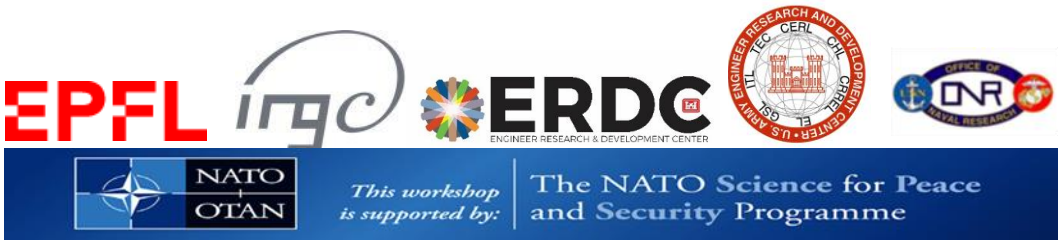

Security for Emerging Synthetic Biology and Biotechnology Threats

EPFL, Lausanne, Switzerland, 7-10 July 2019

Should we be concerned that synthetic biology be used improperly or maliciously?

Synthetic biologists are able to construct new biological systems and functions with applications in energy, health care, farming and elsewhere. Yet these same technologies can also be misused by negligent actors or deliberately used to create dangerous pathogens for which there is no known treatment. What can we do to advance science and technology for the common good while at the same time managing the risks of "dual-use" research, or research that can be turned against people or the environment?

Through the Science for Peace and Security Programme, the North Atlantic Treaty Organization (NATO) convened an Advanced Research Workshop to explore the core questions of biosecurity for synthetic biology. The workshop was co-organised by EPFL (International Risk Governance Center) and the US Army Engineer Research and Development Center, and hosted by EPFL.

Research and applications of synthetic biology within medicine, environmental sustainability, energy innovation, and other fields can support humanity and our vital resources. However, inadvertent or deliberate misuse of synthetic biology's capabilities can expose these same systems to both known and unknown threats. To ensure that synthetic biology's beneficial use is both possible and productive, these threats and uncertainties must be minimized and the exposed systems must be prepared to absorb and recover from any damages resulting from misused synthetic biology. The Lausanne workshop focused particularly on the former by critically exploring the concept of biosecurity and its relationship to existing international and national structures, technological supports, as well as the choices, objectives, and behaviors of actors engaged in synthetic biology development. Opportunities exist to establish more coherent and scalable approaches for biosecurity governance at all scales, and this workshop began the process of envisioning the future of coordinated biosecurity.

The workshop was organised by Benjamin Trump, Igor Linkov and Edward Perkins (US Army ERDC) and Marie-Valentine Florin (EPFL). Scientific advice was provided by Kenneth Oye (MIT and EPFL) and Piers Millet (Oxford University).

Attendees

The workshop convened 70 attendees from 7-10 July 2019 at EPFL, Lausanne, Switzerland. The attendees' organizations represented 17 countries including NATO member states, NATO partner countries and international organizations. Participants' expertise ranged from military operations and threat evaluation, academic applications of synthetic biology, private industry, and regulative and legislative authorities. The workshop also included experts from other fields like cyber security, which has faced similar questions about maximizing benefits while minimizing risks. The range of

Contact: marie-valentine.florin@epfl.ch; bdtrump@umich.edu

subject matter expertise reflects the multi-disciplinary challenge that synthetic biology presents in its development.

Workshop participants

Working Groups

The workshop organized the participants into five working groups. A copy of the read-aheads can be found in appendix.

1. Working Group 1 examined the role of hard law within states and international conventions for governing synthetic biology. The group also considered industrial practices that span borders and must operate under changing regulations. Working Group 1 strove to understand the current state of regulatory and legislative activities relevant to active synthetic biology development programs, and evaluate future needs for governance reform to ensure effective biosecurity and biosafety practices for synthetic biology.

   Working Group 1 observed that existing international instruments like the Biological Weapons Convention and the Chemical Weapons Convention currently encompass synthetic biology developments. However, coordination is needed between conventions to ensure that no aspect of synthetic biology is inadvertently left unaddressed. Nationally, legislation, and regulation vary by country, with some countries purposefully risk averse, others less so, and some not yet considering the synthetic biology at all. Inherent challenges arise from rapid innovations in synthetic biology may outpace efforts to regulate it. Solutions to these challenges will require decision makers dedicated to understanding the emerging science and its governance.

2. In contrast and in parallel to Working Group 1 that considered 'top-down' governance, Working Group 2 examined 'bottom-up' grassroots governance, including with education and outreach. The Group considered the practitioners of synthetic biology and the nascent operating procedures currently in use to promote safety and security in its application. The effectiveness of these measures depends on several factors, including access to information and training, established norms, perceptions of responsibility, funding allocations, and linkages with existing governance structures.

   Working Group 2 emphasized the importance of individual actors performing synthetic biology. These actors are differentiated by their context, their disciplinary training, and well as their culture, all with different degrees of mutability over time. Top-down and bottom-up governance must be coordinated and stakeholder-inclusive to reflect these differences. Working Group 3 imagined that effectively blocking information hazards will require adaptive governance, situational awareness, and creative minds willing to view new information with a lens for malevolent use.

3. Working Group 3 examined information hazards posed by disseminating research innovations that can be coopted by actors with nefarious purposes. When synthetic biology developers

provide information to the public, whether through academic publication or speculative strategizing, they should have the tools and knowledge to weigh the risks against the anticipated benefits. Existing mechanics for review and control should complement efforts to block malevolent actors from accessing critical information without stymying technological advancement, biosafety oversight, and communications with policy makers.

4. Working Group 4 considered the technical aspects (screening guidance, attribution and traceability) that would support identifying and managing increased risks in synthetic biology development. This is a two-pronged challenge, needing both screening purchases of biological material that could be recombined or modified deliberately or accidentally into a harmful agent, and tools to assess whether a state or non-state group has developed a harmful agent or bioweapon in secret. These capabilities assume an understanding of risks embodied in synthetic biology products and the usually harmless constituent components that would indicate their production. Existing tools for rapid sequencing for biological material have not prioritized addressing gene edited organisms. Screening, diagnostics, and forensics must be applied to genetically-altered organisms to best protect against potentially harmful usages.

   Working Group 4 began mapping current technological achievements that support sequencing screening, attribution and traceability. These can support near-term opportunities for prevention, detection and response, though each of these steps offers its own challenges and solutions. In the long term, future thinking will be necessary to understand implications for adaptive risk management.

5. Working Group 5 acknowledged the uncertainties that developments in synthetic biology might bring to existing technologies and policies, reviewed various foresight techniques that can support institutions in their work to look into the future, and examined how foresight is used by various institutions to support the anticipation of near and intermediate term changes and to prevent large negative disruptions. This includes the likelihood of biosecurity threats from state-based or non-state-based actors and of careless use. Credible forecasting of dangers should generate policies that mitigate dangers while critical assessments of uncertainties can galvanize efforts to close key gaps in knowledge. Therefore, the quality of foresight exercises will strongly influence system preparedness for threats arising from synthetic biology applications.

   Working Group 5 clarified the objectives of a foresight exercise: engage and inform stakeholders, develop appropriate governance mechanisms, gain insight into adversarial capabilities, realize the opportunities and harness them, identify key trends and warning signals, and mitigate identified threats. A foresight exercise needs an audience and group of participants, who might overlap. A foresight process could elicit key questions and ensure transparency and limitations are acknowledged.

Next Steps:

An edited book from many workshop participants will be completed within 9 months of the close of the workshop. The chapter drafts for the workshop are due in November and will greatly expand upon these abbreviated findings. In conclusion, there is much work to be done ensuring both biosafety and biosecurity amid the advancements of synthetic biology, but with a greater understanding of the challenges and their interconnectivities, a roadmap can be drawn.

Appendix: Working group read-ahead

Group 1: Top Down National and International Governance for Biosecurity

National governments and international organizations have considerable influence in shaping policy, regulation and best practices of technologies. Such organizations have vested interests in promoting security to protect against the dangers of inadvertent or deliberate misuse of a technology from state-based or non-state-based actors for harmful purposes. These considerations are relevant for the development of national regulations, bilateral agreements, and multilateral conventions.

Policymakers and other key stakeholders in government have the ability to craft, implement, and revise *hard law* (or formal legislative instruments that carry the full weight of law based upon expectations for safe operating procedures). Such hard law can be an effective tool to mandate best practices and protect against biosecurity threats. However, it can also be cumbersome and difficult to reform due to political and institutional costs for developing, operating, and reforming such hard law.

To date, hard law such as current regulations pertaining to conventional biotechnology, GMOs, and chemicals have been applied to the process and products associated with synthetic biology. Few *sui generis* tailored regulatory instruments have been implemented to address specific aspects of advanced forms of synthetic biology, including multiplex gene editing and de novo synthesis. A question within many communities centers upon whether and to what extent such *sui generis* hard law may be necessary for this field, what such law should look like, and how to adapt such hard law to account for changes in the extent and diffusion of scientific knowledge and technical capabilities within synthetic biology.

Transnational private regulation can also be seen as a form of top-down private agreements of various types, reflecting, for example, the decision of industry to abide by negotiated codes of conduct. As markets and regulatory tasks become increasingly global, forms of private international regulatory cooperation are emerging along with – or sometimes as a replacement for – inter-governmental cooperation. Creative and stakeholder-driven strategies are needed.

This group will consider the top-down governance landscape, and reflect upon (a) the current state of regulatory and legislative activity within various countries with active synthetic biology development, and (b) potential future needs for regulatory and legislative reform to institute formal best practices, testing requirements, and formal operating procedures for technological security.

Key questions:

- *Is there a need to revise or adapt current (a) international conventions, (b) national regulations and (c) transnational private arrangements? Or should priority be given to better enforcement of current laws?*
- *How should government and other leaders communicate on the potential for malevolent actions without being inhibited by concerns over enabling malevolent action?*
- *How can governments arbitrate trade-offs between enhancing security and stimulating innovation to remedy important environmental or health problems?*
- *What forms of surveillance and warning of malevolent or unsafe actions could and should be put in place?*

Group 2: Bottom-Up Grassroots Governance with Education and Outreach

University researchers, non-governmental organizations, research funders, community laboratories and international educational initiatives play significant roles in developing synthetic biology. Though the field is still nascent, many such organizations and consortia have begun to foster acceptance of strong safe operating procedures in the field and to apply existing conventions and agreements to synthetic biology and its enabling technologies. Bottom-up initiatives span a myriad of places where safety and responsibility can be practised concretely, and thus serve to identify emerging concerns throughout the process of a technology development.

First, researchers in conventional institutions and unconventional DIY have developed voluntary codes of conduct to address biosecurity and biosafety risks. For example, academic researchers doing gene drive work and the private foundations funding such work have agreed on standards to limit risks. Likewise, synthesis firms formed voluntary consortia to address security concerns by screening orders. The self-governance or 'do-it-yourself' (DIY) movement in community labs is now contributing to shaping the direction of biosafety and biosecurity considerations. Synthetic biology has a vibrant DIY and self-governance culture. DIY labs are naturally concerned with biosecurity concerns (i.e., active and passive monitoring for misuse of synthetic biology to engineer hazardous biological agents). These bottom-up initiatives have included experiments on informal best practices, codes of conduct, and operating agreements that reflect and shape the value systems and behaviour of researchers and innovators. Second, bottom-up initiatives include a variety of biosafety and biosecurity educational and training programs. These programs share a common goal that those who develop synthetic biology do it in full consideration of safety, security and responsibility aspects. These aspects include both conventional dual-use concerns with deliberate intention to cause harm and unintentional misuse when lack of safety of scientific knowledge inadvertently leads to the creation and/or dissemination of hazardous material or information. These educational initiatives include activities within universities and in unconventional international initiatives such as iGEM.
In parallel to Group 1 (top-down governance), this group will consider the role of bottom-up approaches to synthetic biology risk in biosecurity efforts. Specifically, this group will review and discuss existing security requirements. gaps and potential challenges, as well as the instruments and actions that such groups can take to foster biosecurity and enhance trustworthiness within their research areas.

Key questions:

- *How well have existing bottom-up voluntary codes worked? Is their effectiveness likely to decrease or increase? Should codes be modified? Expanded? How?*
- *Have existing educational programs fostered lab safety and responsibility? Should such activities be modified? Expanded? In what respects?*
- *Who should be mobilized and trained on dual-use and biosecurity threats without revealing too much on worst-case scenarios? (Link to Group 3)*
- *How can the conventional institution based scientific community and non-traditional and non-institutional actors enhance responsible conduct and beneficial use?*
- *With regards to DIY biology and citizen science communities,*
  - *What are the responsibilities of institutions (academic, government, industry) in supporting DIY communities with regards to biosafety, biosecurity and training in general? How can professional scientists contribute to best practice in DIY communities?*
  - *Should institutions be encouraged to provide financial (funding) or in-kind resources to DIY communities to increase best practice and responsibility?*
  - *What governance aspects would benefit from the participation of DIY (non-professional or non-institutional) scientists and how to include their views and practices?*

Group 3: Information Hazards

This group will consider the dual-use nature of synthetic biology, with emphasis on the potential for misuse associated with dissemination of information that should not be communicated to a wider audience. Biosecurity analysts have commonly viewed synthetic biology 'information' as a potential hazard to be reviewed and controlled, with emphasis on limiting access to information that could be used by malevolent state and non-state actors to produce biological agents that may endanger human or environmental health. Information hazards were addressed through centralized approaches to the evaluation of specific lines of research and approval of information release to institutions that had the resources and scientific wherewithal to execute such research without endangering security.

The working group on information hazards will engage with two sets of issues that pose challenges to this conventional view.

First, the viability of centralized approaches at biosecurity, including the review and control of information has been eroded by the globalized and increasingly diversified nature of synthetic biology research. In practical terms, the horizontal diffusion of research capabilities across international boundaries and the vertical diffusion of research capabilities from traditional universities and firms to unconventional actors are in conflict with current mechanisms for review and control.

Second, managing information hazards to limit access by malevolent actors is complicated by the existence of tradeoffs with other legitimate areas of concern. Measures to limit information access by malevolent actors may also limit access by:

(1) researchers who need fuller information to enable scientific and technical advance;
(2) biosafety officers and educators who need information on hazards to reduce the likelihood of unintended harmful acts by uninformed careless actors; and
(3) policy-relevant actors who need unbiased information to inform deliberations on research funding, environment, health and safety regulation and biosecurity.

This group will identify tradeoffs across benefits and costs of information controls and develop ways to improve the terms of tradeoffs in a world of rapidly diffusing research capabilities. Solutions must be appropriate for all actors involved. Well-intentioned actors include biosafety officers, academic and commercial scientists and safety and security managers. Malevolent state and non-state actors would include relevant national military law enforcement, intelligence authorities and UN BWC staff.

Key questions:

- *What information would be most useful to bad actors? Is it possible to limit access? How?*
- *What information is needed to enable scientific advance? To limit inadvertent dangerous behaviour? To inform policy deliberations? What degree of specificity is needed for these activities?*
- *How should tradeoffs across these ends be managed? Can the terms of tradeoffs be improved by measures such as segmentation of information flows?*
- *What type of research should be allowed or disallowed at various levels of development (i.e., high schools, universities, secured laboratories, etc.?)*
- *What are sources of uncertainty on these issues? How might uncertainty be reduced?*
- *Who decides what information should be withheld? Who watches the watchers?*

Group 4: Technical aspects: screening guidance, attribution and traceability

Prevention of and protection against deliberate misuse or careless use of synthetic biology and enabling technologies requires proper processes, methods, and tools to identify and better understand the scale and implications that the modified organism poses to human and environmental health. This is a two-pronged challenge, with need for: (a) biological screening for university or industry purchases of biological material that could be recombined or modified deliberately or accidentally into a harmful agent, and (b) forecasting, diagnostic, and forensic tools to assess whether a state or non-state group has developed a harmful agent or bioweapon in secret.

These tools underscore the need to detect when a modified organism has been released into the environment, as well as to diagnose critical questions about the characteristics, implications, and the challenges associated with potential quarantine or remediation. Detection and identification involve a mixture of passive and active surveillance mechanisms to determine when a threat event may be occurring. Once the threat has been identified, the next step is to determine *how* genetic modification was executed, as well as *what* genomic change was undertaken in order to achieve a given phenotypic characteristic. This task involves rapid sequencing and synthesis tools that, while increasingly economically feasible, have not been prioritized or tested to address gene edited organisms. A lack of detection and identification capability can significantly increase the time it takes to isolate, synthesize, and remediate/ameliorate an engineered threat.

This group will consider the technical challenges, gaps, and future requirements related to the screening, diagnostics, and forensics of genetically-altered organisms in the biosecurity landscape. Specifically, to better protect against the outcomes of deliberate misuse or careless use of synthetic biology's enabling technologies, it will be important to understand what existing scientific tools and procedures are available to conduct such inquiries, and better understand the critical questions of (a) what type of genetic modification was undertaken on the organism, (b) who did it and within which laboratory, and (c) how/with what instruments was the modification undertaken. For example, the group will discuss the development of standards and tools to track and identify SynBio/biotechnology-modified constructs/organisms such as IARPA's FELIX (Finding Engineering-Linked Indicators).

Key questions:

- *What do we know from scientific assessments of the potential of biological materials to be used to cause deliberate harm? How credible are the assessments?*
- *What technical steps can be taken to mitigate misuse? Classified or open software? What types of containment measures or other technical means could be deployed to prevent intentional spread of dangerous material? What are the gaps?*
- *Is it possible to construct and query databases of hazardous DNA sequences that secure queried sequence fragments and database contents?*
- *What is a safe research environment? For example, are there specific aspects of gene drive that either cause concerns or could be enhanced to limit the spread of undesirable germline editing? Would security-preserving technologies (encryption or blockchain) help ensure security?*
- *What key sources of uncertainty exist in this domain? What would you like to know more about? What policy or research measures would you suggest to fill gaps?*

Group 5: Foresight: developing near and intermediate term perspectives

Considering the three main areas of concern (blocking weapons production by state actors, blocking development and production of biological agents by non-state terrorists, and reducing risks that synthetic biology may be carelessly used), this working group will discuss foresight around technology and policy developments that might reduce future risks, as well as those that pose risks.

Both the direction of synthetic biology and how synthetic biology might combine with other technologies are unclear. Therefore it is difficult to anticipate the nature and likelihood of biosecurity threats from state-based or non-state-based actors and of careless use in the coming years. These difficulties are compounded by the inherent contingency of forecasting. Future biosecurity risks will depend on responses to forecasts, where responses will depend on policy decisions, interaction and feedback between various stakeholders, and the quality of diagnoses of vulnerabilities. Credible forecasting of dangers should generate policies that mitigate dangers. Credible assessments of critical sources of uncertainties should generate policies that close key gaps in knowledge.

Early-warning systems for early identification of signals of biosecurity concerns, horizon scanning for short-term developments, and foresight for longer term exploration of the future serve as imperfect but valuable tools to identify potential futures of a technology's growth, commercialization, and use – often under the guise of likely, best case, and worst case scenarios. Foresight-centred exercises seek to follow paths of development and derive assumptions that would drive field developments towards one direction or another. For biosecurity, such discussion seeks to identify potential technological improvements or developments that further the dual-use nature of synthetic biology, and/or the socio-political drivers that may influence the use of synthetic biology for harmful use purposes such as bioweapons, WMDs, or similar objects of concern.

This group will discuss strategic foresight to identify major biosecurity trends and risks that we may need to respond to in the next 20-30 years and will suggest ways to mitigate risks. It will focus on (a) the emerging development path of synthetic biology at varying time intervals (within 5, 10, and 25 years); (b) possible future large-scale applications and regulatory frameworks; (c) interactions between stakeholders that might alter trajectories of technology development and application; and (d) what near-term national and international biosecurity policies might help prepare for anticipated long-term developments.

Key questions:

- *What technological developments and applications are we afraid of? Through what new routes or platforms could synthetic biology be misused for the purposes of terrorism or mass disruption?*
- *How does one forecast carelessness in biological research? Are there bottlenecks or inflection points that, if not properly addressed, could trigger a significant safety threat?*
- *Will the combination of diffusing technologies, rising geo-political and economic competition and cultural diversity vitiate state and non-state biosecurity collaboration?*
- *Will geopolitical tensions and governance deficits enable free-riding? Over the long term, will international agreements and moratoria against biological weapons hold?*
- *What policy developments might reduce future risks, or pose new risks?*
- *What sources of long-term policy-relevant uncertainty are evident? What near-term actions might mitigate uncertainty and inform future deliberations?*