Security Implications of Emerging Biotechnologies: Workshop Summary, Analysis, and Recommendations

Diane DiEuliis and Charles Lutes

June 2016

Security Implications of Emerging Biotechnologies
Workshop Summary, Analysis, and Recommendations

Diane DiEuliis and Charles Lutes

On April 26th, 2016, the Center for the Study of Weapons of Mass Destruction (CSWMD) at National Defense University held a workshop to explore "Security Implications of Emerging Biotechnologies." Participants from government, NGOs and academia discussed opportunities and challenges of a new era of biotechnology, one highlighted by the advancing ease with which the genomes of organisms can be engineered for specific purposes, potentially more rapidly than we are prepared to assess and deal responsibly with its ramifications. Synthetic biology and associated genome editing tools will be essential for addressing the global challenge of resource scarcity, provide unprecedented advances in public health and medicine, and create innovative products that can support national defense, as well as commodities that stimulate the US economy. At the same time, new dual-use technologies will present significant challenges to biosecurity, biosafety, and have already begun to generate ethical and moral dilemmas. Participants stressed the need to address these issues in ways that do not stifle the technology's advancement nor America's competitiveness in the global bioeconomy.

The workshop was convened to consider the potential biosecurity concerns of emerging biotechnologies and their impact on national security. The dual use problem was discussed in the context of "biosecurity by design," a concept conceived specifically in preparation for the workshop in which government, industry, academia, national laboratories, and individual users should be mindful of developing potential security solutions at each step of technology development. Participants also confirmed that the scope of biosecurity should extend to the protection of people, the environment and the economy, as all may be vulnerable in the face of emerging biotechnologies. It further was noted that threats could include those perpetrated for "strategic effect," and should not be limited to those traditionally associated with weapons of mass destruction (WMD).

It was agreed that the initial premises for convening the workshop are valid, i.e. current regulations and their associated compliance mechanisms are not scalable to the changes happening in biotechnology although future solutions may share some of the features of current governance tools. A particular challenge for governance is the "democratization" of the science and its accessibility by varied actors. Participants identified a number of unmet needs and discussed recommendations for moving forward, including a desire to meet regularly as a "Community of Interest" on emerging biotech to enable ongoing, dynamic discussions of both technological advances as they occur and to vet potential policy solutions. The following sections reflect observations and recommendations either discussed explicitly during the workshop or informed by those discussions.

Trends

Several important trends affect the arc of emerging biotechnologies and set the context for the security dimension:

- *Biology is a strategic technology for the 21st century.* Just as information technology and the internet have transformed society, business, government, and warfare since the late 20th century, biotechnology will similarly shape the global landscape for the next several decades. In order to establish and maintain global leadership in biotechnology, the United States requires a holistic national approach that supports innovation and growth in the bioeconomy, establishes strategic priorities, and ensures responsible use.

- *Industrial innovation and recognized societal needs are increasingly leveraging emerging biotechnology, rapidly developing a "bioeconomy."* The locus of this economic innovation is in industry, and particularly startups. Government funding does not currently drive the bioeconomic trajectory, making government just one of many actors shaping the trend.

- *Convergence with other emerging technologies will further accelerate economic development and societal change.* Emerging trends in nanotechnology, robotics, information technology and other fields will impact biotechnology's advancement. For example, the industry is in the process of adopting automated manufacturing platforms (automated fermentation platforms, for example, and automated laboratory processes), which may pose additional vulnerabilities and biosecurity challenges.

- *The rapid pace of change in biotechnology far outpaces policy innovation.* For example, innovations in gene editing technology, specifically the development and growth of the CRISPR method, has occurred largely since the last Biological Weapons Convention (BWC) Review Conference (REVCON) in 2011; thus the primary international body for addressing biological threats has yet to fully consider the impact of gene editing. The five-year periodicity of the REVCON is insufficient to adequately address fast moving technology changes such as CRISPR.

- *The "democratization of science" will enable widespread diffusion of knowledge of advanced biotechnologies, beyond the purview of government to regulate its flow.* The open nature of the life sciences has resulted in both deskilling and lower costs for advanced techniques in biology. A wider range of actors have easier access to both explicit and tacit knowledge, lowering the barriers to entry for some portions of the pathway to biological weapons development. Do-it-yourself (DIY) open biology laboratories, and the annual International Genetically Engineered Machine competition (IGEM) are examples of this trend.

Security Concerns

The dual use nature of biotechnology presents a number of challenges to policy and governance. The scientific community is engaged in a robust discussion on biosafety concerns as well as ethical issues[1]. Security issues have garnered less attention among scientists but are beginning to engender significant attention by national security and homeland security

[1] http://www.nationalacademies.org/gene-editing/Gene-Edit-Summit/index.htm

policymakers. Taking a broad notion of security, the following issues will have significant implications for the policy landscape.

- *Biotechnology creates challenges and opportunities for biosecurity, national security, and economic security.* Security—broadly conceptualized—will be impacted by emerging biotechnologies in a variety of ways. Advances in the life sciences can create new pathways for biological weapons development but at the same time will provide new capabilities for countering those weapons. Bio-inspired innovations (human performance enhancements, advanced materials, "living" sensors, and new forms of energy production) will enable new military capabilities that can alter current dynamics in military competition. Social and economic shifts are likely to occur as biotechnology offers new industrial and consumer goods, changing the nature of global economic competitiveness.

- *The WMD paradigm is an inappropriate lens through which to view emerging biotechnology.* While emerging biotechnologies will challenge current nonproliferation regimes, WMD concerns should not drive the overall U.S. approach to biotechnology, but should be considered in the context of a holistic policy.

- *Synthetic biology may enable intentional creation of new forms of biological weapons that include modifications or enhancements of traditional threats, novel threat agents, and genetic weapons.* Workshop participants agreed that the bar is potentially lowered for the *creation* of biological agents, rather than testing, scale up, or delivery, although convergent technological advancement in other fields such as nanotechnology, could be enabling of the latter.

- *Emerging biotechnology will be increasingly available and possibly of greater interest to nefarious actors with malicious intent.* The new capabilities described above, the ability to circumvent traditional detection and countermeasures, and increasing ease and access to technology, will empower a diverse range of actors to investigate the feasibility of biological weapons. However, significant challenges remain—particularly in the areas of weaponization and dissemination—that will not be overcome solely through advancements of biotechnology.

- *Harmful biological entities may be created accidentally.* This is a fundamental biosafety concern and should continue to be considered in governance deliberations.

- *Gene drives, enabled by emerging biotechnology, may be subverted as disease dissemination tools, or environmental or agricultural threats; and our lack of ability to detect them may also be a problem.* We do not yet know all of the potential impacts to humans, the environment or the economy that gene editing technology may have when introducing engineered species into laboratories and/or environments, yet we have the capability now to create engineered species. We do not have a good baseline for monitoring biological/ecological systems that would indicate when a harmful gene drive had been introduced.

- *Protection of genomic information is a critical biosecurity issue.* An understanding of the underlying function of DNA and genomes is a key enabler of emerging biotechnology. Genome data will be crucial to the bioeconomy, national biodefense, and important health initiatives such as Precision Medicine[2]. It will be key to leverage genomic data for best advantage to US science, economy, and biodefense, while safeguarding against potential misuse and protecting group and individual privacy. .

- *"Democratization of biotechnology" and continual innovation complicate situational awareness of the biotechnology landscape.* Numerous features of emerging biotechnology are making it accessible to a wider variety of actors, thus it will be much harder to track those with the requisite experience and capability to do harm.

- *The constantly evolving nature of biotechnology will stymie list-based efforts to restrict technology.* Our current approach to controlling "select agents" will be inadequate for dealing with synthetically developed agents.

- *Emerging biological threats may have strategic significance without creating "mass destruction."* The traditional definition of biological weapons as WMD may be an inadequate lens through which to view the scope of threat. The threat could include actions taken by adversaries or malicious actors for "strategic" or "instability" effects, rather than large scale mass effects on people; for example, just a very few sickened individuals, particularly if discriminately targeted, could promote societal fear/panic.

Policy and Governance

Our current set of tools include the Biological Weapons Convention (BWC), United States bioterrorism statutes, the Biological Select Agent Program (BSAT), export controls, Terms and Conditions of research awards, and biosafety and other guidance. A detailed taxonomy of current governance tools was presented at the workshop, however these current tools are insufficient to address the security issues creating by emerging biotechnologies. This section discusses the features and characteristics of a desirable governance structure along with observed gaps and unmet needs of the current structure.

The goals of governance would be to: *mitigate danger of attacks* by helping to prevent them or by improving our ability to respond to them accordingly, and to *facilitate legitimate activity*, and to *protect public trust.* Governance tools should meet conditions of utility (ability to mitigate risk), feasibility, and credibility. While we want to promote the bioeconomy writ large, that does not mean that there cannot be a small "tax" which promotes biosecurity—the caveat being that the cost of any governance mechanism should be proportional to its benefits (a modest protection from harm should have a modest cost).

Governance tools could range from rules and expectations regarding the creation of DNA; where research could be done and by whom; transparency on who has access to biological materials; and conditions on supply chains. Other aspects of governance tools related to

[2] https://www.nih.gov/precision-medicine-initiative-cohort-program

responsibility, accountability, and education and awareness are particularly relevant to the increasing accessibility of emerging biotechnologies.

Before we can design an effective governance structure, we need to understand both the scope of biotechnology and the growing bioeconomy and their consequential dual use implications. We need to understand how securing people, the environment, and the economy are related, and how they differ. This is a multivariate problem which will require a purposeful systems approach to resolve.

Policymakers should address the following gaps in developing new policy and governance measures:

- *The U.S. does not have a holistic national approach to emerging biotechnology that addresses biotechnology needs for defense, for public health, and for the bioeconomy.* The National Bioeconomy Blueprint[3], for example was published in 2012, and describes five strategic objectives with the potential to generate economic growth and address societal needs. However its scope did not extend to biosecurity, and it would be important to revisit and expand its goals in light of emerging trends. To the extent that biology can become a strategic technology for the US in the 21st century, increased high level strategic guidance should be considered that emphasizes "biosecurity by design" from the outset.

- *In order to better define specific threats, we need a better understanding of resources, infrastructure, and technological experience that potential adversaries and malevolent actors would need in order to utilize emerging biotechnologies for harm.* The assumption that wider access to emerging biotechnology will increase the risk of biological threats needs to be explored systematically: specifically, how these technologies will affect the pathway to a biological weapon (whether done by a state on an industrial scale or improvised by a non-state actor) and what pathway barriers remain.

- *We currently do not have a common baseline with which to understand perturbations to biosystems*. Detection, surveillance, and attribution will be further challenged and it will be important to be able to detect environmental changes from the norm. For example, we do not have an ecological baseline that would serve to identify a maliciously introduced synthetic organism (congruent to the already present invasive species problem).

- *Similarly, if we knew all the pathways/mechanisms by which pathogens can cause disease, we could formulate more generalized countermeasures*. There are a limited number of pathways that a pathogen could exploit, so whereas there may be a great many infectious organisms and an unlimited number of ways those organisms could be modified, there may only be a few common pathways that these pathogens could exploit to cause disease.

- *There is a shortage of life scientists and biotechnologists working in national security agencies*. There is a shortage both in scientific skills and basic understanding of the life sciences in some security sectors of government. For example, the Department of Defense

[3] https://www.whitehouse.gov/sites/default/files/microsites/ostp/national_bioeconomy_blueprint_april_2012.pdf

has a well-entrenched physics-based mindset with great depth of understanding of kinetic and nuclear weapons, but the Department is less familiar with the life sciences except in niche areas.

- *Our traditional approach to dealing with biological threats by developing and stockpiling particular medical countermeasures will not suffice to address the full scope and diversity of the threat.* Synthetic biology will enable tailored threat agents. A nimble, flexible system of countermeasures development will be required to deal with constantly evolving threats.

General Recommendations

The security challenges presented by emerging biotechnologies will require a coordinated national approach. As such, the U.S. should:

- *Promote "biosecurity by design" to ensure biosecurity measures are built-in as the technology develops.* Government, industry, academia, national laboratories, and individual users should be mindful of developing potential biosecurity solutions at each step of technology development. Non-governmental entities may look for governmental guidance in how to do so.

- *Revisit U.S. national-level strategic goals for advancing the bioeconomy, and potentially devise renewed, holistic strategies which encompass emerging biotechnology broadly.* A security component should be embedded within any emerging biotechnology or bioeconomy funding/initiatives moving forward, rather than separate conversations.

- *Prioritize economic security.* As noted, the participants in the workshop agreed that we cannot afford the opportunity cost of not being competitive in the future bioeconomy.

- *Strive to fully reap the benefits of biotechnology, and to do so from a position of global leadership, both in terms of commercial success as well as establishing global biosecurity norms and standards.* To do so will require that the nation better understand the bioeconomy and our competitive position within it.

- *Incorporate biosecurity, as appropriate, into various components of the Federal regulatory system for biotechnology.* We are in the midst of a process to modernize the Federal regulatory system for biotechnology products and to establish mechanisms for periodic updates to that system[4]. While this process focuses on plants, animals and microbes[5] (not human drugs or medical devices), it represents an opportunity to introduce and include biosecurity mechanisms to protect the health and the environment.

- *Support a research agenda, both classified and unclassified, that identifies "paths to harm" that bad actors could take and provides insights into the intent of bad actors.* It will be

[4] https://www.whitehouse.gov/sites/default/files/microsites/ostp/modernizing_the_reg_system_for_biotech_products_memo_final.pdf

[5] https://www.aphis.usda.gov/brs/fedregister/coordinated_framework.pdf

essential to continually update our understanding of the art of the possible in order to realistically characterize the risks.

- *Develop robust protection measures for genomic data.* DNA databases must be secured both for privacy and security. The U.S. must ensure standards for collection and storage of critical bioinformatics information.

- *Incentivize industry to offer "biosecurity by design" solutions.* The same technology that will create new challenges will create new opportunities in solving those problems. The U.S. should develop an incentive structure to ensure industry seeks those solutions early in their development of biotechnology products and processes.

- *Create an environmental "baseline" of data that enables detection and/or attribution.* Systems like NEON[6] and others are disconnected from the biosecurity arena, and could be valuable resources for defense.

- *Provide more outreach and engagement*. There are some areas in which we are already comfortable and engaged, but perhaps have not been leveraged or utilized to best advantage in light of emerging biotechnologies. Specifically, more could be done on:

    - Defining norms of appropriate and non-appropriate behavior.
    - Education, increasing security awareness and training in institutions, and providing outreach to leadership of laboratories to instill biosecurity awareness.
    - Outreach to industry, professional societies, and international partners should be included.
    - Building a "citizenship for science". It was noted that the original National Strategy for Countering Biological Threats[7] is a particularly good example of how to do this
    - Providing incentives for "Biosecurity by Design" through awards or prize competitions
    - Ensuring the USG is more visible and involved, for example, by providing financial support for initiatives like iGEM and synbioleap.

- *Seek better ways to increase S&T understanding among the lay public*. There is a need to articulate the importance of emerging biotechnology and engage with the public on how it can lead to the production of goods and services that will benefit them in ways that do not put them or their values at risk. Loss of public trust and confidence could generate demand for ineffective or counterproductive policy measures.

- *Explore ways to further increase, improve, and accelerate preparedness and response capabilities to swiftly characterize emerging threats and create countermeasures quickly.* Continue to evolve ways in which industry can \provide surge capabilities for rapid countermeasures in response to a biological event with novel agents.

[6] http://www.neonscience.org/

[7] https://www.whitehouse.gov/sites/default/files/National_Strategy_for_Countering_BioThreats.pdf

- *Seek to understand how our biosecurity actions affect the international landscape.* With its general purpose criterion, the BWC continues to establish norms against the malicious use of biological agents and delivery systems, no matter how they are constructed. However, the BWC and its associated mechanisms should be reviewed to see whether and how they might be adapted to address the security challenges of biotechnology not foreseen, or fully so, at the time the treaty was negotiated. In the 2016 BWC Review Conference, the U.S. should ensure an active, ongoing discussion on emerging biotechnologies.
- *Develop a regular, ongoing forum where issues around emerging technologies may be discussed with government and non-government subject matter experts.* This "Biotechnology Community of Interest" could be leveraged not only for discussing emerging trends, but for vetting ideas or proposals on governance. The establishment of such a forum would have to be mindful of the requirements of the Federal Advisory Committee Act and other applicable statutes.

Appendix: DoD Specific Recommendations

In addition to the national level recommendations in the main body of this report, the following are more specific actions that the Department of Defense should consider:

- *Form a DoD-wide cross-functional team to address the full scope of emerging biotechnology.* The Senate version of the National Defense Authorization Act[8] includes provisions for cross-functional teams, and biotechnology should be one of them, to enable consideration of both opportunities and security challenges.
- *Conduct a study on potential ways that emerging biotechnology could be used to defeat current and planned force protection measures and countermeasures.* A classified assessment should be conducted as to the susceptibility of the force to potential use of synthetic agents.
- *Conduct "red-teaming" to consider scenarios in which emerging biotechnologies might be used for harm, particularly in a military context.* Using its analytical and wargaming competencies, DoD should consider ways in which adversaries might find utility for emerging biotechnologies in countering U.S. military advantages.
- *Engage and incentivize the biotechnology industry to promote biosecurity by design and seek technology solutions.* This could be achieved through initiatives such as the Defense Innovation Unit Experimental (DIUX)[9], and strategies such as "Hacking 4 Defense"[10] to crowd source security solutions, and to work in collaboration with academia.
- *Continue to develop a biotech workforce.* DoD needs to develop its own deep bench of expertise in biotechnology, continue to inform and educate policy makers, while also including biotechnology as part of professional military education.

[8] https://www.congress.gov/114/plaws/publ92/PLAW-114publ92.pdf
[9] http://www.diux.mil/
[10] http://hacking4defense.stanford.edu/