and supranational level. Horizontal directionality entails multipolar

policy structures of both state and non-state bodies. In such a decentralised architecture, guidelines and policies are developed at "multiple points in the matrix" and require "interlinkages between the various layers and poles of authority and practice" [14]. This multilevel and multipolar architecture is likely to be easier to implement and better suited to meet current dual use challenges than a centrally administered authority backed up by national powers. Additionally, it is going to be less affected by centralising political forces and national influence. Finally, it is better suited to empower researchers and promote bottom-up initiatives for responsible innovation.

At the subnational level, governance mechanisms should be aimed at developing incentives and easy-to-follow pathways (including ethical and professional guidelines) for legitimate research, while controlling the export of illegitimate (e.g., weaponised) components. These mechanisms should have a threefold function: (i) preventing the criminalisation of well-intentioned researchers using potentially misusable agents (e.g., biological pathogens and malware); (ii) promoting the value of dual use-conscious research as a scientific merit; and (iii) providing researchers (including nonprofessional researchers and biohackers) with simple and unambiguous codes of conduct to comply with. Export controls developed in the context of cyberweapons [14] could offer a solid basis also for dual use research involving bioweapons or other threats. This subnational governance can be implemented in a coordinated way by a variety of governance bodies including ethics review committees, advisory boards, regional funding agencies and single research institutions.

It is worth noting, however, that biohackers, security hackers, DIY experimenters and other individuals who conduct their research activities outside traditional institutions usually do not submit their work to any of the afore-listed bodies and are typically not required to comply with their guidelines. Given the proliferation of actors and the consequent fragmentation of the risk scenario, several biosecurity-sensitive activities are likely to slip under the radar of traditional oversight mechanisms. Strict regulatory approaches that prohibit biosecurity-sensitive research conducted outside of licensed facilities (as in the German GenTG*)* might increase overall security, but are also likely to thereby infringe upon the freedom of research of noninstitutional actors. This might threaten the very existence of citizen-science initiatives and deter well-intentioned hackers and DIY researchers. One approach to better balance security and freedom might be replacing regulations based on where the research is conducted (licensed vs unlicensed facilities) with norms based on the degree of transparency of the research. For example, noninstitutional researchers may be legally required to register their research activities on a free and publicly available online registry. In such a registry, they could provide data elements related to their project that facilitate disclosure and anticipate possible risks of their work. This would allow authorities to better monitor noninstitutional research activities and help DIY researchers comply with safety and security guidelines. Of course, such a registry would not eliminate malevolent DIY researchers, but could make it easier for law enforcement to differentiate them from benevolent researchers, isolate them, and enforce penalties against them. For example, fines can be imposed for individuals who are found in possession of certain biohacking equipment (e.g., CO_2 incubators or DIY PCR machines) in absence of a register entry.

National regulation could harmonise subnational governance mechanisms and implement them at a higher level of governance, particularly at the level of national funding agencies such as the Swiss National Science Foundation (SNF). Among other mechanisms, national authorities could include compliance with specific codes of conduct as a requirement for funding applications, hence making sure that safeguards against misuse are considered early on in the research design phase. For example, authors have argued that a "biosecurity section" could be incorporated into the standard templates of research project submissions to national funding agencies in a similar manner to other requirements such disclosure of conflict of interest and authorship declaration [48]. A step in this direction has been taken in the United Kingdom, where several national agencies such as the Biotechnology and Biological Sciences Research Council (BBSRC), the Medical Research Council (MRC), and the Wellcome Trust include this type of requirement. At the international and supranational level, the European Union's funding guide for dual use research offers practical orientation to researchers in dual-use-sensitive areas, helps them navigate the legislative vacuum and provides normative suggestions. Such biosecurity sections should be mindful of the diversification of domains and digitalisation of potential threats, and require researchers to disclose not only traditional biosecurity risks (e.g., those related to harmful biological or biochemical substances), but also emerging threats resulting from the datafication and digitalisation of the life sciences. As the cyberweapon examples show, the increasing dependence of several areas of the life sciences on computing tools and methods determines that such areas are more likely to be exposed to the typical vulnerabilities and risks of computer systems and networks. To mitigate this problem, researchers may be required to disclose during the peer-review process any possible negative societal consequences of their work, including those at the algorithmic level. This proposal has already been advocated by the Future of Computing Academy (FCA), an initiative created by the Association for Computing Machinery (ACM), the world's largest computing society (see Nature News Q&A: https://www.nature.com/articles/d41586-018-05791-w [last accessed 30 August 2018]).

When implementing governance strategies, national and international regulators should avoid both over- and under-regulation. Overregulation could make compliance too hard to achieve for researchers, hence ultimately undermine the effectiveness of regulation altogether. Under-regulation could, in contrast, cause decisional uncertainty among well-intentioned researchers and undermine deterrence against malevolent actors.

In addition, regulators should be mindful of what has been called the "circular dynamics of dual use" [12], namely the fact that biomedical technologies that have been re-proposed for military aims can subsequently spill over into the biomedical domain through enhanced beneficial applications. An example of this phenomenon is the re-proposing for military aims of biomedical technologies such as elec-

troencephalography and wearable robotics, which then returned to the biomedical domain through more reliable and better performing applications [12]. Too strict export controls and inflexible regulation (e.g., global bans) risk interrupting this circular dynamic and prevent the benefits of defence-related research from returning to the biomedical domain. Furthermore, over-regulation could neglect the fact that dual use research can be used not only for offence but also for defensive aims. As the hackers' motto "sometimes you have to demo a threat to spark a solution" (usually attributed to Barnaby Jack) goes, testing the resistance of security standards can have constructive consequences.

Breaching biosecurity defences can be done for nonmalicious reasons, similarly to the way in which ethical hackers exploit the weaknesses of computer systems and networks to anticipate threats through penetration tests and promptly fix them before malevolent hackers (usually called "black hats") could exploit those same weaknesses maliciously. Recognising this constructive feature of dual use research will require a proactive shift in dual use governance. Focusing exclusively on preventing the co-option of beneficial knowledge and technology for malevolent aims is insufficient. Adequate governance mechanisms should also exploit the potential of dual-use-sensitive research for social good. For example, distributed ledger computing, the same technology that was used to demand untraceable ransom payments from healthcare institutions during the WannaCry breach, could be used to implement decentralised global governance across multiple actors.

When switching from reactivity to proactivity, focus on prevention is paramount. Scientific and technological innovation should anticipate future dual use risks and develop preventive strategies that mitigate the magnitude, duration and severity of threats. As observers have noted, concerns about misuse of bioagents through genetic engineering and weaponisation have not yet resulted in global preventative measures against the risk of pandemics [22]. The non-negligible probability of a large and lethal modern-day pandemic should trigger a "coordinated global approach" consisting of better tools, early detection and global response systems [22]. Developing such preventative measures, however, is not without cost. Therefore, increased funding will be required. A positive step in this direction is the recently established Coalition for Epidemic Preparedness Innovations (CEPI), an alliance working to prevent epidemics. Launched at the World Economic Forum 2017 in Davos, CEPI has received an initial investment of $460 million from the governments of Germany, Japan and Norway, the Bill and Melinda Gates Foundation, and the Wellcome Trust.

Finally, following the diversification of dual use domains, it will be important to develop domain-specific frameworks that can adaptively inflect the general global governance architecture to the specific problems, technologies, methods and actors of each specific research community. As in any decentralised infrastructure, each node of the matrix (e.g., each research community) has a responsibility to anticipate the dual use challenges that emerge from their domain-specific tools, methods and operational context. In addition, each community has a professional obligation to raise awareness of those dual use challenges among their peers. For example, researchers have argued in favour of adapting the general biosecurity framework of the life sciences to the specific challenges of neuroscience such as the sensitive nature of brain-related data, their correlation with mental information (e.g., personal preferences) and the reportedly suboptimal awareness of dual use issues among neuroscientists [49]. This sharing of responsibility across various scientific communities is a key element of a bottom-up and nonhierarchical approach to governance.

The situation in Switzerland

Given its self-imposed and permanent neutrality policy, Switzerland offers an interesting angle from which to look at dual use dilemmas. A recent study has qualitatively investigated the views and perspectives of Swiss life scientists on the regulation of DURC [48]. These study results indicate that, unlike researchers from other countries [50, 51], Swiss scientists are generally aware of the dual use problem. However, results show that they often fail at self-reflectively identifying dual use aspects related to their own work. From a regulatory perspective, Swiss researchers widely consider freedom of research a non-negotiable value, but generally favour regulation of DURC, especially via external advisory boards [48].

This study also provided a set of recommendations for researchers and policy bodies with a threefold aim: raising awareness on DURC in the life sciences, improving risk-assessment among individual scientists, and identifying preventative strategies. These strategies include (i) the creation of a solid and generalisable theoretical framework on dual use research, (ii) the upgrade of current educational curricula in the life sciences with the aim of including or expanding bioethics and biosecurity training, and (iii) discussing at the policy level the calibrated use of regulatory interventions aimed at maximising biosecurity without thereby hampering freedom of research. In implementing such strategies, the authors recommended a cooperative effort involving scientists, ethicists, security experts and regulatory agencies on an equal footing.

Some of these recommendations have gained consensus within the Swiss research community. In 2017, the Forum for Genetic Research of the Swiss Academy of Sciences (SCNAT) released a discussion document titled "Misuse Potential and Biosecurity in Life Sciences Research." The document was developed as a result of a series of workshops with scientists from Swiss academic institutions and has a twofold aim: creating a discussion basis for scientists on how to address dual use dilemmas in biological research, and reinforcing life scientists' commitment to responsible research. The document also outlines six major issues that require paramount attention when designing, conducting or communicating dual-use-sensitive research. These are: being aware of the inherent misuse potential of life science research, developing tools and methods to assess such misuse potential, designing safe and secure research strategies, treating unexpected findings carefully, communicating results responsibly, and fostering effective educational and preventive strategies.

These developments suggest that Switzerland, given its political neutrality, established tradition in security policy research and higher awareness within its scientific community, could be well-positioned to take a leading role in

promoting a global governance of dual use research in the coming decades.

Financial disclosure
This work was supported by the Swiss Academy of Medical Sciences under award Käthe-Zingg-Schwichtenberg-Fonds (KZS) 20/17 and by the Swiss National Science Foundation under awards 407540_167223 and PP00P3_157556.

Potential competing interests
No potential conflict of interest relevant to this article was reported.

References

1 Badash L. Scientists and the development of nuclear weapons: from fission to the Limited Test Ban Treaty, 1939-1963. London: Humanities Press Intl; 1995.
2 Guarner J, Jernigan JA, Shieh W-J, Tatti K, Flannagan LM, Stephens DS, et al.; Inhalational Anthrax Pathology Working Group. Pathology and pathogenesis of bioterrorism-related inhalational anthrax. Am J Pathol. 2003;163(2):701–9. doi: http://dx.doi.org/10.1016/S0002-9440(10)63697-8. PubMed.
3 DiEuliis D, Giordano J. Gene editing using CRISPR/Cas9: implications for dual-use and biosecurity. Protein Cell. 2018;9(3):239–40. doi: http://dx.doi.org/10.1007/s13238-017-0493-4. PubMed.
4 Imperiale MJ, Casadevall A. A new synthesis for dual use research of concern. PLoS Med. 2015;12(4):. doi: http://dx.doi.org/10.1371/journal.pmed.1001813. PubMed.
5 WHO. Report of the WHO Informal Consultation on Dual Use Research of Concern. Geneva, Switzerland World Health Organization; 2013.
6 Imai M, Watanabe T, Hatta M, Das SC, Ozawa M, Shinya K, et al. Experimental adaptation of an influenza H5 HA confers respiratory droplet transmission to a reassortant H5 HA/H1N1 virus in ferrets. Nature. 2012;486(7403):420–8. doi: http://dx.doi.org/10.1038/nature10831. PubMed.
7 Herfst S, Schrauwen EJ, Linster M, Chutinimitkul S, de Wit E, Munster VJ, et al. Airborne transmission of influenza A/H5N1 virus between ferrets. Science. 2012;336(6088):1534–41. doi: http://dx.doi.org/10.1126/science.1213362. PubMed.
8 Casadevall A, Shenk T. Mammalian-transmissible H5N1 virus: containment level and case fatality ratio. MBio. 2012;3(2):. doi: http://dx.doi.org/10.1128/mBio.00054-12. PubMed.
9 Duprex WP, Fouchier RAM, Imperiale MJ, Lipsitch M, Relman DA. Gain-of-function experiments: time for a real debate. Nat Rev Microbiol. 2015;13(1):58–64. doi: http://dx.doi.org/10.1038/nrmicro3405. PubMed.
10 Dual Use Research of Concern. National Institutes of Health, 2017. at https://osp.od.nih.gov/biotechnology/dual-use-research-of-concern/.)
11 Heidari Feidt R, Ienca M, Elger BS, Folcher M. Synthetic Biology and the Translational Imperative. Sci Eng Ethics. 2017. dio:. http://dx.doi.org/10.1007/s11948-017-0011-3. PubMed.
12 Ienca M, Jotterand F, Elger BS. From Healthcare to Warfare and Reverse: How Should We Regulate Dual-Use Neurotechnology? Neuron. 2018;97(2):269–74. doi: http://dx.doi.org/10.1016/j.neuron.2017.12.017. PubMed.
13 Marchant G, Gulley L. National security neuroscience and the reverse dual-use dilemma. AJOB Neurosci. 2010;1(2):20–2. doi: http://dx.doi.org/10.1080/21507741003699348.
14 Stevens T. Cyberweapons: an emerging global governance architecture. Palgrave Communications. 2017;3:16102. doi: http://dx.doi.org/10.1057/palcomms.2016.102.
15 Kramer DB, Fu K. Cybersecurity Concerns and Medical Devices: Lessons From a Pacemaker Advisory. JAMA. 2017;318(21):2077–8. doi: http://dx.doi.org/10.1001/jama.2017.15692. PubMed.
16 Bonaci T, Yan J, Herron J, Kohno T, Chizeck HJ. Experimental analysis of denial-of-service attacks on teleoperated robotic systems. Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems; 2015: ACM. p. 11-20.
17 Ienca M, Haselager P. Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity. Ethics Inf Technol. 2016;18(2):117–29. doi: http://dx.doi.org/10.1007/s10676-016-9398-9.
18 Barrangou R, Doudna JA. Applications of CRISPR technologies in research and beyond. Nat Biotechnol. 2016;34(9):933–41. doi: http://dx.doi.org/10.1038/nbt.3659. PubMed.
19 Oye KA, Esvelt K, Appleton E, Catteruccia F, Church G, Kuiken T, et al. Regulating gene drives. Science. 2014;345(6197):626–8. doi: http://dx.doi.org/10.1126/science.1254287. PubMed.
20 DiEuliis D, Giordano J. Why gene editors like CRISPR/Cas may be a game-changer for neuroweapons. Health Secur. 2017;15(3):296–302. doi: http://dx.doi.org/10.1089/hs.2016.0120. PubMed.
21 Doudna JA, Charpentier E. The new frontier of genome engineering with CRISPR-Cas9. Science. 2014;346(6213):. doi: http://dx.doi.org/10.1126/science.1258096. PubMed.
22 Gates B. Innovation for Pandemics. N Engl J Med. 2018;378(22):2057–60. doi: http://dx.doi.org/10.1056/NEJMp1806283. PubMed.
23 Riener R. The Cybathlon promotes the development of assistive technology for people with physical disabilities. J Neuroeng Rehabil. 2016;13(1):49. doi: http://dx.doi.org/10.1186/s12984-016-0157-2. PubMed.
24 Monnet J, Saito Y, Onishi K. Exoskeleton robot using hydraulic Bilateral Servo Actuator system for non-ambulatory person's transfer. IASTED International Conference on Biomedical Engineering, Biomed; 2011.
25 Kopp C. Exoskeletons for warriors of the future. Defence Today. 2011;9:38–40.
26 Pycroft L, Aziz TZ. Security of implantable medical devices with wireless connections: the dangers of cyber-attacks. Taylor & Francis; 2018.
27 Pycroft L, Boccard SG, Owen SLF, Stein JF, Fitzgerald JJ, Green AL, et al. Brainjacking: implant security issues in invasive neuromodulation. World Neurosurg. 2016;92:454–62. doi: http://dx.doi.org/10.1016/j.wneu.2016.05.010. PubMed.
28 Selk A. Bill Gates: Bioterrorism could kill more than nuclear war—but no one is ready to deal with it. The Washington Post February 18, 2017.
29 Taddeo M, Floridi L. Regulate artificial intelligence to avert cyber arms race. Nature. 2018;556(7701):296–8. doi: http://dx.doi.org/10.1038/d41586-018-04602-6. PubMed.
30 Signorini A, Segre AM, Polgreen PM. The use of Twitter to track levels of disease activity and public concern in the U.S. during the influenza A H1N1 pandemic. PLoS One. 2011;6(5):. doi: http://dx.doi.org/10.1371/journal.pone.0019467. PubMed.
31 Szomszor M, Kostkova P, de Quincey E. #Swineflu: Twitter Predicts Swine Flu Outbreak in 2009. In: Szomszor M, Kostkova P, editors. Electronic Healthcare 2012. Berlin, Heidelberg: Springer Berlin Heidelberg; 2012. p. 18–26.
32 Tamura Y, Fukuda K. Earthquake in Japan. Lancet. 2011;377(9778):1652. doi: http://dx.doi.org/10.1016/S0140-6736(11)60672-7. PubMed.
33 White RW, Doraiswamy PM, Horvitz E. Detecting neurodegenerative disorders from web search signals. NPJ Digital Medicine. 2018;1(1):8. doi: http://dx.doi.org/10.1038/s41746-018-0016-6.
34 Nali C, Lorenzini G. Air quality survey carried out by schoolchildren: an innovative tool for urban planning. Environ Monit Assess. 2007;131(1-3):201–10. doi: http://dx.doi.org/10.1007/s10661-006-9468-2. PubMed.
35 Sultana P, Abeyasekera S. Effectiveness of participatory planning for community management of fisheries in Bangladesh. J Environ Manage. 2008;86(1):201–13. doi: http://dx.doi.org/10.1016/j.jenvman.2006.12.027. PubMed.
36 Bonney R, Cooper CB, Dickinson J, Kelling S, Phillips T, Rosenberg KV, et al. Citizen science: a developing tool for expanding science knowledge and scientific literacy. Bioscience. 2009;59(11):977–84. doi: http://dx.doi.org/10.1525/bio.2009.59.11.9.
37 Vayena E, Tasioulas J. "We the Scientists": a Human Right to Citizen Science. Philos Technol. 2015;28(3):479–85. doi: http://dx.doi.org/10.1007/s13347-015-0204-0.
38 Vayena E, Tasioulas J. The ethics of participant-led biomedical research. Nat Biotechnol. 2013;31(9):786–7. doi: http://dx.doi.org/10.1038/nbt.2692. PubMed.
39 Penders B. Biotechnology: DIY biology. Nature. 2011;472(7342):167. doi: http://dx.doi.org/10.1038/472167a.
40 Keulartz J, van den Belt H. DIY-Bio - economic, epistemological and ethical implications and ambivalences. Life Sci Soc Policy. 2016;12(1):7. doi: http://dx.doi.org/10.1186/s40504-016-0039-1. PubMed.
41 Smalley E. FDA warns public of dangers of DIY gene therapy. Nat Biotechnol. 2018;36(2):119–20. doi: http://dx.doi.org/10.1038/nbt0218-119. PubMed.
42 Jwa A. Early adopters of the magical thinking cap: a study on do-it-yourself (DIY) transcranial direct current stimulation (tDCS) user community. J Law Biosci. 2015;2(2):292–335. doi: http://dx.doi.org/10.1093/jlb/lsv017. PubMed.
43 Wurzman R, Hamilton RH, Pascual-Leone A, Fox MD. An open letter concerning do-it-yourself users of transcranial direct current stimulation. Ann Neurol. 2016;80(1):1–4. doi: http://dx.doi.org/10.1002/ana.24689. PubMed.

44 Ledford H. Garage biotech: Life hackers. Nature. 2010;467(7316):650–2. doi: http://dx.doi.org/10.1038/467650a. PubMed.

45 Chapman A, Wyndham J. A human right to science. Science. 2013;340(6138):1291. doi: http://dx.doi.org/10.1126/science.1233319. PubMed.

46 Casadevall A, Fang FC. Important science--it's all about the SPIN. Infect Immun. 2009;77(10):4177–80. doi: http://dx.doi.org/10.1128/IAI.00757-09. PubMed.

47 Biermann F, Pattberg P, Van Asselt H, Zelli F. The fragmentation of global governance architectures: A framework for analysis. Glob Environ Polit. 2009;9(4):14–40. doi: http://dx.doi.org/10.1162/glep.2009.9.4.14.

48 Engel-Glatter S, Ienca M. Life scientists' views and perspectives on the regulation of dual-use research of concern. Sci Public Policy. 2018;45(1):92–102. doi: http://dx.doi.org/10.1093/scipol/scx050.

49 Flower R, Dando M, Hay A, et al. Brain Waves Module 3: Neuroscience, conflict and security. Royal Society; 2012.

50 Kelle A. Synthetic biology and biosecurity awareness in Europe. Bradford Science and Technology Report No. 9. 2007. Available from: http://www.synbiosafe.eu/uploads/pdf/Synbiosafe-Biosecurity_awareness_in_Europe_Kelle.pdf.

51 Dando MR, Rappert B. Codes of conduct for the life sciences: Some insights from UK academia. Bradford Briefing Papers 2005;16.