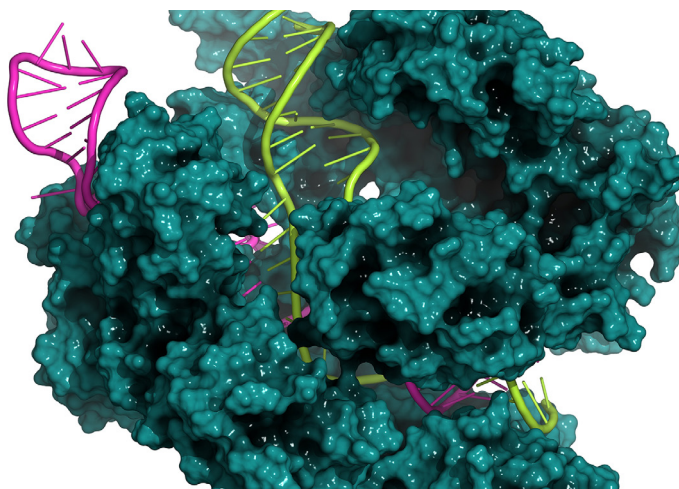


Double Helix, Dual-Use

Securing Synthetic Biological Laboratories

Hali | Czosnek



Brief No. 9.3

The Project on International Peace and Security © 2017
All rights reserved.

Please direct inquiries to:
The Project on International Peace and Security (PIPS)
Institute for the Theory and Practice of International Relations
The College of William and Mary
427 Scotland Street
Williamsburg, Virginia 23185
tele. 757.221.1441
fax. 757.221.4650
pips@wm.edu

Electronic copies of this report are available at www.wm.edu/pips

The Project on International Peace and Security

Launched in 2008, the Project on International Peace and Security (PIPS) is an undergraduate think tank based at the College of William and Mary. PIPS represents an innovative approach to undergraduate education that highlights the value of applied liberal arts training to producing the next generation of foreign policy analysts, leaders, and engaged citizens.

PIPS is premised on two core beliefs: (1) rigorous policy-relevant research is a core component of a student's education; and (2) when guided by faculty and members of the foreign policy community, undergraduates can make meaningful contributions to policy debates; their creativity and energy are untapped resources. To this end, PIPS each year selects six research fellows and six research interns. Research fellows identify emerging international security challenges and develop original policy papers. Research interns support the work of the fellows and learn the craft of conducting policy research and writing briefs.

For more on PIPS, visit www.wm.edu/pips.

Amy Oakes
Dennis A. Smith
Co-directors

Double Helix, Dual-Use
Securing Synthetic Biological Laboratories

APRIL 2017

Hali Czosnek

Double Helix, Dual-Use

Securing Synthetic Biological Laboratories

The rapid growth of gene-editing technology, combined with lapses in laboratory safety, risks exposing people to viruses that standard protocols cannot contain and vaccines cannot fight. The potential proliferation of genetically modified viruses requires the United States to secure domestic and foreign laboratories that have access to both pathogens and gene-editing technology, thereby applying its knowledge of securing nuclear and biological weapons to address this new challenge. By physically securing laboratories and standardizing laboratory safety training, the United States can preempt deadly pandemics.

Introduction

The combination of gene-editing technology and dangerous pathogens could spur international pandemics. This threat looms larger as gene-editing technology proliferates, because the misuse of dual-use techniques will grow.¹ Expanding the Nunn-Lugar Global Program is a first step to mitigating the risk of pathogen-editing. The Program can physically secure laboratories and standardize laboratory safety protocols to prevent an accidental or intentional security breach. By securing laboratories that contain gene-editing technology and pathogens, the security threat is addressed, while allowing private individuals and educational institutions continued access to beneficial gene-editing technology.

Gene Editing Technology: A Proliferation Problem

“You’ve got Fortune 50 companies fighting with start-ups fighting with universities. That almost never happens. But with CRISPR, the range of potential uses is so huge — everybody wants in.”

— Rodolphe Barrangou, Biologist at North Carolina State University, 2015²

Pathogen-splicing projects will continue to grow as technology becomes more affordable and accessible. One popular virus-editing technology is CRISPR-Cas9, because it is accurate, low cost, and easy to use. CRISPR, as a result, has become ubiquitous within synthetic biological research.³

Investment-growth field

The global CRISPR-Cas9 market is projected to be worth more than \$1.5 billion by 2022.⁴ The United States, therefore, will likely see an increase in dual-use research projects both domestically and abroad.

- *Utility of CRISPR-Cas9.* CRISPR allows scientists to identify and cut the region of a pathogen that they wish to alter.⁵ The ability to edit the genome at any site lets CRISPR rewrite entire genes, changing the functions of the cells themselves. CRISPR has become so indispensable that scientists use CRISPR-modified genomes to treat aggressive cancers. In November 2016, scientists at Sichuan University used CRISPR to edit a human genome that was later inserted back in a patient suffering from lung cancer.⁶
- *Accessibility of pathogen-editing technology.* Gene-editing technology will continue to proliferate and become more affordable, decreasing barriers to entry. Private companies now are providing gene-editing technology online at low costs, increasing access. Because of the rise in accessibility, non-scientists can now use this technology outside of labs and without supervision.⁷
- *Gene-editing proliferation.* Gene-editing technology will continue to proliferate because of its range of uses in different fields of research. As CRISPR and similar technologies become more widely available, scientists produce modified viruses in laboratories. The number of amateur scientists working with the gene-editing technology will also increase.⁸ For example, undergraduate students at the University of Colorado-Denver use CRISPR in Molecular Biology class to edit the genomes of cells, and high school students worldwide used CRISPR as part of an annual synthetic biology competition.⁹ While the techniques and expertise needed to create a deadly virus using CRISPR are beyond the capabilities of a lay biologist, the proliferation of CRISPR increases the likelihood that the technology will fall into the wrong hands.¹⁰

The proliferation of gene-editing technology alone does not pose a serious threat to American security.¹¹ The security threat arises when gene-editing technology is combined with dangerous pathogens in poorly secured laboratories. The more gene-editing technology becomes available, an accidental security lapse becomes increasingly likely.

Splicing Pathogens: A Security Threat

Pathogen-editing technology, combined with access to pathogens, poses serious threats to the United States' domestic and transnational security interests.

- *Poor laboratory procedures.* Procedural failures in U.S. laboratories pose a serious threat to the American public.¹² Between 2003 and 2015, investigators at the U.S. Government Accountability Office (GAO) found that 21 labs had failed to report laboratory incidents involving highly dangerous pathogens.¹³ A few of these incidents related to incomplete inactivation of pathogens that pose a severe threat to human health.¹⁴ If these inactivated viruses are sent between laboratories, anyone involved in their transportation could have been infected without their knowledge.¹⁵ Currently, no vaccines exist to protect the public against modified pathogens. The unknown effects of modified pathogens on humans suggest that traditional pandemic protocols will not work.¹⁶

- *Genetically modified pathogens.* Gene-editing technology allows scientists to transform previously treatable strains of bacteria into deadlier, antibiotic-resistant strains. On January 15, 2017, American news outlets reported that a woman in her seventies died from a bacteria resistant to the 26 antibiotics currently available in the United States.¹⁷ American health officials warn that this incident will happen again. The risk of antibiotic resistance would have been even greater if the infection had involved a genetically modified bacteria that would certainly have been resistant to all antibiotics. Antibiotics are the United States' first and last defense against bacterial infection, making prevention of a laboratory security breach the United States' only option.
- *Deadlier pandemics.* There is growing interest in research that focuses on genetically modifying diseases to understand how pathogens could evolve in the future. Scientists are modifying H5N1 to make the virus airborne and transmissible between humans; this practice allows a epidemiologists to predict how future H5N1 outbreaks could affect human health. Epidemiologists hypothesize that a pandemic version of avian flu (H5N1) has a 60 percent case fatality rate.¹⁸ Thus, a modified strain of H5N1 has the potential to kill over half of the world's population.¹⁹ Importantly, the United States does not have any vaccines, medication, or public health protocols to control a pandemic resulting from such an edited virus.²⁰
- *Damaging the food supply.* Scientists are modifying pathogens that can be used to target crops or animals. If a modified pathogen is introduced into the food system, the United States would not be able to control the spread of the disease within the agricultural industry. Should a modified pathogen be used to infect a livestock population, the agent would cause higher death rates among animals, and the pathogen could potentially infect human consumers. In 2010, for example, an accidental release of anthrax spores from a Ugandan laboratory infected the local hippopotamus population. This outbreak led to the deaths of four people who consumed the infected meat.²¹

The domestic and international threats from modified pathogens must be addressed. The current policy framework, however, is insufficient and requires clearer laboratory security standards for physical security and personnel training.

Current Policy: A Focus on Biological Weapons

"We can't wait for the bugs to spread."

—Senator Richard Lugar, 2010²²

Current policy on pathogens and gene-editing research focuses on the potential weaponization of biological research. These policies are an ineffective patchwork of consensus-based export control agreements and weakly-enforced biological weapons treaties.

Patchwork of international policies

The current approach to managing pathogens is a patchwork of international policies. Chief among these policies are the Wassenaar Arrangement and the Biological Weapons Convention (BWC). The Wassenaar Arrangement manages export controls, while the BWC monitors production and stockpiling of biological agents and focuses on countering threats from state and non-state actors trying to develop or use a biological weapon.²³

- *Informal export control arrangements.* The Wassenaar Arrangement functions as an export control group for dual-use technology among 41 countries predominantly located in North America and Europe.²⁴ This non-binding, voluntary arrangement monitors the transfer of dual-use goods and technologies to non-Wassenaar members, ensuring no single state accumulates dual-use technology. Enforcement and monitoring of commitments is costly. Due to the Arrangement's informal nature, enforcement is not a priority. Wassenaar thus fails to address the security threat of gene-editing technology paired with access to naturally occurring pathogens.
- *Ineffective agreements with weak verification.* The Biological Weapons Convention is the first multilateral treaty that prohibits the “development, production and stockpiling of weapons of mass destruction.”²⁵ While a more robust alternative to the Wassenaar Agreement, the BWC lacks a thorough verification mechanism for monitoring state compliance with the treaty.²⁶ The weaknesses of the Convention's framework and its failure to address pathogen-editing research conducted in laboratories renders the BWC an incomplete policy to address current biosecurity threats.²⁷

The existing policies that manage biological agents are informal and difficult to enforce. These policies do not address the proliferation of gene-editing technology and pathogen access. Future approaches must recognize these threats and work to prevent the release of modified pathogens.

The United States: The Silver Standard for Laboratory Security

The United States currently represents the best model for laboratory security as it publicly reports facility breaches. While accidents can go unreported, greater transparency offers the potential to improve upon existing standards to decrease future security failures.

- *Reporting failures.* There is no official international ranking of countries with the best laboratory security. Many governments refuse to disclose major lapses and, in some cases, any lapses in laboratory security. Without government recognition of security breaches, these failures are not subject to public scrutiny that could produce improved laboratory security. The United States, however, has a record of acknowledging failures in laboratory security and working towards improvements.²⁸
- *A Need for Better Standards and Training.* While the United States sets the silver standard in laboratory security, there are still shortcomings. Many accidents result from complacency within these laboratories, which is due to a lack of centralized oversight from

the federal government. However, reports on U.S. laboratory security breaches and plans to remedy them are steps yet to be taken globally.²⁹ CDC laboratory technicians and scientific researchers never handled pathogens during training and only came into contact with dangerous substances when they first stepped into the lab.³⁰ Training is underemphasized within major health research organizations, like the Center for Disease Control (CDC). Former CDC employees have criticized the federal organization for a fragmented training program that is primarily conducted online.³¹

The lack of international laboratory security standards points to the need for a gold standard in laboratory safety. While the U.S. system is imperfect, “laboratory security” in many countries consists of padlocked fridges.³² The United States can use its experience in laboratory security to help standardize global physical security and laboratory training protocols.

Pandemic Prevention: Nunn-Lugar Revisited

The lack of global standards for laboratory security means that an accidental or intentional release of a modified pathogen from a laboratory would have serious international health implications. The following recommendations represent the first steps to curb the threat of modified pathogens stored in poorly secured labs worldwide. Nunn-Lugar Global Program is the best means of delivering laboratory security and standardized training to biotechnology facilities. It provides a framework for bilateral partnerships through which Nunn-Lugar could expand its current framework to physically secure laboratories and standardize laboratory safety training.

Building on Nunn-Lugar Global Program

Recent increases in Nunn-Lugar Global Program’s budget for biological threat reduction via the Cooperative Biological Engagement (CBE) program demonstrate a pre-existing commitment within Nunn-Lugar to biological threat reduction.³³ The proposed upgrades to the Nunn-Lugar Global Program further strengthen the program’s historically successful operations.

- *Securing Soviet loose nukes.* Senators Sam Nunn and Richard Lugar originally created the Nunn-Lugar Global Program to counter the threat from “loose nukes” in the Soviet Republics following the disintegration of the former Soviet Union (FSU).³⁴ Specifically, the senators feared that Ukraine, Kazakhstan, and Belarus would become safe havens for terrorists who could access unsecured nuclear weapons. These terrorists could take advantage of the fluid security environment to use nuclear weapons for attacks inside and outside the FSU.³⁵

The Nunn-Lugar Global Program successfully dismantled the nuclear capabilities of Ukraine, Kazakhstan, and Belarus. The program retrofitted biological weapons laboratories in the FSU with enhanced physical security measures to prevent dangerous actors from accessing weapons laboratories.³⁶ In addition to physically securing former weapons

facilities, the Nunn-Lugar Global Program retrained Soviet nuclear weapons scientists to use their knowledge for peaceful purposes.³⁷

- *Securing Weapons of Mass Destruction outside of the Former Soviet Union.* In 2003, Congress passed the Nunn-Lugar Expansion Act enabling the Nunn-Lugar Global Program to partner on a bilateral basis with states outside of the FSU to secure nuclear, biological, and chemical materials.³⁸ Nunn-Lugar Global Program’s successful adaptation to counter emerging nuclear, biological, and chemical threats in the early 2000s demonstrates the program’s suitability for further expansion. It could expand to include the areas of laboratory safety, dual-use research, and pathogen-editing technology.
- *Mitigating Biological Threats.* The Cooperative Biological Engagement Program (CBE), established through Nunn-Lugar, works bilaterally with partner countries to mitigate biological threats. Specifically, the CBE addresses biosecurity threats of select traditional agents and potentially pandemic pathogens.³⁹ CBE works with partner countries to improve the biosafety and security of laboratories working with select agents.⁴⁰ Recently, the United States partnered with the Philippines, Indonesia, and Thailand to secure biological research facilities. These successful partnerships indicate the growing demand for securing laboratories conducting biological research and an increased U.S. commitment to achieve this objective.⁴¹ In addition to its work in Asia and the Middle East, the Nunn-Lugar Global Program is working with CBE in Uganda and Kenya to improve biosecurity in the face of regional terror threats.⁴²

The Nunn-Lugar Global Program’s prior experience enhancing security within the former Soviet Union, and more recently in East Africa and Southeast Asia, demonstrates its capacity to secure facilities conducting pathogen-editing research.

Nunn-Lugar Global Program Revisited

“With nuclear weapons you’d think you would stop after killing 100 million. Smallpox won’t stop. Because the population is naïve, and there are no real preparations. That, if it got out and spread, would be a larger number [of deaths].”

— Bill Gates, 2017⁴³

Nunn-Lugar’s CBE program could be extended to physically secure laboratories and standardize laboratory safety training with partner countries. The expanded program could prevent accidental or intentional security breaches that could result in deadlier pandemics.

Recommendation 1: Physically secure laboratories

A necessary first step to prevent the release of a pandemic pathogen is to physically secure government laboratories within Nunn-Lugar Global Program partner countries. Securing these government laboratories is essential to mitigating the possibility of biological agents

intentionally or accidentally exiting regulated spaces.⁴⁴ Once these facilities are physically secured, the United States could pass on the majority of maintenance costs to the partner country.⁴⁵ The proposed policy would not alter the budget of the Nunn-Lugar Global Program itself. Rather, it would require the CBE program to adjust its program budget in order to implement vital prevention measures.⁴⁶

Past criticism has targeted the use of nuclear models to secure biological weapons. This criticism is due to fundamental differences between nuclear and biological material, both in terms of availability and usage.⁴⁷ Biological materials are more readily available and less regulated than nuclear materials.⁴⁸ Their wide availability makes controlling access to such materials for weapons purposes difficult.⁴⁹ However, extensive tacit knowledge is required to build a usable biological weapon. Policy emphasis should be placed on securing government laboratories that conduct gene-modification research using pathogens, rather than emphasizing the accessible nature of biological material as the main issue. As gene-editing technology proliferates, and modification techniques simplify to the point that tacit knowledge is no longer a barrier, controlling access to biological material may become a security concern which policies twenty years from now should address.

Future policy in the next decade requires expanding physical security and standardized training protocols to civilian laboratories. Expansion to civilian laboratories will require cooperation among foreign and domestic actors in order to effectively target these laboratories. Future policymaking will be necessary to secure civilian laboratories in addition to the government-run laboratories that the expanded Nunn-Lugar program targets.

Recommendation 2: Standardize laboratory personnel training

An expanded Nunn-Lugar Global Program could provide standardized, in-person training to scientists working in laboratories capable of editing viruses.⁵⁰ Standardization reduces the need for continued education and increases the efficiency of training and personnel management within laboratories.⁵¹

The standardized Nunn-Lugar Global Program training program could work within domestic and foreign laboratories to provide uniform in-person training, reducing the probability of a security breach. Nunn-Lugar Global Program's success in both physically securing facilities and training former weapons scientists demonstrates that it is the best vehicle for standardizing laboratory training in synthetic biology laboratories.⁵²

The United States could provide both on-site training and publish security standards and laboratory manuals for Nunn-Lugar partner countries. Laboratory workers trained through the expanded Nunn-Lugar training program can later train new employees using the standardized protocols developed in the manuals. This training framework creates an enduring and cost-effective standardized training program.

Conclusion

Gene-splicing technology is moving beyond the walls of controlled laboratory environments into private, unregulated spaces. CRISPR will become more accessible to the average individual with a few hundred dollars to spend. CRISPR's accessibility to non-scientists, however, poses little threat to U.S. security. The potential for a catastrophic event, however, soars as biological laboratories obtain both gene-editing technology and pathogens. In the face of weak domestic and international lab security, the United States could physically secure laboratories in order to prevent accidental or intentional releases of genetically modified pathogens.

The Nunn-Lugar Global Program could be expanded to physically secure synthetic biological laboratories and implement standardized laboratory training protocols. The Nunn-Lugar Global Program has the requisite experience to secure existing laboratories and train scientists in standardized protocols. The proposed expansion to the Program requires an upfront financial investment for physically securing laboratories and providing standardized in-person training. Following the initial cost, ongoing security and training efforts can be left to the partner laboratory, freeing the United States of additional or unforeseen costs.

The expanded Nunn-Lugar Global Program is the United States' best and least costly option for preventing the accidental or intentional misuse of genetically-modified viruses. Biological warfare may be inevitable by 2035, and the United States can never be too early or too prepared to prevent a possible attack.⁵³ The only way for the United States to guard against a pandemic of epic proportions is to prepare for it today; these preparations begin with an upgraded Nunn-Lugar Global Program.

¹ Recent advancements in synthetic biology have enabled scientists to make precise alterations to genomes of living cells. A subfield of synthetic biological is gain of function (GOF) research, which uses gene-editing technology to make pathogens more lethal. GOF research is dual-use because it can be used to advance scientific discovery or harnessed as a weapon. For example, widely available gene-editing technology can help to eradicate infectious diseases and cure cancer. However, gene-editing can also be used to make pathogens more lethal which increases the potential for pandemics. As the technology continues to proliferate, the risk of accidental or intentional misuse of gene-editing technology grows.

² Jennifer Kahn, “The Crispr Quandary,” *New York Times*, November 9, 2015, <https://www.nytimes.com/2015/11/15/magazine/the-crispr-quandary.html>.

³ For the purposes of this paper, all references to CRISPR refer to the CRISPR-Cas9 system. There are several CRISPR-Cas systems, distinguished by the signature gene and protein they use. CRISPR-Cas9 is the fastest growing gene-editing technique within the CRISPR-Cas family because it is cheaper and easier to use than other systems.

⁴ “Global CRISPR/Cas9 Market Outlook 2022,” *Research and Markets*, October 2016, <http://www.researchandmarkets.com/research/dsj9jw/global>.

⁵ Prashant Mali, Kevin M. Esvelt, and George M. Church, “Cas9 as a versatile tool for engineering biology,” *Nature Methods*, September 27, 2013, 957-963, doi: 10.1038/nmeth.2649.

⁶ David Cyranoski, “CRISPR gene-editing tested in a person for the first time,” *Nature*, November 2016, 479, doi: 10.1038/nature.2016.20988.

⁷ Alex Reis, Breton Hornblower, Brett Robb, and George Tzertzinis, “CRISPR/Cas9 and targeted genome editing: a new era in molecular biology,” *New England BioLabs*, January 2014, 2-4, <https://www.neb.com/tools-and-resources/feature-articles/crispr-cas9-and-targeted-genome-editing-a-new-era-in-molecular-biology>.

⁸ Joi Ito, Director of the Massachusetts Institute of Technology Media Lab, compared CRISPR’s implications in biotechnology to the birth of email: “Suddenly, a janitor had the ability to communicate with the chairman of the board...The filters disappeared.” Ito’s observation that access to CRISPR has become so democratized is supported by a simple Google search for the product, which returns links to online shops where CRISPR kits are sold for less than one thousand American dollars. See Michael Specter, “Rewriting the code of life,” *The New Yorker*, January 2, 2017, <http://www.newyorker.com/magazine/2017/01/02/rewriting-the-code-of-life>.

⁹ The International Genetically Engineered Machine (iGEM) competition is a worldwide synthetic biology competition that encourages high school, undergraduate, and graduate students to think about problems within the field of genetic engineering and create solutions. At the beginning of the annual competition, participating students receive starting kits that contain the DNA-based building blocks needed to engineer the biological system that is judged at the competition. In 2015, CRISPR-Cas9 plasmids were included in the starting kits. See Todd Kuiken, “Governance: learn from DIY biologists,” *Nature*, March 2016, 1667-168, doi: 10.1038/531167a; Vicki Hildner, “What’s CRISPR Phiel connects undergrads with the very latest technology,” *CU Denver Today*, April 4, 2016, <http://www.cudenvertoday.org/crispr-comes-to-undergraduate-molecular-biology-lab/>.

¹⁰ Todd Kuiken, “Governance: learn from DIY biologists,” *Nature*, March 2016, 1667-168, doi: 10.1038/531167a.

¹¹ Ouagrham-Gormley, an expert on bioweapons, views the procurement of biological weapons as the result of the interactions between highly specialized individuals combining their expertise to produce a “working technologic artifact.” See Sonia Ben Ouagrham-Gormley. *Barriers to bioweapons: the challenges of expertise and organization for weapons development*. (Ithica: Cornell University Press, 2014), 12-13. Despite a proliferation of technology and published research pertaining to modifying pathogens, she argues that even the most highly trained scientists have difficulties replicating previous dual-use experiments. See Sonia Ben Ouagrham-Gormley. *Barriers to bioweapons: the challenges of expertise and organization for weapons development*. (Ithica: Cornell University Press, 2014), 9. This assertion mitigates concerns of lay people using pathogen-editing technologies to create a potential pandemic pathogen. Instead it places emphasis on expert labs with knowledgeable personnel accidental or intentional creating such modified pathogens.

¹² Robert Roos, “Study notes H5N1 tweaks that boost airborne spread,” *Center for Infectious Disease Research and Policy*, April 14, 2014, <http://www.cidrap.umn.edu/news-perspective/2014/04/study-notes-h5n1-tweaks-boost-airborne-spread>.

¹³ Highly dangerous pathogens are determined and identified by the Federal Select Agent Program; such pathogens pose severe threats to human health, such as Ebola and SARS. See “Select Agent and Toxins List” *Federal Select Agent Program*, <https://www.selectagents.gov/selectagentsandtoxinslist.html>. Following the GAO report, the

Program mandated three laboratories develop “corrective plans” to address their respective incidents. According to the GAO, the federal laboratories that had similar incidents received no mandates from the Select Agent Program. See “High containment laboratories: improved oversight of dangerous pathogens needed to mitigate laboratories” *United States Government Accountability Office*, August 2016, 42-43, <https://www.gao.gov/assets/680/679392.pdf>.

¹⁴ The highest profile case to come out of the GAO report involved 575 shipments of incompletely deactivated anthrax over the course of 12 years at the Department of Defense’s Life Sciences Division in Dugway Proving Ground, Utah. A Department of Defense (DOD) review of the Dugway incident determined there was insufficient evidence to establish a single cause of the incident, but does note that the senior management at Dugway “allowed a culture of complacency to flourish at the facility, resulting in laboratory personnel who did not always follow rules, regulations, and procedures.” See Paul A. Ostrowski, “Individual and institutional accountability for the shipment of viable *bacillus anthracis* from Dugway Proving Ground”, *United States Army*, December 17, 2015, <https://cryptome.org/2016/01/dugway-anthrax-16-0119.pdf>.

¹⁵ Beverly Sher, interviewed by Hali Czosnek at the College of William and Mary, October 5, 2016.

¹⁶ *Ibid.*

¹⁷ Sarah Zhang, “A woman was killed by a superbug resistant to all 26 American antibiotics,” *The Atlantic*, January 13, 2017, http://www.theatlantic.com/health/archive/2017/01/a-superbug-resistant-to-26-antibiotics-killed-a-woman-itll-happen-again/513050/?utm_source=atfb.

¹⁸ Tim McCoy, “H5N1 Bird flu effects downplayed as WHO calls for weaponized strain to go public,” *Natural Society*, February 25, 2012, <http://naturalsociety.com/h5n1-bird-flu-effects-downplayed-who-weaponized-strain-public/>.

¹⁹ The 60 percent case fatality ratio will only increase if the avian flu is modified so that the virus becomes transmissible through air droplets.

²⁰ Eve Conant, “New gene map of deadly bird flu points to pandemic concerns,” *National Geographic*, April 11, 2014, <http://news.nationalgeographic.com/news/2014/04/140410-virus-bird-flu-national-security-pandemic-science/#close>.

²¹ “The African Mission: Nunn-Lugar Global,” *United States Senate Committee on Foreign Relations*, 4, November 2010, <http://www.foreign.senate.gov/imo/media/doc/The%20Africa%20Mission%20Nunn-Lugar%20Global%20November%202012.pdf>.

²² “The African Mission: Nunn-Lugar Global,” *United States Senate Committee on Foreign Relations*, 5, November 2010, <http://www.foreign.senate.gov/imo/media/doc/The%20Africa%20Mission%20Nunn-Lugar%20Global%20November%202012.pdf>.

²³ Mary Beth D. Nikitin and Amy F. Woolf, “The evolution of cooperative threat reduction: issues for Congress,” *Congressional Research Service*, 42, June 13, 2014, <http://fas.org/sgp/crs/nuke/R43143.pdf>.

²⁴ “About us”, *The Wassenaar Arrangement*, 2017, <http://www.wassenaar.org/about-us/>.

²⁵ “The Biological Weapons Convention,” *United Nations Office for Disarmament Affairs*, accessed February 23, 2017, <https://www.un.org/disarmament/wmd/bio/>.

²⁶ Weaknesses of the BWC framework - namely ineffective monitoring and verification capabilities - have led to the Convention’s failure to prevent several nations from pursuing clandestine biological weapons programs. Most notable of such programs in direct violation of the BWC is the Former Soviet Union’s (FSU) bioweapons program, which continued to stockpile anthrax, smallpox, plague, and other pathogens until 1992 despite signing the BWC in 1972. The possession of offensive biological weapons in China, Iran, North Korea, and Syria further illustrates the weakness of the BWC lacking a verification regime for monitoring signatories’ compliance with the treaty. See Laura H. Kahn, “The Biological Weapons Convention: Proceeding with a verification protocol,” *The Bulletin*, May 9, 2011, <http://thebulletin.org/biological-weapons-convention-proceeding-without-verification-protocol>.

These shortcomings of the BWC have been widely recognized. At the eighth review conference of the Biological Weapons Convention, Secretary-General Ban ki-Moon warned that “there are glaring gaps” in the ability to prevent and respond to the accidental or intentional release of a biological agent. Despite Ban ki-Moon stating that it is the duty of State Parties to strengthen the Convention, a lack of protocol reform prevails, largely due to conflicting interests of State Parties. See “Secretary-General Warns of Glaring Gaps in Ability to Prevent, Respond to Catastrophic Biological Attack, at Review Conference Opening,” *United Nations Meetings Coverage and Press Releases*, November 7, 2016, <https://www.un.org/press/en/2016/sgsm18256.doc.htm>.

²⁷ Frustration over the ineffectiveness of the BWC has led for a push among academics, such as biologist Malcolm

Dando at the University of Bradford's Department of Peace studies, to have the BWC forgo the issue of developing an efficient verification mechanism. Instead, many academics advocate for the education of scientists and instead educate scientists within member states about the dangers of dual-use research. See Malcolm Dando, "Educating the life scientists," *The Bulletin*, November 1, 2011, <http://thebulletin.org/educating-life-scientists>.

²⁸ Robert Roos, "Scientists voice support for research on dangerous pathogens," *Center for Infectious Disease Research and Policy*, July 30, 2014, <http://www.cidrap.umn.edu/news-perspective/2014/07/scientists-voice-support-research-dangerous-pathogens>.

²⁹ Nick Lewis, Mark J. Campbell, and Carole R. Baskin, "Information Security for Compliance with Select Agent Regulations," *Health Security* 13.3 (2015): 207, <http://doi.org/10.1089/hs.2014.0090>.

³⁰ Alison Young, "Labs cited for 'serious' security failures in research with bioterror germs," *USA Today*, August 28, 2015, <http://www.usatoday.com/story/news/2015/08/28/lab-security-violation-bioterrorism-select-agent-regulation/32439491/>.

³¹ Ibid.

³² Brazil, Sweden, Russia, China, Singapore and the United Kingdom reported few security lapses within their highest- security labs. The reported failures mainly stemmed from ill-fitting equipment and leaky drainage systems, and included lethal pathogens like anthrax, Severe Acute Respiratory Syndrome (SARS), Foot and Mouth Disease (FMD). Pakistan, Turkey and Ukraine have reported no accidents of any nature in their highest-level labs in the last 20 years. This indicates the lack of transparency about laboratory failures amongst the international community. See Committee on Anticipating Biosecurity Challenges of the Global Expansion of High-Containment Biological Laboratories; National Academy of Sciences; National Research Council, *Biosecurity Challenges of the Global Expansion of High-Containment Biological Laboratories* (Washington DC: National Academy Press, 2011), Appendix E.

³³ The CBE program has expanded financially from less than 10% of the Nunn-Lugar Global Program budget in the late 1990s to over 60% of the FY2015 budget request (with the overall Nunn-Lugar program budget equaling approximately \$500 million). It is important to note that the funds of the Cooperative Biological Engagement program are used to provide material assistance to recipient countries, as opposed to other programs that may directly allocate aid money to selected countries. See Mary Beth D. Nikitin and Amy F. Woolf, *The Evolution of Cooperative Threat Reduction: Issues for Congress* (CRS Report No. R43143) (Washington, DC: Congressional Research Service, 2014), 37, <https://fas.org/sgp/crs/nuke/R43143.pdf>.

³⁴ "Nunn-Lugar Global," *The Africa Mission*, November 2010, <https://www.foreign.senate.gov/imo/media/doc/The%20Africa%20Mission%20Nunn-Lugar%20Global%20November%202010.pdf>.

³⁵ Kathleen M. Vogel, "Pathogen Proliferation: Threats from the Former Soviet Bioweapons Complex," *Politics and the Life Sciences* 19.1 (2000): 3-16.

³⁶ Amy F. Woolf, *Nonproliferation and Threat Reduction Assistance: U.S. Programs in the Former Soviet Union* (CRS Report No. RL31957) (Washington, DC: Congressional Research Service, 2012), 8, <https://fas.org/sgp/crs/nuke/RL31957.pdf>.

³⁷ Ibid, 24.

³⁸ Richard Lugar, "Eliminating the Obstacles to Nunn-Lugar," *Arms Control Association*, March 1, 2004, https://www.armscontrol.org/act/2004_03/Lugar.

³⁹ U.S. Strategic Command Center for Combating Weapons of Mass Destruction, *The Cooperative Biological Engagement Program Research Strategic Plan: Addressing Biological Threat Reduction Through Research*, June 2015, 3,

http://www.dtra.mil/Portals/61/Documents/Missions/CBEP%20Research%20Strategy_FINAL_July%202015.pdf.

⁴⁰ As part of the CBE's mission to improve biosafety and biosecurity, thereby ensuring the secure handling of dangerous pathogens used for beneficial research, it has partnered with many countries to aid in securing their biological research facilities. For instance, the CBE build a biosecurity level three (BSL-3) lab at a research institute in Kazakhstan in partnership with the Kazakh Ministry of Education and Science amidst rising concerns of improperly secured pathogens. The CBE has also worked with renovating Afghani facilities and equipment upgrades within Iraq's Ministry of Science and Technology laboratories. See U.S. Cooperative Biological Engagement Program, *FY2015 Annual Accomplishments*,

<https://www.dtra.mil/Portals/61/Documents/Missions/CBEP%20FY15%20Annual%20Accomplishments.pdf?ver=2>

016-09-16-150152-690 (accessed February 24, 2017).

⁴¹ U.S. Congress, Committee on Foreign Relations, *The Nunn-Lugar CTR Program's Role in the Administration's Asia-Pacific "Rebalancing" Initiative*, 112th Cong., 2d sess., 2012, Committee Print 77-807, 1-8.

⁴² Within the past decade, the CBE has placed a priority on addressing bioterrorism in Africa, which is a great risk due to highly unsecure laboratories. On a visit to Ugandan and Kenyan facilities in 2010, Senator Lugar expressed his concern over biosafety in Africa, stating: "A potential source of pathogens that could be used in a bioterror attack are the hundreds of poorly-secured laboratories in Africa...these facilities often lack sufficient safeguards to prevent break-ins and theft by terrorists, or smuggling by insiders." Reinforcing Lugar's observation of a Kenyan laboratory situated immediately beside the largest slum in Nairobi, Kibera. Kibera is a known area from which groups, like al-Shabaab, to next to Kibera, the largest slum in Nairobi and a known area where terrorist groups, namely Al Shabaab, source recruits. This laboratory is characterized by broken windows and a short concrete wall that can be easily crossed. Inside the facility, samples of deadly agents are kept in poorly secured refrigerators with basic padlocks securing them. See Richard Lugar, "Nunn-Lugar: Science Cooperation Essential for Nonproliferation Efforts," *Science & Diplomacy* 1.1 (2012): 3-4, <http://www.scienceiplomacy.org/perspective/2012/nunn-lugar.>, Rachel Oswald, "Senate Developing Bill to Modernize, Expand Nunn-Lugar Program," *New Senate Legislation*, April 11, 2013, <http://nti.org/26671GSN>.

A lead Kenyan pathologist expressed his concern over the state of laboratory facilities to Senator Lugar, stating: "We can deal with the diseases, but our facilities were built 42 years ago without consideration for biosafety or security. We want to do the right thing. We need an upgrade." See "Nunn-Lugar Global," *The Africa Mission*, November 2010, 5, <https://www.foreign.senate.gov/imo/media/doc/The%20Africa%20Mission%20Nunn-Lugar%20Global%20November%202010.pdf>.

⁴³ Dave Burke, "Biological terrorism could kill hundreds of millions of people as genetic engineering unleashes terrifying new weapons, warns Bill Gates," *Daily Mail*, February 18, 2017, <http://www.dailymail.co.uk/news/article-4237614/Bill-Gates-Bioterrorism-kill-hundreds-millions.html>.

⁴⁴ In 2011, the U.S. National Research Council Committee on Prudent Practices in the Laboratory put together recommendations for improving laboratory security systems. Among the recommendations were physical security (e.g., proper exterior barriers and controls on doors and equipment), electronic security (e.g., alarm systems and video surveillance systems), operational security (e.g., personnel background checks and authorization procedures), and information security (e.g., data backup systems) improvements. See National Research Council (US) Committee, "Prudent Practices in the Laboratory: Handling and Management of Chemical Hazards: Updated Version," *National Academies Press*, 2010, <https://www.ncbi.nlm.nih.gov/books/NBK55881/>.

⁴⁵ Nunn-Lugar's previous efforts to retrofit bioweapons in the FSU cost around \$3 million per facility and required two to three years for completion. Once facilities are properly secured, there will be minimal additional funding required of the United States, as the majority of costs pass to the recipient country once Nunn-Lugar has completed the contracted upgrades. See Kathleen M. Vogel, "Pathogen Proliferation: Threats from the Former Soviet Bioweapons Complex," *Politics and the Life Sciences* 19.1 (2000): 3-16.

⁴⁶ Mary Beth D. Nikitin and Amy F. Woolf, *The Evolution of Cooperative Threat Reduction: Issues for Congress* (CRS Report No. R43143) (Washington, DC: Congressional Research Service, 2014), 37, <https://fas.org/sgp/crs/nuke/R43143.pdf>.

⁴⁷ Jonathan B. Tucker, "Preventing the Misuse of Pathogens: The Need for Global Biosecurity," *Arms Control Association*, June 1, 2003, https://www.armscontrol.org/act/2003_06/tucker_june03.

⁴⁸ Brad Roberts, "Controlling the Proliferation of Biological Weapons," *The Nonproliferation Review*, 1994, <https://www.nonproliferation.org/wp-content/uploads/npr/robert21.pdf>.

⁴⁹ Jonathan B. Tucker, "Preventing the Misuse of Pathogens: The Need for Global Biosecurity," *Arms Control Association*, June 1, 2003, https://www.armscontrol.org/act/2003_06/tucker_june03.

⁵⁰ The 2008 Maputo Declaration on Strengthening Laboratory Systems recognized the necessity of lab standardization and called upon national governments, donors, and implementing partners to coordinate efforts to achieve their goals. While countries (India, Thailand, Vietnam, Cambodia, Haiti, Kenya, Uganda, and Tanzania) have agreed to increase and standardize lab training, none have been completely successful in their efforts. These countries might be receptive to partnering with Nunn-Lugar Global Program as an implementing partner to increase the standardization, safety, and security of their labs. See "The Maputo Declaration on Strengthening of Laboratory Systems," *World Health Organization*, 2008, www.who.int/diagnostics_laboratory/Maputo-Declaration_2008.pdf?ua=1.

The World Bank's 2014 *Laboratory Professionals in Africa* report looked at the infrastructure and standardization of laboratories in Kenya, Uganda, Tanzania, and to a lesser extent, Rwanda and Zambia. The World Bank identified the flaws and insufficiencies in current laboratory practices in these countries. While Kenya, Uganda, and Tanzania made a few changes in lab training since they signed the Maputo Declaration in 2008, they still fell short in many areas by the 2014 World Bank report. See Jane Carter, Russell J. Dacombe, and Miriam Schneidman, "Laboratory professionals in Africa: the backbone of quality diagnostics," *World Bank Group*, November 2014, <https://openknowledge.worldbank.org/bitstream/handle/10986/21115/927280WP0Labor00Box385377B00PUBLIC0.pdf;jsessionid=3CF637334EBC3976A8B5E8A4814AA0F4?sequence=1>. The Nunn-Lugar Global Program could provide the standardization and funding needed to help these countries fulfill their commitments made in the Maputo Declaration.

⁵¹ Trevor F. Peter, Yoko Shimada, Richard R. Freeman, Bekezea N. Ncube, Aye-Aye Khine, and Maurine M. Murtagh, "The Need for Standardization in Laboratory Networks," *American Journal of Clinical Pathology* 131.6 (2009), 867-874, <https://doi.org/10.1309/AJCPCBMOHM7SM3PJ>.

⁵² Kathleen M. Vogel, "Pathogen Proliferation: Threats from the Former Soviet Bioweapons Complex," *Politics and the Life Sciences* 19.1 (2000): 3-16.

⁵³ Joel O. Almosara, "Biotechnology: Genetically Engineered Pathogens," *The Counter-proliferation Papers Future Warfare Series* 53, 28, <http://www.dtic.mil/dtic/tr/fulltext/u2/a556597.pdf>.