CNS

OCCASIONAL PAPER

#26 · APRIL 2017

Findings from the 2016 Symposium on Export Control of Emerging Biotechnologies

Steven Fairchild, Caroline R. M. Kennedy, Philippe Mauger, Todd J. Savage, Raymond A. Zilinskas

INTERNATIONAL BIOSECURITY AND PREVENTION FORUM

TWIST BIOSCIENCE

Middlebury Institute *of* International Studies at Monterey

James Martin Center for Nonproliferation Studies

The views, judgments, and conclusions in this report are the sole representations of the authors and do not necessarily represent either the official position or policy or bear the endorsement of the James Martin Center for Nonproliferation Studies, the Middlebury Institute of International Studies at Monterey, the President and Fellows of Middlebury College, Twist, or the IBFP.

James Martin Center for Nonproliferation Studies
nonproliferation.org

The James Martin Center for Nonproliferation Studies (CNS) strives to combat the spread of weapons of mass destruction by training the next generation of nonproliferation specialists and disseminating timely information and analysis. CNS at the Middlebury Institute of International Studies at Monterey is the largest nongovernmental organization in the United States devoted exclusively to research and training on nonproliferation issues.

Middlebury Institute for International Studies at Monterey
www.miis.edu

The Middlebury Institute for International Studies at Monterey provides international professional education in areas of critical importance to a rapidly changing global community, including international policy and management, translation and interpretation, language teaching, sustainable development, and nonproliferation. We prepare students from all over the world to make a meaningful impact in their chosen fields through degree programs characterized by immersive and collaborative learning, and opportunities to acquire and apply practical professional skills. Our students are emerging leaders capable of bridging cultural, organizational, and language divides to produce sustainable, equitable solutions to a variety of global challenges.

International Biosecurity and Prevention Forum (IBPF)
https://www.ibpforum.org/

The International Biosecurity and Prevention Forum (IBPF) is a United States government initiative developed in partnership with the International Criminal Police Organization (INTERPOL), to prevent the misuse of biological agents as weapons of mass destruction. The IBPF is a unique, member-driven initiative that brings together the world's leading experts from the health and security communities to share expertise on key biosecurity and bioterrorism prevention issues. Our mission is to prevent the misuse of biological agents as weapons of mass destruction by sharing, exercising, and implementing biosecurity and bioterrorism prevention and response best practices. IBPF welcomes the participation of organizations that have a role in biosecurity and bioterrorism prevention.

James Martin Center for Nonproliferation Studies
Middlebury Institute of International Studies at Monterey
460 Pierce Street Monterey, CA
93940, USA
Tel: +1 (831) 647-4154
Fax: +1 (831) 647-3519

Findings from the 2016 Symposium on Export Control of Emerging Biotechnologies

October 18-20, 2016
Monterey, California

Steven Fairchild, Caroline R. M. Kennedy, Philippe Mauger, Todd J. Savage, Raymond A. Zilinskas

INTERNATIONAL BIOSECURITY AND PREVENTION FORUM

TWIST BIOSCIENCE

Middlebury Institute *of* International Studies at Monterey
James Martin Center for Nonproliferation Studies

Table of Contents

Executive summary

The Symposium on Export Control of Emerging Biotechnologies was held in Monterey, California during October 18–20, 2016. The symposium was planned and hosted by the International Biosecurity and Prevention Forum (IBPF) and the James Martin Center for Nonproliferation Studies (CNS). The symposium's objectives were as follows:

1. Identify emerging biotechnologies and services that might pose biosecurity risks.
2. Evaluate identified biotechnologies and services to determine those of concern that are not already under controls.
3. Assess the feasibility and desirability of potential control mechanisms for mitigating identified risks.

A total of sixty experts from fifteen countries participated in the symposium. They represented the scientific, policy, industry, legal, and enforcement fields in roughly equal proportions.

Participants identified seventeen emerging biotechnologies and services and debated whether each posed significant biosecurity risks. Participants then assessed options for new hard controls (export controls) and soft approaches (e.g., industry codes-of-conducts). Most participants flagged four biotechnologies and associated services as engagement priorities. These items and the proposed soft approaches are summarized in Table 1.

Table 1. Priority biotechnologies and associated services identified at the 2016 Symposium on Export Control of Emerging Biotechnologies and their potential for additional controls.

Biotechnologies and associated services	Can export controls be defined?	Are export controls desirable?	Potential soft approaches
Ground-based aerosol generating systems	Yes	No prevailing opinion	Outreach
DNA synthesis and assembly equipment	Yes	No prevailing opinion	Outreach
High-throughput screening systems	Likely	No prevailing opinion	Outreach
Facility-wide production control software	Further study needed	No prevailing opinion	Outreach

The symposium participants also identified five biotechnologies and associated services where an industry survey and further evaluation was deemed necessary for determining the viability of additional controls. These five were as follows:

1. Human disease models
2. Nano-packaging / microencapsulation
3. Predictive software for genetic engineering
4. Gene editing kits
5. Selection media

Along with identifying potential technologies and services for control and associated control mechanisms, the symposium participants generated six recommendations to help improve global biosecurity. Briefly, these recommendations are as follows:

1. Ensure that grant proposals for life sciences projects include a category on minimizing potential dual-use risks posed by their proposed research.
2. Globalize "know-your-customer" policies as an ethical business norm through international government and professional/industrial associations.
3. Should new export controls be devised for biotechnology equipment and services, these should make use of "sunset" clauses to ensure their timely reevaluation.
4. Ensure governments have a dedicated biotechnology working group within their ministry or multi-ministerial unit responsible for export controls.
5. Amend customs classification codes to better monitor the trade in controlled dual-use biotechnologies, and provide correlation tables between customs classification codes and their national dual use control codes to facilitate industry compliance.
6. Have governments work to internationalize gene synthesis sequence order screening practices.

1. Introduction

The International Biosecurity and Prevention Forum (IBPF) program is a US government effort to improve global biosecurity through international collaboration.[1] A goal of the IBPF program is to hold in-person events to allow individuals working in research, industry, health, policy, and law enforcement to share and improve biosecurity best practices. To further this goal, IBPF collaborated with the James Martin Center for Nonproliferation Studies (CNS) to organize and conduct the Symposium on Export Control of Emerging Biotechnologies.[2]

The symposium was held during October 18–20, 2016, in Monterey, California. A total of sixty participants from fifteen countries attended the symposium.[3,4] The participants are listed in Appendix 1.[5] They represented the scientific, policy, industry, legal, and enforcement fields in roughly equal proportions. The symposium had the following objectives:

1. Identify emerging biotechnologies and services that might pose biosecurity risks.
2. Evaluate identified biotechnologies and services to determine those of concern that are not already under controls.
3. Assess the feasibility and desirability of potential control mechanisms for mitigating identified risks, to include "hard" controls (export controls) and "soft" controls (e.g., industry codes-of-conducts, law enforcement outreach, government-issued guidelines, etc.).

2. Methods

The symposium's agenda was designed to accomplish the following tasks:

- Provide symposium participants with relevant background information.
- Allow participants to discuss topics in small groups.
- Allow all participants to review and discuss findings from individual groups for further questions and input.

Most of the symposium's first day and parts of the symposium's second and third days were dedicated to providing participants with relevant background information. The background information was provided via 20–45 minute presentations and panel discussions followed by

[1] International Biosecurity and Prevention Forum, <https://www.ibpforum.org/> (accessed November 20, 2016).
[2] James Martin Center for Nonproliferation Studies, <http://nonproliferation.org/> (accessed November 20, 2016).
[3] Some members of the organizing staff were also participants.
[4] Argentina, Australia, Bangladesh, Canada, Ethiopia, France, Germany, India, Jordan, Kenya, South Korea, Sweden, Switzerland, the United Kingdom, and the United States.
[5] Participants were given the opportunity to request that their names not be mentioned.

question and answer sessions. The topics for these presentations and panels included discussions of current emerging biotechnologies, reviews of existing export control regulations, and real-world examples of how biotechnology export control enforcement functions.

Following background presentations, participants met in small working groups with a designated moderator. The organizers assigned participants to specified groups to ensure that each group retained balanced expertise.

At the end of each day, all participants gathered for a plenary session to discuss findings from each group. In these sessions, the moderator from each group presented a summary of the group's findings along with points of contention or uncertainties. After moderators finished their reports, all participants could ask questions, clarify what had been discussed, and offer comments and suggestions.

The approach listed above had the following advantages:

- Each group could draw on other groups' findings during end-of-day plenary sessions.
- Each group could focus on the emerging technologies best known to the group's members, while the symposium could still cover a broad range of topics.
- Examining independent findings from each group enabled the identification of common areas of concern and topics where consensus was lacking.

2.1. Risk assessment criteria

When assessing whether an emerging biotechnology or service posed security concerns, participants were asked to consider whether it significantly enhanced a proliferator's ability to:

- Screen for or select biological agents.
- Screen for or select chemical agents through biological means.
- Modify an agent (enhanced pathogenicity/virulence/transmissibility, altered host range, improved drug resistance, evasion of diagnostics, evasion of host immune system including vaccine-induced response, enhanced hardiness).
- Produce and filter biological agents.
- Produce and filter biologically-derived chemical agents (toxins/peptides/bioregulators).
- Disseminate agents.
- Pose some other, non-traditional, threat.

2.2. Controllability assessment criteria

When participants identified a biotechnology or service that posed a security concern, the next step was determining whether the biotechnology or service could be amenable to controls. Participants were advised to consider the following factors when making this determination:

- The relative risk posed compared to what is already available to a proliferator (can they carry out a malicious act more consequential than before? With greater ease?).
- The degree to which the technology or service in question has dispersed globally or is expected to disperse globally. Also, if a technology is not dispersed, the reasons why this is the case (e.g., whether special capabilities are required to manufacture the equipment).
- The ease of commercialization of the associated services (if a proliferator cannot secure the equipment or does not know how to operate it, can they pay a service provider to do the work for them?).
- The sophistication and ease-of-use of the technology (whether the item or service would require state-level resources to be of use or would mostly be of interest to an advanced state-level BW program).
- Whether the equipment or service is already covered by existing multilateral export controls such as the Australia Group (AG) or Wassenaar Arrangement (WA).
- Whether industry-led or other "soft" approaches are already in place to address security risks posed by the technology or service under consideration.
- If considering potential export controls, whether the item can be clearly and precisely defined (e.g., so that the definitions sufficiently encompass relevant variants of the controlled item while minimizing overlap with items that governments do not intend to control).[6]

[6] The following served as a reference: Wassenaar Arrangement, "Criteria for the Selection of Dual-Use Items," agreed in 1994 and amended at the 2005 Plenary <http://www.wassenaar.org/wp-content/uploads/2015/06/Criteria_as_updated_at_the_December_2005_PLM.pdf> (accessed November 20, 2016).

3. Findings for biotechnologies and services considered

During the symposium, participants identified and assessed seventeen biotechnologies and associated services of potential concern. The findings are summarized in Table 2 and described further in Section 3.1 to Section 3.17 (below). Importantly, reported findings are based on the symposium team's interpretation of points raised by participants.

In Table 2, the first column names biotechnologies and services identified and assessed by symposium participants. The second column indicates whether participants felt that it was worth further assessing the feasibility and desirability of export controls and/or soft approaches for each item. In this column, "Yes" indicates the item appeared to warrant further evaluation, "No" indicates further investigation was generally deemed unwarranted by symposium participants, and "Further study" indicates that the participants lacked sufficient information about the technology and/or its various uses to make a determination.

The third and fourth columns in Table 2 indicate the symposium participants' beliefs that export controls could be defined for the item and the desirability of placing the item under export controls, respectively. For the third column, "Likely" indicates participants generally believed controls could be defined that address specific aspects of the technology, "No" indicates the opposite, "N/A" implies that definitions for the item were generally not discussed,[7] and "Further study" indicates participants did not have sufficient information to evaluate how well controls could be defined for the item. For the fourth column, the "desirability" of placing each item under export control included consideration of threats posed by the item (when misused), the item's existing availability, potential for unintended negative consequences of export controls, and enforceability of export controls. For entries in the fourth column, "No prevaling opinion" implies participants had varied opinions on the desirability of hard controls, "No" implies participants generally agreed export controls were not desirable, and "Further study" indicates participants did not have sufficient information / time to assess control desirability. The fifth and last column lists potential soft controls proposed for each item.

The assessments of each biotechnology and service, summarized in Table 2, are provided in the following subsections. These subsections report the points made by symposium participants along with notes on any disagreements and areas for further study.

[7] This typically occurred when participants believed the item should not be placed under export control and therefore did not spend time evaluating how controls would be defined.

Table 2. Findings from symposium participants for seventeen different biotechnologies and services.

Biotechnologies and associated services	Consider further?	Can export controls be defined?	Are export controls desirable?	Potential soft approaches
Ground-based aerosol generating systems	Yes	Likely	No prevailing opinion	Outreach
DNA synthesis and assembly equipment	Yes	Likely	No prevailing opinion	Outreach
High-throughput screening systems	Yes	Likely	No prevailing opinion	Outreach
Facility-wide production control software	Yes	Further study	No prevailing opinion	Outreach
Human disease models	Further study			
Nano-packaging / microencapsulation	Further study			
Predictive software for genetic engineering	Further study			
Gene editing kits	Further study			
Selection media	Further study			
BioBrick parts	No	No	No	None
3.11. Disease mapping software and *databases*	No	No	No	None
DNA sequencers	No	N/A	No	None
Lab-in-a-container setups, industrial biosynthesis lines	No	N/A	Current controls deemed sufficient	None
CRISPR/CAS9	No[8]	N/A	No	None
Antibody-drug conjugates	No	N/A	No	None
3-D printers and bioprinters	No[9]	N/A	No	None
Certified virus-free fertilized eggs	No	N/A	No	Monitoring customs data (if not already implemented)

[8] Participants flagged CRISPR/Cas9 security risks but did not identify export controls or soft approaches that would directly address these concerns. However, gene editing kits that employ CRISPR/Cas9 to facilitate dual-use modifications should be assessed as part of the further study of gene editing kits in general.

[9] Symposium participants noted that 3-D printers likely were not worth considering for export control for biosecurity purposes. However, participants also noted 3-D printers may be worth considering for other domains.

3.1. Ground-based aerosol generating systems

Participants broadly agreed that ground-based aerosol systems present a major loophole in existing AG controls, which are solely focused on aerosol dissemination systems designed to be carried on aircraft platforms. Existing AG controls only apply to systems "specially designed or modified for fitting to aircraft, lighter than air vehicles or UAVs [unmanned aerial vehicle]" that can generate an aerosol with an initial droplet volume median diameter "less than 50 microns at a flow rate of greater than two litres per minute" starting from a liquid suspension.[10] However, ground-based aerosol systems can also be used as effective biological agent dispensers, and participants felt that non-state groups were far more likely to use ground-based dispensers rather than attempt air dispersal. Several participants noted Aum Shinrikyo's repeated attempts at developing and using ground-based spray systems.[11]

Quite a few participants proposed to place ground-based aerosol generating systems under controls by modifying the AG Dual-use Biological Equipment and Related Technology and Software Common Control List so that the "specially designed or modified for fitting to aircraft, lighter than air vehicles or UAVs" requirement was dropped. Some participants further suggested removing the current "flow rate of greater than two litres per minute" control requirement. Air platforms have minimum flow rate requirements to ensure efficient coverage depending on their usage, but these requirements are not necessarily applicable for covert ground disseminators as several models are marketed that can be operated continuously for longer periods of time. Participants explained that the "less than 50 microns" control requirement made strong technical sense and should not be relaxed (i.e. "50" should not be reduced to a smaller number).

However, some participants expressed reservations as to the feasibility of expanding the controls in this manner given the number of civilian products that could be captured. These participants expressed uncertainties as to the size of the civilian market for ground-based aerosol generators, which have many applications, including pesticide application, hospital sanitization, and artificial fog generation. Participants also flagged that ground-based aerosol generators were necessary for experimental aerosol vaccine systems, although these systems were thought to be rare.[12] Some participants noted that ground-based aerosol generators capable of aerosolizing particles in the 10

[10] Australia Group, "Control List of Dual-use Biological Equipment and Related Technology and Software," section I, subsection 9 a), b), and c) <http://www.australiagroup.net/en/dual_biological.html> (accessed November 20, 2016).
[11] Aum Shinrikyo was the Japanese terrorist group responsible for the Tokyo subway sarin attack in 1995. See Holly Fletcher, Council on Foreign Relations, "Aum Shinrikyo," June 19, 2012, <http://www.cfr.org/japan/aum-shinrikyo/p9238> (accessed November 20, 2016).
[12] Raymond A. Zilinskas and Hussein Alramini, "Aerosol Vaccines," in Jonathan B. Tucker, ed., *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies* (Cambridge: MIT Press, 2012), pp. 267-268.

micron size particle range are already being sold over the Internet by vendors in non-AG countries.[13] Should these items turn out to be widely sold and manufactured in many countries, the proposed export controls would likely be unenforceable.

A few participants also expressed reservations that a terrorist group attempting to acquire a ground-based aerosol generating system could do so within the national borders of the country it is planning to attack, in which case export controls would be of no help to any attempts that aim to prevent terrorists from acquiring the aerosol generating system they might need.

Because of these uncertainties, participants considered ways of making the proposed export control criteria more specific to minimize the risk of accidentally controlling non-sensitive items ("unintended capture"). One method considered by participants was to specify controls for "nozzles" because they control the rate of flow, speed, direction, and size of aerosol particles emitted by a dissemination system. The major advantage of this method is its specificity, in that it controls a key component of a dissemination system rather than the overall system. The major drawback to this approach is that there are other methods that can be used to generate an aerosol that do not require nozzles.

Some participants wondered whether it would be possible to control nozzles based on specific parameters, such as diameter of the aperture, rather than on the particle size produced. This proposal appeared difficult to realize given the complexities of aerosol spray system designs. In addition, one participant had concerns that identifying suitable nozzles at the level of detail necessary to make such controls useable could reveal too much to a would-be terrorist who, unlike a state-level actor, could not easily obtain such information.

One alternative that was considered and resolutely rejected by participants was specifying a certain minimum total liquid capacity for the ground dissemination system. While a low capacity would limit the amount of agent that could be disseminated in a single attack, it was also thought likely to be an advantage to a proliferator in that it made the ground unit easy to move and hide. Participants also felt that it would be extremely easy for a proliferator to modify container systems to achieve any desired liquid capacity. Participants noted that attempting to control this parameter would likely create a loophole that allowed the sale of a sensitive aerosolization system if it did not have an associated high-capacity container.

[13] Raymond Zilinskas and Philippe Mauger, "Biotechnology e-commerce: A Disruptive Challenge to Biological Arms Control," CNS Occasional Paper 21 (Monterey, CA: Center for Nonproliferation Studies, 2015), pp. 33 <http://www.nonproliferation.org/wp-content/uploads/2015/06/biotech_ecommerce.pdf>.

3.2. DNA synthesis and assembly equipment

Many participants flagged equipment for synthesizing DNA as posing a biosecurity risk in that the technology underpins genetic engineering capabilities that can, themselves, be misused. For example, a proliferator could seek to insert a DNA segment (gene) coding for toxin production in an organism, either in an attempt at increasing the lethality of a pathogen, or for synthetic production of toxins. By far the easiest way of doing so would first involve the use of a DNA synthesizer to produce this DNA segment coding for toxin production.

Participants also noted that DNA synthesizers could eventually enable the circumvention of pathogen strain export controls. Several DNA sequences synthesized by a DNA synthesizer can be stitched together to obtain the genome of a controlled pathogen. After transcription (for viruses) or currently very difficult transplantation work (for bacteria), it is possible to "boot" this genome into a functional, replicating organism.[14,15] Presently, the technology allows for the synthesis of small RNA viruses.

Before further discussing DNA synthesizers, it is important to flag the existence of a large gene synthesis service industry. Desktop DNA synthesizers are expensive (currently in the $40,000 range), and the synthesis process becomes challenging and time consuming as the length of the desired DNA segment increases. As a result, many researchers rely on commercial services that ship a desired DNA segment lyophilized or prepared as part of a plasmid. Voluntary industry codes of conduct, adhered to by most commercial providers based in the United States and the European Union (EU) and which are adopted by at least one Chinese company, stipulate that commercial gene synthesis service providers screen orders for sequences of concern, such as sequences from the variola virus genome.[16,17,18] A proliferator that cannot purchase a DNA synthesizer therefore could attempt to purchase a desired sequence from a service provider and would probably try to do so from a company that does not screen orders or conduct "know-your-customer" checks.

Participants broadly agreed that DNA synthesizers have already diffused globally to the point where blanket "all DNA synthesizers" export controls would not be feasible. As such, several participants

---

[14] Daniel G. Gibson et al., "Creation of a Bacterial Cell Controlled by a Chemically Synthesized Genome," *Science* 329, Issue 5987 (July 2, 2010), pp. 52-56 <http://science.sciencemag.org/content/329/5987/52> (accessed November 20, 2016).
[15] Department of Chemistry, University of Maine, "Synthesizing Genomes," January 31, 2012, <http://chemistry.umeche.maine.edu/CHY431/Synthetic1.html> (accessed October 24, 2016).
[16] International Association Synthetic Biology (IASB) draft code of conduct (unpublished).
[17] International Gene Synthesis Consortium (IGSC), "Harmonized Screening Protocol: Gene Sequence & Customer Screening to Promote Biosecurity," November 18, 2009, pp. 1-4 <http://www.genesynthesisconsortium.org/images/pdf/IGSC%20Harmonized%20Screening%20Protocol-11_18_09.pdf> (accessed November 22, 2016).
[18] Jonathan Tucker, "Double-Edged DNA: Preventing the Misuse of Gene Synthesis," *Issues in Science and Technology* 26, No. 3 (Spring 2010), <http://issues.org/26-3/tucker-2/>.

tried to identify a "next-generation" subset that could be suitable for some form of traditional list-based control, or alternatively for "soft" approaches such as enhanced monitoring. Two criteria were proposed to define "next-generation" systems:

- only systems that were capable of synthesizing DNA segments and stitching these segments together ("assemblers");
- *de novo* synthesizers capable of producing "x"- long DNA segments in "y" hours (with "x" and "y" being suitable, as-yet-undetermined numbers).

Some participants stressed that DNA synthesizers required certain sophisticated subcomponents, namely special print heads and inks, optical results screening elements, and specialized software. For these participants, the difficulty in manufacturing these specialized subcomponents meant that new export controls on DNA synthesizers conceivably could be enforceable.

The question of whether "next-generation" DNA synthesizers *should* be placed under traditional export controls proved divisive. Some participants argued that the technology's rapid development and diffusion would render any such definitions obsolete and that the technology was vital to civilian research. Other participants retorted that the technology was too enabling to be left uncontrolled. They proposed to use a "sunset" clause stipulating that the export control entry would automatically expire after a set amount of time to force regulators to keep the entry up-to-date.

However, most participants from both sides of this discussion agreed that "soft" approaches should be attempted. Two specific proposals were made. First, law enforcement should conduct education and outreach to equipment manufacturers of DNA synthesizer and subcomponent and reagent suppliers if they had not yet done so. Second, the relevant industry groups should be encouraged to form a professional organization and adopt a code of conduct that included "know-your-customer" and record-keeping requirements in a similar fashion to what the DNA sequence service providers have done. In addition, some participants proposed that academic groups with gene synthesis capabilities be encouraged to join an existing industrial gene synthesis service provider association.

Other "soft" approaches were discussed, including various schemes requiring the registration of DNA synthesizers or where the underlying software came with certain security restrictions. The modest benefits and limitations of requiring the registration of DNA synthesizers had already been thoroughly described as early as 2007.[19] One benefit of this approach is that it would increase law enforcement visibility to the numbers and locations of synthesizers within their jurisdiction, which

[19] Michele S. Garfinkel, Drew Endy, Gerald L. Epstein, and Robert M. Friedman, "Synthetic Genomics: Options for Governance," J. Craig Venter Institute and Center for International and Strategic Studies, October 2007, pp. 35-36, 49 <http://www.jcvi.org/cms/fileadmin/site/research/projects/synthetic-genomics-report/synthetic-genomics-report.pdf> (accessed November 20, 2016).

would assist outreach planning. The major drawback is the additional cost in time and resources that registration entails for both researchers and enforcement personnel.

Some participants also wondered whether it would be possible to place restrictions on the software in DNA synthesizers so that the device's software would screen requested sequences against a clearing-house database and refuse to print DNA sequences associated with controlled pathogens. This approach is most likely infeasible. First, the government would need to create and maintain a suitable list against which to screen. This list could not simply be compiled by aggregating the lists used by gene synthesis service providers because, unlike the latter, it would need to be fully automated and could not rely on a human to interpret sequence annotations. Second, given the sizeable number of false positives reported by the existing gene sequence industry during their sequence screening activities, this approach would also severely limit the utility of the machines. That is, the machine would not be able to resolve false positives unlike the service providers' human review process. A conservative approach would significantly restrict the DNA sequences that the machine could print. Some participants thought that doing so would create a market for DNA synthesizers manufactured in countries where the government did not require such controls. Some participants pointed out that laboratories in developing countries depended on the acquisition of fully-capable DNA synthesizers because DNA synthesis services provided from out-of-country were prohibitively expensive. Third, ensuring that the screening took place against an up-to-date clearing-house database would presumably require that the synthesizer have an Internet connection, and doing so would open up large cyber-security risks.

3.3. High-throughput screening systems

Several working groups concluded that high-throughput systems are enabling platforms for the screening and design of pathogens and novel harmful chemicals of chemical warfare (CW) relevance.

One group noted that high-throughput systems themselves might be mostly composed of components that are relatively simple to manufacture. Therefore, export controls might be ineffective against proliferators with some machining capability and good engineers (i.e. state-level proliferators). However, the same group noted that there could still be some key subcomponent(s) that could be difficult to manufacture. They drew attention to the necessary optical read-out subsystem, the fluid control robotics, the throughput controls, and the underlying software as possibilities. In any case, even a machine that uses only simple-to-build subcomponents can nevertheless be difficult to assemble into a reliable whole, in which case placing the machine under export controls would remain useful.

Some participants suggested export controls on high-throughput assays that enable high-throughput screening for phenotypes of concern. They explained that what they had in mind went beyond

simple binding or toxin production assays and beyond deep tissue assays. These participants also called for the information related to the creation of high-throughput assays for "sophisticated" phenotypes of concern to be classed as Dual-Use Research of Concern (DURC).

3.4. Facility-wide production control software

Facility-wide production control software takes the various outputs from all of the equipment-specific sensors (such as temperature, pressure, pH, and flow rate sensors) in a production line and synthesizes and presents these on a control screen. Some participants noted that these greatly increased the safety and efficiency of industrial-scale production lines and thus warranted further discussion.

Currently this type of software does not appear to be under either AG or WA controls. That said, control software suites are presumably still captured under national export control "catch-all" clauses. Chemical and biological weapons (CBW)-interdiction relevant "catch-all" clauses stipulate that, if an exporter within the government's jurisdiction is aware or is made aware that the item they are attempting to export may be intended for use in connection with chemical or biological weapons activities, they then are obligated to inform and seek an export authorization from the national authorities – even if the item is not otherwise controlled for export.[20]

As with other software considered in section 3.7., most participants were reluctant to propose that software be subject to export controls because of unintended capture problems. Participants were especially concerned that hospital waste management and disinfection control software could be impacted. In considering hypothetical new list-based export controls, some participants considered whether a "specially designed for the production of pathogenic microorganisms" clause might be of use in limiting unintended capture. Others felt that this wording would be too restrictive and would allow loop-hole products. Some participants then proposed a "specially designed for medical use" carve-out clause, but such a clause would still leave other life-saving civilian applications at risk of unintended capture.

Participants emphasized that software was not necessary for BW agent production runs. Some participants further noted that specialized facility-wide production control software were also an issue for CW export controls.

Participants suggested that law enforcement agencies conduct outreach to companies that produce, sell, and install facility-wide production control software in the life sciences and chemical industries.

[20] US Department of State, "Catch-All Controls," 2011, <http://www.state.gov/strategictrade/practices/c43179.htm> (accessed November 23, 2016).

3.5. Human disease models

Some participants discussed the potential to place items used as infection models (e.g. laboratory animals) for human diseases under export controls. However, participants lacked the necessary commercial information to determine whether these had already diffused globally and were therefore poor candidates for controls. That is, some participants wondered whether, for a model to be recognized as a good infection model, it would first have to be widely studied and therefore be widely available. In addition, animals and certain animal-derived bioproducts are already export-controlled through public health and endangered animal species legislation.

3.6. Nano-packaging / microencapsulation

Nano-packaging involves the manipulation of particles at the molecular level to develop materials with novel, unique properties that address vexing packaging problems.[21] Several participants noted that these technologies posed security risks, but there was debate as to the feasibility of controls on these technologies. In addition, it was unclear whether AG controls on spray dryers sufficiently restricted these techniques, or whether common microencapsulation processes existed that could draw upon other pieces of equipment. Participants disagreed on the extent of the commercialization of this technology and therefore on the potential for export controls to be effective. Participants noted that microencapsulation equipment was already on the AG Awareness Raising list. The subject warrants further study, to include a survey of the industry.

3.7. Predictive software for genetic engineering

To start, several participants pointed out that free, public-domain software for DNA editing has been available for at least ten years.[22] In addition, public-domain databases exist with data on phenotypes of concern.

Other participants asserted that what they wanted to discuss was emerging, far more sophisticated, software that assists users in predicting the effects of genetic modifications. Several participants noted the potential for misuse of agent design software and predictive model software when coupled with databases containing data on phenotypes of concern. The development of this type of software

---

[21] Michael F. Cole and Lynn L. Bergeson, "FDA Regulation of Food Packaging Produced Using Nanotechnology," *Food Safety Magazine*, April/May 2006, <http://www.foodsafetymagazine.com/magazine-archive1/aprilmay-2006/fda-regulation-of-food-packaging-produced-using-nanotechnology/> (accessed November 20, 2016).
[22] Michele S. Garfinkel, Drew Endy, Gerald L. Epstein, and Robert M. Friedman, "Synthetic Genomics: Options for Governance," pp. 40.

has repeatedly been flagged as a dual-use advance at recent expert meetings.[23,24] As for the facility-wide production control software discussed in section 3.4 above, currently no organism design software appears to be under neither AG nor WA controls.

However, it should be noted that the utility of available and near-future prediction and other design assistance software remains highly dependent on the knowledge and know-how of the individuals using said software. Bioengineering workflows still rely on the use of multiple non-linked software suites.[25] For instance, a 2011 review article identified seven workflow stages, each of which involved the use of separate software.[26] Software specifically enabling end-to-end design of organisms is not yet available.

Participants were highly reluctant to suggest export controls for software on pragmatic grounds given the enormous risk of unintended capture that these would present. Some participants further opposed such a proposal on principle, and this was a more controversial point; these participants felt that export control mechanisms should not cover fundamental research tools. Other participants disagreed with this characterization of the software as "fundamental." One point of contention was whether there existed software add-ons or proprietary databases that were specific to research on phenotypes of concern and therefore could be considered sensitive products. Another point of contention was whether, even if such software suites were on the market now or might be commercialized in the near future, they would be sufficiently reliable or enabling to warrant controls.

Participants generally agreed that law enforcement outreach should be carried out to companies that produce and commercialize agent design software or otherwise sell design services. Doing so would ensure that the software vendors understood the dual-use nature of their products and therefore would be aware of their requirements under "catch-all" export control legislation. Outreach would also yield valuable insights into the industry and allow the latter's experts to provide their input on the subject.

---

[23] Biological Weapons Convention Implementation Support Unit, "Advances in enabling technologies," BWC/MSP/2012/MX/INF.1, June 11, 2012, pp. 12-14 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G12/611/26/PDF/G1261126.pdf?OpenElement> (accessed January 6, 2017).
[24] Biological Weapons Convention Implementation Support Unit, "Advances in science and technology related to the Convention," BWC/MSP/2013/MX/INF.1/Rev.1, August 19, 2013, pp. 10 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/625/24/PDF/G1362524.pdf?OpenElement> (accessed January 6, 2017).
[25] Samik Ghosh, Yukiko Matsuoka, Yoshiyuki Asai, Kun-Yi Hsin, and Hiroaki Kitano, "Software for systems biology: from tools to integrated platforms," *Nature Reviews: Genetics* 12, No. 12 (December 2011), pp. 821-832.
[26] Ibid, pp. 824. These were: data and knowledge management, data-driven network inference, deep curation, *in silico* simulation, model analysis, physiological modelling, and molecular interaction modelling.

3.8. Gene editing kits

Participants were in broad agreement that the term "kit" is undefined, that many basic "gene editing kits" were ubiquitous, and that the term "gene editing kit" is therefore far too broad to be useful for a discussion on export controls. A survey of existing commercial kit capabilities and their producers would be necessary before progress could be made on whether this item ought to be controlled in some manner. Some participants noted that enhanced reporting and monitoring of sales might be a worthwhile soft approach to implement should specific kits be determined to be particularly proliferation-enabling.

3.9. Selection media

One group of participants raised the possibility that specific, completely-formulated, selective growth media might have been developed or could be imagined that would facilitate the isolation and growth of specific dangerous pathogens, and so might be considered for controls. For ease of reference, the concept was summarized using the term "selection media." However, no participant was able to confirm that such media was sufficiently unique or posed sufficient additional risks to already-traded growth media to warrant novel controls. Given the limited timespan of the symposium and the novel nature of this suggestion, it was agreed that the topic warranted further study.

3.10. BioBrick parts

Some participants discussed the potential for misuse of BioBrick parts. BioBrick parts are documented DNA sequences that encode a particular function that can be readily combined with other BioBrick parts and therefore can in theory be used to engineer more complex biological systems.[27] The large number of existing harmless BioBrick parts would pose an extreme signal-to-noise ratio for detecting and then regulating potential dual-use BioBrick parts. In addition, the iGEM committee that maintains the BioBrick parts catalog already screens projects that generate new BioBrick parts to minimize their security risks.[28] For these reasons, participants concluded that controls were both undesirable and infeasible.

3.11. Disease mapping software and databases

Some participants considered disease mapping software (i.e. software that maps where diseases occur) and their underlying databases because these might enable proliferators to obtain pathogens from natural sources more easily. Participants generally felt that controls were both undesirable and

[27] iGEM, "Registry of Standard Biological Parts- Synthetic Biology" <http://parts.igem.org/Help:Synthetic_Biology> (accessed November 20, 2016).
[28] Kenneth Oye, Todd Kuiken, and Piers Millett, "iGEM Safety and Security Screening: A Testbed for Addressing Biosecurity Issues," March 28, 2012, pp. 1-4 <http://igem.org/Security> (accessed November 20, 2016).

infeasible. They deemed controls undesirable because these systems are of extreme importance for public health early warning, the security risk remains limited since a proliferator would still have to successfully harvest the desired pathogen, and because the underlying disease outbreak information is often already in the public domain. In addition, controls were felt to be infeasible because of the wide variety of disease tracking databases already available to the public.

3.12. DNA sequencers

Participants appeared to be in agreement that DNA sequencing equipment had already diffused to the point where a blanket control over DNA sequencing equipment was impractical. Participants also appeared to be in agreement that controls on DNA sequencers, even on some "high-technology" or "next-generation" subset, were not desirable. Several participants proclaimed that DNA sequencers were vital to the life sciences and to public health and noted that this equipment was not necessary for a BW program by emphasizing that DNA sequencers were simply tools that generated information. Therefore, participants felt that DNA sequencers were poor candidates for additional control and did not recommend any new hard or soft controls.

3.13. Lab-in-a-container setups / industrial biosynthesis lines

One working group noted that it could be possible and might be desirable to place the sale of advanced "lab-in-a-container" testing and/or production systems on the control list in the same way that entire BSL-3 and BSL-4 facilities and certain crucial subcomponents thereof are subject to controls.[29] Since the capability of greatest concern was judged to be high-throughput systems, gene synthesizers, or other high-technology equipment present within a "lab-in-a-container" setup, the question of controls over "lab-in-a-container" exports was reduced to that of whether to control the underlying pieces of equipment themselves (leading back to considerations listed above).

Several participants wondered whether to propose similar control mechanisms for whole biomanufacturing production lines for toxins or certain peptides of concern. These production capabilities are increasingly sought after to meet growing civilian markets for pharmaceutical and cosmetic products. The participants' question was whether the equipment necessary for these production lines was already controlled, as it was not clear whether these new industrial biosynthesis production lines lent themselves to the use of non-AG-controlled equipment. In the end, however, the participants decided not to propose new controls for two reasons. First, the non-AG equipment they thought might suffice to enable production was also thought to be too ubiquitous to be placed under controls. Second, for these lines to produce controlled toxins or peptides, a suitable seed

[29] Australia Group, "Control List of Dual-use Biological Equipment and Related Technology and Software," section I, subsection 1 a) and b).

culture is still required, and those already are controlled. Specifically, the AG's "genetic elements and genetically-modified organisms" clauses ensure that organisms modified to express controlled toxins or peptides are themselves controlled.[30]

3.14. CRISPR/Cas9

Many participants highlighted the serious security implications of CRISPR/Cas9 technology, which enables genomic editing of pathogens as well as the creation of malicious gene drives. CRISPR/Cas9 genomic editing depends on the ability to synthesize DNA (discussed in section 3.2.) and on kits to facilitate the insertion process (discussed in section 3.8.). As such, participants did not identify any non-ubiquitous pieces of equipment and consumables underpinning CRISPR/Cas9 genomic editing that had not already been considered for additional controls.

3.15. Antibody-drug conjugates (ADCs)

Some participants discussed the potential for misuse of ADCs, for instance as hypothetical assassination weapons if tailored against an individual using input from personalized medicine data. These participants felt that controls on ADCs were not desirable because the risk posed was remote; it would require cutting-edge research and development capabilities to design and validate such a hypothetical weapon. Current ADC production techniques rely on a slew of expensive equipment that – depending on their specifications – already may be controlled, such as high-containment rooms, protective suits with air supplies, and isolators.[31] In addition, delivery of simple ADC therapies relies on intravenous (IV) infusion;[32] participants generally agreed that an assassin that had this level of access to their target could rely on a myriad number of simpler ways to sicken or kill their intended victim. The general impression amongst participants was that a malicious actor with the capability to employ ADC techniques for malicious purposes would be unlikely to be impeded by dual-use export controls.

3.16. 3-D printers and bioprinters

Several working groups considered 3-D printers and 3-D bioprinters, also known as additive manufacturing equipment. Participants discussed the potential for 3-D printers to print controlled

---

[30] Australia Group, "List of Human and Animal Pathogens and Toxins for Export Control," August 2016, <http://www.australiagroup.net/en/human_animal_pathogens.html>; Australia Group, "List of Plant Pathogens for Export Control," June 2012, <http://www.australiagroup.net/en/plants.html> (accessed November 20, 2016).
[31] Cynthia Wooge, "Process Challenges of Antibody-Drug Conjugates," *BioProcess International*, June 1, 2014, <http://www.bioprocessintl.com/manufacturing/monoclonal-antibodies/process-challenges-of-antibodydrug-conjugates/> (accessed December 17, 2016).
[32] For an introduction to ADCs, see for example: Michael A. Firer and Gary Gellerman, "Targeted drug delivery for cancer therapy: the other side of antibodies," *Journal of Hematology & Oncology* 5 No. 70 (2012), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3508879/> (accessed November 20, 2016).

equipment[33] but noted that, even if a suitable 3-D printer could be secured, this would add yet another complex preparatory step to a proliferator's BW program. Ultimately, it was deemed that 3-D printers were likely to be regulated for other security reasons and that the biosecurity risks posed were insufficient to warrant BW-related controls.

Regarding 3-D bioprinters, participants concluded that highly dense assays for the printing of tissues were not uniquely enabling as other techniques could be employed to achieve the same effect.

3.17. Certified virus-free fertilized eggs

Some participants considered whether certified virus-free fertilized eggs were worth placing under increased controls. These can be used to propagate certain viruses through a process of inoculation and incubation. Several participants felt that these were not good candidates for export controls and noted that growth media was not export controlled by the AG. In addition, participants highlighted the lack of commercial information to determine how frequently such eggs were produced, traded, and used. However, participants saw no harm in recommending that governments should monitor exports of virus-free fertilized eggs through customs data for anomalies in quantities and destinations if this practice is not already commonplace.

4. General recommendations

In addition to the technology-specific findings reported above, participants elaborated six general recommendations:

4.1. Adjust the research grant system to reward dual-use risk minimization

Grant proposals for life sciences research projects should include a category on how researchers plan to minimize the dual-use risk posed by their proposed research. Doing so would reward researchers who already address dual-use security issues and provide a financial incentive structure in support of law enforcement education and outreach efforts. Some participants further suggested that research institutions should be requested to provide necessary dual-use risk assessment training as a condition of funding. Precedent for such practice exists. Certain government grants and certain journals already require scientists to declare and address dual-use implications of their proposed research or publication regardless of the pathogen studied. As another example, the organizers of the iGEM synthetic biology competition require participating teams to flag and minimize potential security concerns.[34] For security reasons, this requirement need not require a detailed account of how the scientist's proposed work might be misused, and the category could be covered under

[33] The maximum size of the 3-D printer places a technical constraint on a proliferator in this regard.
[34] iGEM, "Security" <http://igem.org/Security> (accessed November 20, 2016)

special security confidentiality guarantees to include exemption from public information access unless the experiment is approved and funded.

Participants were generally opposed to attempts to subject research results generated at civilian institutions to export-control mechanisms. Participants emphasized the conflict between any such controls and increasingly-strict scientific reproducibility requirements. Most participants felt that the only effective way to prevent sensitive research results from being "exported" was to ensure that research that posed serious security risks but generated findings that were of dubious gain to science or industry should not be conducted to begin with. The above recommendation emerged from this discussion. Some participants suggested that, should publication controls nevertheless become a common occurrence, governments should also ensure that a mechanism exists to share the research results with scientists that can demonstrate a "need-to-know."

4.2. Globalize "know-your-customer" policies as an ethical business norm

Governments and professional and industrial associations should promote the "know-your-customer" export control concept as a global norm of ethical businesses. Under a "know-your-customer" policy, the seller has a responsibility to take measures to ensure that a potential customer is who they say they are and that they are seeking a product for legitimate purposes. Participants felt that governments should work with industry and professional trade organizations so that this responsibility is accepted as a standard business practice throughout the world.

A company with a "know-your-customer" policy must be confident in its ability to explain who a would-be customer is, why the latter is seeking the specific transaction, and why the proposed order makes technical sense given the customer's usual business requirements. A company with a "know-your-customer" policy in place will:

- verify that the proposed purchase has none of the common signs of front procurement attempts ("red flags");[35]
- ensure that they do not "self-blind" by purposefully limiting the information asked of would-be customers in an effort to avoid detecting "red flags";
- actively seek out answers to "red flags" and subsequently re-evaluate the proposed purchase;
- either deny orders with unresolved "red flags," or seek appropriate governmental approval by providing all of the relevant information in the form of an export license request;
- contact law enforcement agents as appropriate; and

[35] Bureau of Industry and Security, US Department of Commerce, "Red Flag Indicators" <https://www.bis.doc.gov/index.php/enforcement/oee/compliance/23-compliance-a-training/51-red-flag-indicators> (accessed November 20, 2016).

- provide employees with governmental "hot-line" contact information that allows them, should they so wish, to anonymously report internal violations of this policy.[36]

4.3. Employ "sunset" clauses in cases of new biotechnology export controls

Should new export controls be considered that affect biotechnology, they would benefit from the inclusion of "sunset" clauses. "Sunset" clauses are clauses in regulations that stipulate that the regulation automatically expires after a set number of years unless it is re-approved. Sunset clauses have been used in export control lists before, notably by the WA.

Several participants expressed concerns that the extremely rapid rate of innovation in the life sciences would conflict with list-based biotechnology export controls that depend on technical specifications. For example, innovations that were cutting-edge items at the time a new regulation was adopted in one country might already have become commonly available in other countries. Further, it could be that items that are subject to controls might be superseded by new biotechnology products that possess similar or superior capabilities but would not be captured by existing control criteria. New civilian items could also become unwittingly and unnecessarily subjected to extant controls simply because of a shared mode of technical operation. At the same time, several participants highlighted that items deemed "obsolete" by regulators could still be of interest to proliferators and offered specific examples in support of this thesis. While participants were divided over whether to call for any new list-based biotechnology export controls, participants did not object to the idea of recommending sunset clauses if controls were inevitable.

4.4. Dedicate an export control working group to biotechnologies

Symposium participants noted that it would be valuable to have a dedicated biotechnology working group within a government's agency in charge of dual-use export control regulations. For instance, in the United States, the Bureau of Industry and Security has an Emerging Technology and Research Advisory Committee (ETRAC) that provides a line of communication for research and industry sector representatives to flag emerging security concerns including, but not limited to, biotechnology threats.[37,38] Participants agreed that life science researchers and bio-industrialists were likely to be the

[36] Adapted from: Bureau of Industry and Security, US Department of Commerce, "Know Your Customer Guidance" <https://www.bis.doc.gov/index.php/compliance-a-training/export-management-a-compliance/23-compliance-a-training/47-know-your-customer-guidance> (accessed November 20, 2016).
[37] Bureau of Industry and Security, US Department of Commerce, "BIS Technical Advisory Committees (TAC)" <https://tac.bis.doc.gov/> (accessed November 20, 2016).

first individuals to notice emerging security issues in their fields and that it therefore would be beneficial to provide them with a dedicated communications channel to contact government regulators. Several participants felt that the rapid growth of the biotechnology industry and the dual-use nature of the life sciences warranted the establishment of a dedicated committee or subcommittee on emerging biotechnology export control issues within government.

4.5. Amend customs classification codes and provide correlation tables

Symposium participants noted that governments should amend customs classification codes to better capture controlled BW-relevant exports and should provide correlation tables between customs classification codes and their national dual use control codes. Several participants observed that the existing World Customs Organization (WCO) "Harmonized System" item classification codes used by over 200 countries were ill-suited for tracking BW-relevant exports.[39] No clear-cut commodity code exists for well-known items such as fermenters, let alone for emerging biotechnologies. Proposals to amend the WCO codes have previously been proposed, but little progress has been made.[40]

Several participants highlighted the utility of the European Union's walk-through table that correlates the codes under the European Union's Harmonized Commodity Description and Coding System with those under the European Union's Control List of Dual-Use Items and lamented the fact that the United States lacked a similar table.

4.6. Globalize sequence screening practices

Symposium participants noted that governments should do more to internationalize security screening practices by gene synthesis companies. Because the number and complexity of sequence orders is increasing, and since security reviews of flagged sequences cannot be effectively automated, the cost of complying with voluntary industry standards for sequence order screening is steadily increasing. As a result, companies that do not abide by these industry standards have a growing

---

[38] Bureau of Industry and Security, US Department of Commerce, "US Department of Commerce Charter of the Emerging Technology and Research Advisory Committee," July 2, 2012, <https://www.bis.doc.gov/index.php/licensing/28-technology-evaluation/147-emerging-technology-and-research-technical-advisory-committee> (accessed November 20, 2016).

[39] On the WCO system, see: World Customs Organization, "What is the Harmonized System (HS)?" <http://www.wcoomd.org/en/topics/nomenclature/overview/what-is-the-harmonized-system.aspx> (accessed November 20, 2016).

[40] The Research Group for Biological Arms Control, "Trade monitoring for biological dual-use items" <http://www.biological-arms-control.org/projects_trademonitoring.html> (accessed November 20, 2016).

commercial advantage over those that do. Numerous participants highlighted the need for governments to do more to help internationalize this industry practice beyond companies in the US and EU markets so as to ensure a level commercial field.

Participants overwhelmingly held that the creation by industry of a voluntary security practice in the form of sequence screening was a positive development. Some participants were concerned that the growing negative financial impact of these practices on cooperative industry members would set a negative precedent across the wider biotechnology industry that responsibly addressing biosecurity implications was commercially unsustainable. At the same time, some participants noted that, if these voluntary practices collapsed, governments would likely make them mandatory. For instance, governments could legislate that orders filled or imported within their countries must be screened to a certain defined standard against a government sequence list consolidated from currently-used industry lists. While a government-issued list would perhaps reduce industry insurance liability costs and thus help reduce the costs of screening, it would also likely prove harder to update. These participants emphasized that it made good business sense for companies to work within the adaptable framework of self-imposed industry screening standards rather than run the risk of having to comply with ham-fisted regulations.

5. Other considerations

Participants highlighted some additional trends regarding the future of controls on emerging biotechnologies that are worth consideration. These are as follows:

- Compared to items currently controlled for BW-related interdiction reasons, most items considered at the symposium were highly sophisticated. Expertise within governments to ensure good governance is steadily increasing.
- Several participants noted that the clarity of an export control list was critical to facilitate company compliance, minimize the risk of unintended capture, and enable law enforcement action. A related point made by participants was that relying on sweeping export control clauses or relying on "catch-all" controls when formulating traditional export controls is far less desirable than coming up with explicitly-stated control criteria for specific items. As emerging biotechnologies considered for controls become increasingly complex, it is also becoming increasingly difficult to properly formulate specific control criteria.
- Because of the sophistication of the underlying emerging biotechnology equipment and services and because of the rapid pace of progress in the life sciences, list-based export controls can increasingly lead to unintended consequences. Even when symposium participants generally agreed that a biotechnology or associated service posed a medium to high biosecurity risk, symposium participants could not agree on the desirability (or lack

thereof) of placing it under export controls. This lack of consensus reflected general concerns that additional export controls, if poorly designed, could cause more harm than good.

- The rapid growth and globalization in the biotechnology equipment and services industries have made it increasingly difficult for analysts to evaluate the feasibility of potential new export controls and to ensure that existing controls remain up-to-date. Several participants expressed uncertainties regarding the existing markets for items considered at the symposium.
- Some participants held that the emerging biotechnologies and services that had been considered were, in their view, often fundamental research tools. They drew a distinction between several of the emerging technologies considered at the symposium and the items on the AG list, which is heavily comprised of equipment for the industrial production of pathogens. Whereas past export controls were focused on preventing states from being able to acquire the equipment and supplies necessary to develop and produce large quantities of BW agents, the international security community now has to grapple with preventing state and non-state actors from acquiring low quantities of genetically-engineered, "high-footprint," BW agents. This shift is reflected in the technologies discussed at the conference.
- Finally, several participants noted their belief that the format of the symposium lent itself to effectively addressing these challenges because it allowed experts from the necessary disparate fields to flag problems and collaborate on drafting potential solutions.

6. Acknowledgements

The planning committee for the IBPF 2016 export control symposium would like to acknowledge the following organizations and individuals:

- Twist Bioscience for sponsoring food and refreshments during the symposium.
- The James Martin Center for Nonproliferation Studies for hosting an opening reception and snacks and refreshments during the symposium.
- All symposium participants for their exceptional inputs on the challenging topic of emerging biotechnology export control.
- Ms. Edith Bursac for her excellent work solving all the logistic problems and issues that cropped up throughout the preparatory process and managing the symposium.

Appendix 1: List of participants

Addoum, Belgacem	Visiting Fellow (Morocco), James Martin Center for Nonproliferation Studies (CNS), Middlebury Institute of International Studies
Al Hmoud, Nisreen	Centre for Excellence in Biosafety, Biosecurity and Biotechnology, Jordan
Bates, Tom	Lawrence Livermore National Laboratory
Berke, Allison	Stanford Cyber Initiative
Berriman, Annette	Australia Group, Australia
Binz, Thomas	Federal Office of Public Health, Federal Department of Home Affairs, Switzerland
Bolling, Kellie	US Department of Energy
Breithaupt, Holger	European Molecular Biology Organization (*EMBO reports*), Germany
Carson, Michael	eBay Inc.
Casagrande, Rocco	Gryphon Scientific
Cavage, George	Intelyt (formally iControl Inc.)
Clevestig, Peter	Stockholm International Peace Research Institute (SIPRI), Sweden
Cluss, Robert	Middlebury College
Cui, Helen	Los Alamos National Laboratory
Diggans, James	Twist Bioscience
Evans, Samuel Weiss	Harvard/MIT
Fairchild, Steven	International Biosecurity and Prevention Forum (IBPF)
Friedman, Douglas	Engineering Biology Research Consortium
Friedman, Robert	J. Craig Venter Institute
Garrett, Laurie	Council on Foreign Relations

Giles, Kathie	International Biosecurity and Prevention Forum (IBPF)
Gronvall, Gigi Kwik	UPMC Center for Health Security
Hanselman, David	Synthetic Genomics Inc.
Hart, John	Stockholm International Peace Research Institute (SIPRI), Sweden
Hillson, Nathan	Joint BioEnergy Institute
Jackson, Paul	Middlebury Institute of International Studies (MIIS)
Jacobsen, Kirsten	iGEM Pathogen Risk Assessment, Canada
Jaeil, Jo	Strategic Trade Institute (KOSTI), South Korea
Jain, Nitin Kumar	Department of Biotechnology, Ministry of Science & Technology, India
Jeremias, Gunnar	University of Hamburg, Germany
Kebede, Adisu	Public Health Institute, Ethiopia
Kennedy, Caroline	International Biosecurity and Prevention Forum (IBPF)
Kingiri, Ann	African Centre for Technology Studies, Kenya
Kosal, Margaret	Georgia Institute of Technology
Kouts, Jodi	US Department of Commerce
Lee, Betty	US Department of Commerce
Loh, Tyng	Genentech
Martin, Eric-Andre	Bureau of export control of dual-use goods, Ministry of the Economy, France
Mauger, Philippe	James Martin Center for Nonproliferation Studies (CNS), Middlebury Institute of International Studies
McPeak, John	Genentech
Millett, Piers	Biosecure Ltd., UK
Morrow, Naomi	US Department of Commerce

Moudden, Nasser	Visiting Fellow (Morocco), James Martin Center for Nonproliferation Studies (CNS), Middlebury Institute of International Studies
Palmer, Megan	CISAC, Stanford University
Ringel, Brooke	Kelley Drye & Warren LLP
Roffey, Roger	Swedish Defense Research Agency (FOI), Sweden
Russell, Jonathan	International Biosecurity and Prevention Forum (IBPF)
Savage, Todd	International Biosecurity and Prevention Forum (IBPF)
Selgelid, Michael	Monash University Center for Human Bioethics, Australia
Shaw, Robert	James Martin Center for Nonproliferation Studies (CNS), Middlebury Institute of International Studies
Souza, Drew	US Department of State
Spector, Leonard S.	James Martin Center for Nonproliferation Studies (CNS), Middlebury Institute of International Studies
Stewart, Andy	CISAC, Stanford University
Tan, George	Global Trade Security Consulting, Singapore
Tearney, Ronald	GE Healthcare
Thomsen, Roszel (Roz)	Thomsen & Burke LLP
Valles, Edith	Institute of Scientific and Technical Research for Defense, Ministry of Defense, Argentina
Weber, Andrew	Harvard Kennedy School's Belfer Center for Science and International Affairs; Metabiota
Weith, Nils	Division VB4, Federal Ministry for Economic Affairs and Energy, Germany
Zilinskas, Raymond	James Martin Center for Nonproliferation Studies (CNS), Middlebury Institute of International Studies

Appendix 2: Glossary

Additive manufacturing — the manufacture of a three-dimensional product by applying successive, thin, layers of material. See also: 3-D printer and 3-D bioprinter.

AG — Australia Group

ADCs — Antibody-drug conjugates, which are a drug payload system composed of a drug chemically attached to a monoclonal antibody; ADCs are used in medicine for targeted drug delivery.

BioBrick parts — DNA sequences of defined structure and function that can be readily combined with other BioBrick parts. The goal of the BioBricks project is the creation of a large catalog of BioBricks that enables the reliable engineering of more complex biological systems.

Bioregulators — chemical substances secreted by glands in animals that regulate biological processes such as neural responses and blood pressure.

Biosafety practices — precautions and preventive measures that reduce the risk posed by accidents or natural exposure to biological materials or life forms.

Biosecurity practices — precautions and preventive measures that reduce the risk posed by deliberate exposure to biological materials or life forms.

Biotechnology — a collection of processes and techniques to harness living organisms, and products derived from these organisms, for agricultural, industrial, or medical purposes.

BSL-1–BSL-4 — a four-tier biosafety level (BSL) ranking system for laboratories. BSL-1 laboratories have the lowest level of containment and BSL-4 the highest.

BW — biological warfare

BWC — Biological and Toxin Weapons Convention of 1972

"Catch-all" controls related to CBW-interdiction — a legal-regulatory provision requiring exporters to obtain government permission prior to the export of any unlisted item (e.g. an item not on a "control list" of items specifically identified as "export-controlled" and thus requiring an export license) if the exporter knows or has reason to know that the item is intended to support a WMD-related end-use.

CRISPR-Cas9 — a genome editing technique developed in 2009 on the basis of the CRISPR-Cas bacterial defense mechanism.

CW — chemical warfare

CWC — Chemical Weapons Convention of 1993

Database — an organized collection of data packaged within a framework enabling its access.

DNA — deoxyribonucleic acid (DNA) is the carrier of genetic information found in all living organisms (except for a small group of RNA viruses). Every inherited characteristic is coded somewhere within an organism's complement of DNA.

DNA sequencing — a procedure for determining the nucleotide sequence of a DNA fragment.

DNA synthesizer — the building of a known sequence of nucleotides into an oligonucleotide, or DNA.

Dual-use — equipment or research that has civilian applications but that can also be diverted to a military end-use.

DURC — Dual-use research of concern; a US government term used in texts establishing oversight of dual-use research in the life sciences, defined as "life science research that, based on current understanding, can be reasonably anticipated to provide knowledge, information, products, or technologies that could be directly misapplied to pose a significant threat with broad potential consequences to public health and safety, agricultural crops and other plants, animals, the environment, materiel, or national security."[41]

Fermenter — a vessel within which bacteria. fungi, cell extracts, or enzymes are made to undergo biological reactions (alternatively called a bioreactor).

Gene — the fundamental unit of heredity. A gene is a segment of ordered nucleotides that codes for a specific product or control a specific function.

Genome — an organism's complete set of genes and chromosomes.

High-throughput systems — these are automated systems designed to process large numbers of assays, especially in the context of genotyping.

iGEM — the International Genetically Engineered Machine Foundation (iGEM). iGEM is a nonprofit organization that, amongst other activities, runs the international synthetic biology student team iGEM Competition and maintains the Registry of Standard Biological Parts used to document BioBrick parts.[42]

Kit — a package that contains instructions and premeasured chemicals designed to facilitate a specific genetic engineering project.

"Lab-in-a-container" — a design concept harnessing advances in robotics and equipment miniaturization to achieve a contained, fully automated, laboratory that can be remotely tasked with experiments.

---

[41] National Institutes of Health, Office of Science Policy, "Biosecurity: Dual Use Research of Concern" <http://osp.od.nih.gov/office-biotechnology-activities/biosecurity/dual-use-research-concern> (accessed November 23, 2016).

[42] iGEM, "Synthetic biology based on standard parts" <http://igem.org/Main_Page> (accessed November 22, 2016).

Microencapsulation — a process whereby microorganisms are coated with a continuous film of protective material designed to protect the organism from stressful environmental forces.

Micron — one millionth of a meter. A human hair is roughly 100 microns in diameter.

Nucleotide — the fundamental molecule that makes up DNA and RNA. Each nucleotide constituting DNA consists of one of four nucleic acids (adenine, guanine, cytosine or thymine) linked to the phosphate-sugar group deoxyribose. Each nucleotide constituting RNA consists of one of four nucleic acids (adenine, guanine, cytosine or uracil) linked to the phosphate-sugar group ribose.

Oligonucleotides — short DNA molecules, usually containing fewer than 100 bases.

Peptide — a linear polymer of two or more amino acids. Peptides are similar to proteins but smaller. Small molecules that can be synthesized by joining individual amino acids are, by convention, called peptides rather than proteins. The dividing line is at about 50 amino acids; i.e., if the polymer contains fewer than 50 amino acids it is a peptide, if more, it is a protein.

Proliferator (in the BW context) — an entity, be it a nation or a subnational group, that is intent on acquiring a biological warfare program.

"Red flags" in export controls — an indication, within a proposed business transaction, of an attempt to illegally acquire and divert goods, software, and/or technology in contravention to export control and sanctions-related laws and regulations.

Synthetic biology — a relatively new discipline that merge the biological sciences and engineering. By doing so, it is possible to re-design natural biological systems for greater efficiency, as well as the design and assembly of functional genetic circuits and metabolic pathways for a variety of applications.

3-D printer — a device that successively prints thin layers of manufacturing material to assemble an object based on instructions provided by a digital three-dimensional model file.

3-D bioprinter — a 3-D printer that uses different kinds of cells as the manufacturing material and can therefore be used to assemble tissues.

Toxin — a poisonous chemical produced by a living organism.

WA — Wassenaar Arrangement

WCO — World Customs Organization

OCCASIONAL PAPERS AVAILABLE FROM CNS

online at http://nonproliferation.org/category/topics/cns_papers

***#33* Evaluating WMD Proliferation Risks at the Nexus of 3D Printing and Do-It-Yourself (DIY) Communities**
Robert Shaw, Ferenc Dalnoki-Veress, Shea Cotton, Joshua Pollack, Masako Toki, Ruby Russell, Olivia Vassalotti, Syed Gohar Altaf • 2017

***#32* Taiwan's Export Control System: Overview and Recommendations**
Melissa Hanham, Catherine Dill, Daniel Salisbury, P. Alex Kynerd, Raymond Wang • 2017

***#31* Revisiting Compliance in the Biological Weapons Convention**
James Revill • 2017

***#30* Crowdsourcing Systems and Potential Applications in Nonproliferation**
Bryan Lee • 2017

***#29* The Verification Clearinghouse: Debunking Websites and the Potential for Public Nonproliferation Monitoring**
Bryan Lee, Kyle Pilutti • 2017

***#28* Geo4nonpro.org: A Geospatial Crowd-Sourcing Platform for WMD Verification**
Melissa Hanham, Catherine Dill, Jeffrey Lewis, Bo Kim, Dave Schmerler, Joseph Rodgers • 2017

***#27* Searching for Illicit Dual Use Items in Online Marketplaces: A Semi-Automated Approach**
Bryan Lee, Margaret Arno, Daniel Salisbury • 2017

***#26* 2016 Symposium Findings on Export Control of Emerging Biotechnologies**
Steven Fairchild, Caroline R. M. Kennedy, Philippe Mauger, Todd J. Savage, Raymond A. Zilinskas • 2017

***#25* Outlawing State-Sponsored Nuclear Procurement Programs & Recovery of Misappropriated Nuclear Goods**
Leonard S. Spector • 2016

***#24* Strengthening the ROK-US Nuclear Partnership**
Miles A. Pomper, Toby Dalton, Scott Snyder, Ferenc Dalnoki-Veress • 2016

***#23* Replacing High-Risk Radiological Materials**
George M. Moore, Miles A. Pomper • 2015

***#22* A Blueprint to a Middle East WMD Free Zone**
Chen Kane, PhD • 2015

***#21* Biotechnology E-commerce: A Disruptive Challenge to Biological Arms Control**
Raymond A. Zilinskas, Philippe Mauger • 2015

***#20* Countering Nuclear Commodity Smuggling: A System of Systems**
Leonard S. Spector, Egle Murauskaite • 2014

***#19* Alternatives to High-Risk Radiological Sources**
Miles Pomper, Egle Murauskaite, Tom Coppen • 2014

***#18* Stories of the Soviet Anti-Plague System**
Casey W. Mahoney, James W. Toppin, Raymond A. Zilinskas, eds. • 2013

***#17* Ugly Truths: Saddam Hussein and Other Insiders on Iraq's Covert Bioweapons**
Amy E. Smithson, PhD • 2013

***#16* Rethinking Spent Fuel Management in South Korea**
Ferenc Dalnoki-Veress, Miles Pomper, Stephanie Lieggi, Charles McCombie, Neil Chapman • 2013

Older Papers

#15 Engaging China and Russia on Nuclear Disarmament • *2009*

#14 Nuclear Challenges and Policy Options for the Next US Administration • *2009*

#13 Trafficking Networks for Chemical Weapons Precursors: Lessons from the 1980s Iran-Iraq War • *2008*

#12 New Challenges in Missile Proliferation, Missile Defense, and Space Security • *2003*

#11 Commercial Radioactive Sources: Surveying the Security Risks • *2003*

#10 Future Security in Space: Commercial, Military, and Arms Control Trade-Offs • *2002*

#9 The 1971 Smallpox Epidemic in Aralsk, Kazakhstan, and the Soviet Biological Warfare Program • *2002*

#8 After 9/11: Preventing Mass-Destruction Terrorism and Weapons Proliferation • *2002*

#7 Missile Proliferation and Defences: Problems and Prospects • *2001*

#6 WMD Threats 2001: Critical Choices for the Bush Administration • *2001*

#5 International Perspectives on Ballistic Missile Proliferation & Defenses • *2001*

#4 Proliferation Challenges and Nonproliferation Opportunities for New Administrations • *2000*

#3 Nonproliferation Regimes at Risk

#2 A History of Ballistic Missile Development in the DPRK • *1999*

#1 Former Soviet Biological Weapons Facilities in Kazakhstan: Past, Present, and Future • *1999*

nonproliferation.org

Middlebury Institute *of*
International Studies at Monterey
James Martin Center for Nonproliferation Studies