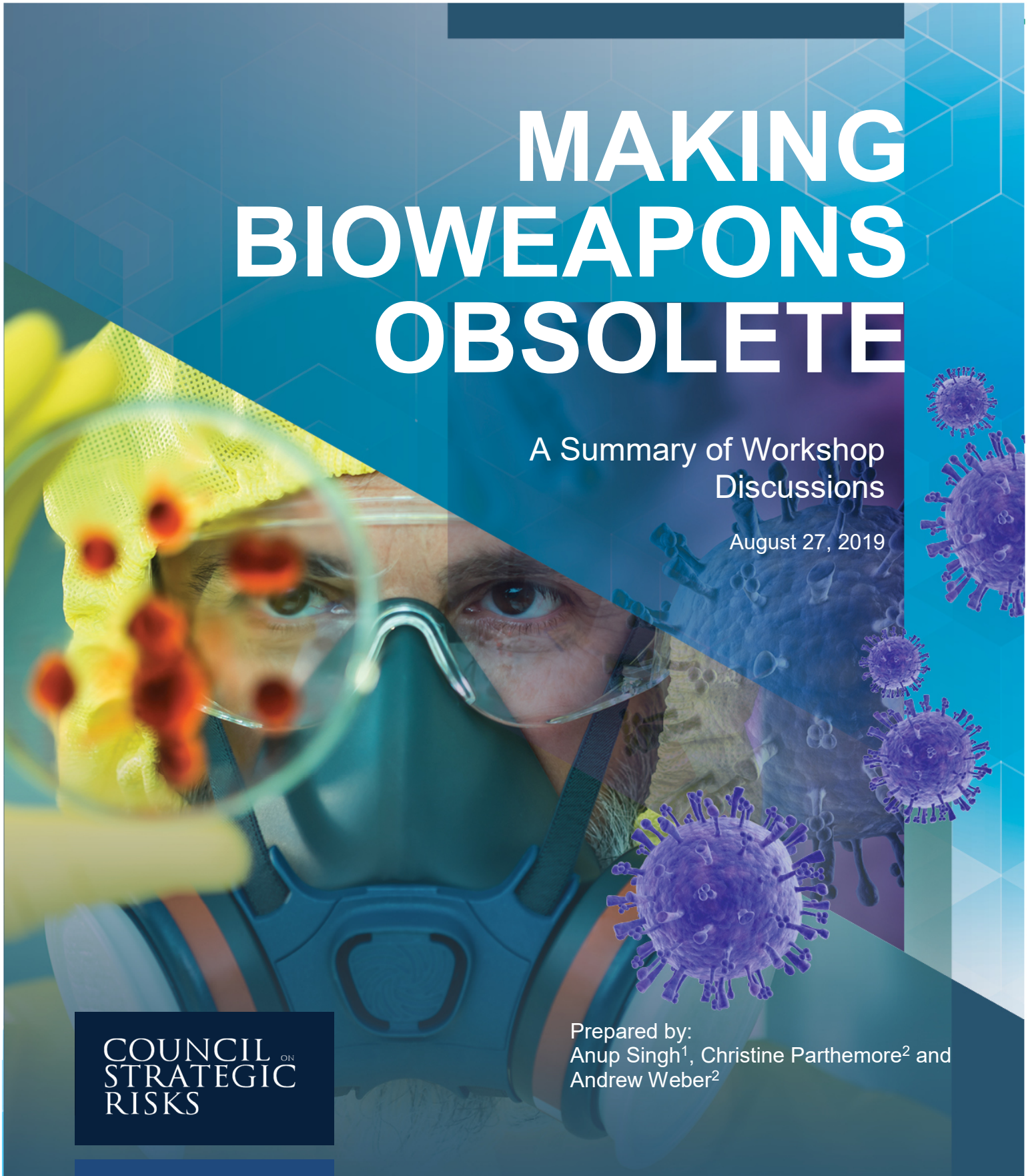
MAKING BIOWEAPONS OBSOLETE

A Summary of Workshop Discussions

August 27, 2019



Prepared by:
Anup Singh[1], Christine Parthemore[2] and Andrew Weber[2]

COUNCIL ON STRATEGIC RISKS

Sandia National Laboratories

1. Sandia National Laboratories
2. The Council on Strategic Risks

Issued jointly by The Council on Strategic Risks and the Sandia National Laboratories, with the latter operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov;
Online ordering: http://www.osti.gov/scitech

Available to the public from

Bioscience Research Foundation
Sandia National Laboratories
Online (Free): Making Bioweapons Obsolete Report

The Council on Strategic Risks
1025 Connecticut Ave, NW Suite 1000
Washington, DC 20036
Telephone: (202) 246-8612
E-Mail: info@csrisks.org
Online (free): https://councilonstrategicrisks.org/programs/csw/

And:

U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

CONTENTS

1. Background 5
2. Acronyms and Definitions 6
3. Workshop Discussions: Introduction 7
   - 3.1. Expected Workshop Outcomes 7
   - 3.2. Workshop Discussions: Setting the Vision 7
     - 3.2.1. The Threat 8
     - 3.2.2. Scoping 9
     - 3.2.3. Strategy 9
     - 3.2.4. Other Facets of Strategy 11
   - 3.3. Workshop Discussions: Technology and Market Changes 12
     - 3.3.1. Objective 12
     - 3.3.2. Key Technical Developments and Trends 12
     - 3.3.3. The Technology Development Environment 14
   - 3.4. Workshop Discussions: What Solutions are Needed? 14
     - 3.4.1. Objective 14
     - 3.4.2. Strategy and Focus 15
     - 3.4.3. Technologies 15
     - 3.4.4. Capabilities 16
   - 3.5. Workshop Discussion: Path Forward 16
     - 3.5.1. Objective 16
     - 3.5.2. Moving from Vision to Specifics 17
     - 3.5.3. Communication and Stakeholder Engagement 17
     - 3.5.4. Roles of Various Entities 18
4. Conclusions 21
   - 4.1. Summary and the Next Steps 21
     - 4.1.1. Scope 21
     - 4.1.2. Technology Trends 21
     - 4.1.3. Solutions 21
     - 4.1.4. Building a “Moon-shot” Initiative 22

Appendix A. Workshop Agenda 23

Appendix B. Workshop Participants 25

TABLES

Table 1. Differences between bioterrorist and state actor attacks 8
Table 2. Differences in biodefense strategy elements based on adversary 10

This page intentionally left blank.

1. BACKGROUND

This report is based on discussions held during an unclassified workshop hosted by Sandia National Laboratories (SNL) and the Council on Strategic Risks (CSR) on August 29, 2019. The first in a planned series, this workshop brought together experts from government, national laboratories, academia, industry, and the policy and entrepreneur communities to examine the potential to use strategy, technology advances, policy, and other tools to make bioweapons obsolete. The workshop provided participants with a rare opportunity to step back from their day-to-day jobs and think strategically about how to achieve this goal more effectively and rapidly.

The conversation was held under the Chatham House Rule. The objective was to generate and share ideas and identify questions that will be critical to answer in pursuit of making bioweapons obsolete. Its purpose was not to create consensus. This report does not represent consensus among participants, nor does it assign specific perspectives to any individual participant or represent the official views of any United States (U.S.) government agency or the organizing institutions namely, SNL and CSR.

About Sandia National Laboratories

For more than 70 years, Sandia National Laboratories has delivered essential science and technology to resolve the nation's most challenging security issues. Sandia National Laboratories is operated and managed by National Technology and Engineering Solutions of Sandia, LLC. (NTESS), a wholly owned subsidiary of Honeywell International, Inc., as a contractor for the U.S. Department of Energy's (DOE) National Nuclear Security Administration (NNSA) and supports numerous federal, state, and local government agencies, companies, and organizations.

About the Council on Strategic Risks

The Council on Strategic Risks (CSR) is a nonprofit, non-partisan security policy institute devoted to anticipating, analyzing and addressing core systemic risks to security in the 21st century, with special examination of the ways in which these risks intersect and exacerbate one another.

2. ACRONYMS AND DEFINITIONS

Abbreviation	Definition
AI	artificial intelligence
AWS	Amazon Web Services
CFIUS	Committee on Foreign Investment in the United States
CRISPR	Clustered Regularly Interspaced Short Palindromic Repeats (genomic editing technology)
CSR	Council on Strategic Risks
DoD	United States Department of Defense
DNA	deoxyribonucleic acid
DRC	Democratic Republic of the Congo
HSPD	Homeland Security Presidential Directive
iGEM	International Genetically Engineered Machine
NTESS	National Technology and Engineering Solutions of Sandia
R&D	research and development
SNL	Sandia National Laboratories
U.S.	United States
WMD	weapons of mass destruction

3. WORKSHOP DISCUSSIONS: INTRODUCTION

On August 27, 2019, Sandia National Laboratories (SNL) and the Council on Strategic Risks (CSR) convened leading experts from government, academia, and business to discuss the vision of making bioweapons obsolete. This report captures important ideas shared during the workshop.

This is an ambitious potential goal for the United States (U.S.). Yet in many ways, entities across the country are already working to make bioweapons obsolete even if that is not yet explicit as a national mission. The U.S. government has many concrete successes relevant to reducing the threat of biological agents that could be viewed as potential indicators of the possibility of making bioweapons obsolete. For example, the U.S. has created a stockpile sufficient to vaccinate every American against smallpox should it be deliberately re-introduced as a threat to the nation. The U.S. government played a critical role in the development of the first-ever Ebola vaccine surrounding the 2014 West Africa outbreak, and that vaccine is now being used in the fight against the disease in the Democratic Republic of the Congo (DRC). Without strong leadership in the White House and U.S. biodefense programs, and the Department of Defense's (DoD) role as a critical enabler, this vaccine would likely not exist today.

To build on these successes and make further strides in eliminating bioweapons threats, U.S. leadership remains critical. The U.S. should expand its efforts in this area, including exercising U.S. influence in international norm-building, expanding U.S. technical leadership in the biological sciences, and much more.

This report begins with overviews of the main areas of discussion during the workshop: setting the vision, technology and market changes, the solutions that are needed, and the path forward (the agenda for the meeting is included in Appendix A). It concludes in brief with the host organizations' synthesized findings and next steps.

3.1. Expected Workshop Outcomes

- Gain a better understanding of the threat and how technology can both increase and mitigate the risk
- Identify solutions that offer the greatest return
- Identify a plan to influence national leadership to provide attention and resources to the issue and engage academia and industry

3.2. Workshop Discussions: Setting the Vision

Objective: This opening segment was future-looking and focused on high-level vision for the U.S., acknowledging the character of current and future threats and opportunities. The questions posed to guide the discussion were as follows:

- Who as an adversary may be interested in bioweapons as weapons of mass destruction more than other approaches to meet their strategic intent and why? What advantages do bioweapons offer?
- What are the implications of a bioweapon for terror vs. strategic ends?
- Does great power competition have potential to increase the risk?
- Have advances in technology lowered the bar and leveled the playing field for adversaries with inferior conventional and/or nuclear options?

3.2.1. The Threat

The biothreat appears to be both changing and increasing, principally because of three factors: 1) advances in technology, 2) increased concern about nation-state peer competitors, and 3) apparent decreased U.S. focus on biothreats.

The recent National Defense Strategy states that "The central challenge to U.S. prosperity and security is the reemergence of long-term strategic competition," and "The homeland is no longer a sanctuary."[1] It highlights strategic trends in national defense including rapid technological advancements (including biotechnology) and the changing character of war. Note that the concern is biotechnology, not just bioweapons, and strategic nation-state competitors, not just terrorists.

Table 1 provides an example of possible differences between a bioterrorist attack and that of a state actor and the potential impact of those differences on a multi-layer biodefense.

Table 1. Differences between bioterrorist and state actor attacks

	Terrorist	Peer Competitor
Goals	Mass casualties	Military or strategic
Deterrence	Nothing to hold at risk; Plausible defense	Policies, red lines, norms; Plausible defense
Why bio	Ability for mass destruction	Stealthiness. Elicit ambiguous response
Attack mode	Target large population; Airborne agent	Smaller size to stay below red-line; various pathways
Tech level	Simple to modest	Sophisticated

Throughout the meeting discussion touched on the evolving character of the bioweapons threat. Conversation ranged from discussion of aspects of the global national security environment to the changing character of conflict to specifics of emerging biothreat agents. The threat space is further complicated by a concern that convergence of threats (bio and non-bio, such as bio/cyberattacks) might enable a new norm to achieve asymmetric effect by many actors.

Some participants raised concerns that laboratory accidents, or premature use of advanced biotechnology may produce significant, wide-scale negative consequences. An additional concern raised was that the objective of a biological attack, especially for a sophisticated state-actor adversary, could cause economic devastation or disruption as well as mass casualties. Therefore, attacks may be tailored to strike economic targets.

With the expansion of technologies and methods that could be employed for biological attacks, there is a widening spectrum of potential scenarios for which the nation must prepare. Traditional, enhanced and advanced agents are all threats that we must continue to be prepared for. The "tactical" threat of a relatively singular, one-time use of biological weapons has not gone away.

However, there is also a concern that perpetrators could consider a long-term, "strategic" attack on our society or economy that more slowly degrades the U.S. position and creates significant

[1] Summary of the 2018 National Defense Strategy
https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

long-term harm. The current Ebola outbreak in the Democratic Republic of the Congo demonstrates challenges that are amplified when disease outbreaks are superimposed on conventional conflict; there is concern that adversaries may try to replicate this in future conflicts, mimicking nature and deliberately spreading diseases to further complicate decision-making and responses. One participant pointed to the ongoing crisis regarding synthetic opioids like fentanyl in the U.S. as potentially providing useful insights applicable to a strategic bioweapon threat. The synthetic opioids devastating communities across the country are mostly being made abroad but are being distributed through our own postal system. Despite significant casualty rates and other harm resulting from the use of synthetic opioids, the public outcry and response are relatively muted. This case highlights the concern that the scale of impact and distribution methods can evolve very rapidly.

For many participants, nation-state threats were of highest concern. And while some characteristics may be unique to nation-states, the world is witnessing continued hybridization of tactics used in conflict, confrontations, and threatening behavior. Nations may use sub-state proxies or tactics more commonly associated with sub-state actors to conduct attacks or operations related to potential future attacks, including to hinder attribution. Furthermore, adversaries can mimic nature to cover their tracks, for example, by creation of a flu-like pandemic that mimics a natural infection. In summary, the future of bio attacks can be very ambiguous - nation states can look like terrorists and attacks can look like natural events.

The competition for narratives may also be a key feature of future bioweapons use scenarios. Those responsible may employ disinformation campaigns before, during, and/or after a biological attack. This may include campaigns to drive public backlash against biotechnology broadly, confuse the public regarding safety of vaccines or countermeasures (especially if they are new or tailored to novel agents), and drive uncertainty among policy makers.

3.2.2. Scoping

Discussions of the threat and the threat space reflect the fact that this is an extremely large and complex (and perhaps overwhelming) problem. The group discussed various ways in which it might be possible to focus the effort or help make the challenge more tractable in other ways. One approach might be to focus on eliminating (or mitigating) the highest risks. Other discussion involved whether or not to include an emphasis on public health risks. Later discussion also spoke to the appropriate balance of emphasis between eliminating risks stemming from traditional versus advanced biothreat agents.

Since clarification of scope is central to informing the vision and articulating a strategy for achieving it, this topic likely requires further dedicated discussion.

3.2.3. Strategy

Efforts to develop biodefense strategy have recognized that there is no singular solution for eliminating the risks posed by adversary use of dangerous bioagents. As noted in Homeland Security Presidential Directive-10 (HSPD-10) [2], and recapitulated in the recent National Biodefense Strategy,[3] an effective biodefense is multi-layered. Defense efforts require attention to all layers of defense, including threat awareness, prevention and protection, surveillance and

[2] Homeland Security Presidential Directive HSPD-10, Biodefense for the 21st Century, United States, Office of the Press Secretary, 2004. https://fas.org/irp/offdocs/nspd/hspd-10.html

[3] National Biodefense Strategy, 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Biodefense-Strategy.pdf

detection, and response and recovery (to use the HSPD-10 "pillars" - the 2018 National Biodefense Plan is formulated around five goals which encompass the same integrated scope in a somewhat different configuration of elements).

Finally, changes in technology must be considered when formulating an effective biodefense strategy. For example, the 2018 National Academies study, *Biodefense in the Age of Synthetic Biology,*[4] recommended (among other things) developing nimble strategies applicable to a wide range of threats, evaluating and improving infrastructure for recognizing unpredictable syn-bio threats, and risk management strategies that supersede current agent-based lists, among other things. An effective strategy could focus on most plausible high risks but should provide a hedge to address surprises arising from rapid and unanticipated technical change.

Table 2 summarizes how biodefense strategy elements may differ depending upon the adversary. The following section discusses it in greater detail.

Table 2. Differences in biodefense strategy elements based on adversary

	Terrorist	Peer Competitor
Threat Awareness	Intel; risk assessments	Intel; risk assessments-monitor "tech surprises"
Prevention & Protection	Strategic National Stockpile; BioShield	Deterrence policies; attribution tools; new medical countermeasures
Surveillance & Detection	BioWatch, syndromic surveillance, public health	Challenging given multiple pathways and novel agents. Solutions include enhancing public health and platform detection technologies for broad range of threats
Response & Recovery	Rapid mass prophylaxis; decontamination	Treatment; attribution; 'measured' response

Workshop participants shared a variety of views regarding the *deterrence* of bioweapon attacks. This included various ideas on the ways and degrees to which nation-state and sub-state actors might be deterred from using bioweapons. In particular, there was a robust conversation on whether a plausible defense against biological attacks was sufficient to effectively deter them; some participants believed this may be the case, while others believed that perpetrators of such attacks may not make fully logical decisions or may use bioweapons in a state of desperation whether or not they are useful at causing mass effect.

Among the experts gathered, there was some divergence in views on what degree attribution and, in particular, rapid attribution is important for deterring biological attacks. Some believed that even without strong attribution capabilities, rapid and effective response capabilities may be sufficient to deter biological attacks, as such attacks would become a relatively ineffective method of

[4] Biodefense in the Age of Synthetic Biology, National Academies of Science, 2018. https://www.nap.edu/catalog/24890/biodefense-in-the-age-of-synthetic-biology

meeting the perpetrator's intended political objectives. Others found attribution to be an acceptable goal while still others believed it may be more economical to invest in increasing threat reduction measures.

Still others believed that attribution would continue to be critical to deterring the use of bioweapons, especially by nation-state actors or their proxies. Increasingly sophisticated attribution tools and methods could help showcase very effective U.S. scientific capabilities in ways that help deter biological attacks.

In any case, from a U.S. government perspective there will be treaty aspects to consider. Nation states signing versus abiding by treaties can differ, and some may drive toward tactics that deliberately impede attribution. The continuing convergence of biological and chemical threats, likewise, carries implications for attribution, both in how new attribution methods may be created and because attribution is treated differently in the Biological Weapons Convention and the Chemical Weapons Convention (though this may evolve over time).

International norms regarding the full spectrum of weapons of mass destruction have changed significantly in recent years. Many are concerned that the taboo against using these weapons may be strained or broken. Because underlying capabilities relate to such a widespread area of the global economy, bioweapons threats may be in some ways the optimal focus for rebuilding norms against Weapons of Mass Destruction (WMD) development and use.

Renewing American commitment to strengthening WMD-related norms could form an important area of soft power. In addition to those norms intended to inhibit WMD production and use, this includes norms around intellectual property as well as uses of technology. Efforts modeled off of the successful Cooperative Threat Reduction Program could help in spreading norms, expanding the odds of whistleblowing, and more. Whatever mechanisms are used, national efforts to re-strengthen global norms related to biothreats must start with an understanding of our common values across sectors, communities, and industries. Determining the amount of leverage the U.S. private sector, scientists, and government have to disseminate these values would also help.

Additionally, it is important to recognize that the U.S. is not the only nation or entity trying to establish what the future looks like regarding the use of biotechnology and the global bio-economy. Some countries which are leading in aspects of these domains do not share our ethos and norms, therefore, concerted American leadership is critical.

Expanding U.S. norm-building contributions must start with serious consideration of ethical issues and a process of identifying shared national values across the public and private sectors. Such shared values can then form the basis of international outreach and collaboration. These areas of activity are difficult but critical, including effective public communications. They should start with recognition that there are ongoing activities that most U.S. scientists and policy leaders would consider to be unacceptable.

3.2.4. Other Facets of Strategy

For effective national strategy, the group discussed the importance of developing means to quickly differentiate natural events (e.g., emerging infectious disease) from human-caused events. The ability to detect novel tinkering will also shape the U.S.' ability to understand and respond effectively to biological events. Improvements in epidemiology and surveillance will be important. The group also highlighted the importance of innovation in characterizing whether events are natural versus human-made in the complex microbial environment.

Response and recovery are likewise critical. The group held an extensive conversation surrounding technical means to quickly develop, test, produce, and deploy medical countermeasures (and the importance of establishing and sustaining the capabilities to do so; this paper further covers this discussion below). Whatever methods are used, it can help to think about responses to bioweapon attacks in terms of U.S. power projection. Developing capabilities and demonstrating them, for example, in responses to disease outbreaks, can help showcase effective American action against biothreats.

One potential angle worth exploring is how to build what one participant described as "mutually assured security." The U.S. may find that there are limited ways to build trust among its peer competitors, but there may still be space for mutual agreement regarding the desire for our nations to survive and thrive. Several participants agreed that common ground may be found in asking how we build a world that we all want to live in alongside adversaries, friends, and peer competitors.

Some participants emphasized that a strong U.S. strategy must account for personal liberties, including an open system by which all Americans can aim to obtain the prosperity and opportunities the bio-economy can provide.

One of the benefits of a national-level vision is that while the government will have to determine its scope and prioritize its resources accordingly, others across the nation may contribute to the same vision in different ways. Regardless of how it is characterized, the actions taken in the years ahead toward making bioweapons obsolete must be tangible, demonstrable, and replicable.

3.3. Workshop Discussions: Technology and Market Changes

3.3.1. Objective

The goal was to discuss how we expect the relevant fields of science, tech development, market evolutions, etc., to shape the landscape (say in the next 10-15 years), both as an enabler of the risk but also as the solution. Questions posed to guide the discussion were as follows.

- What drivers might create paradigm shifts that may increase the risk of innovations being used, intentionally or accidentally, for developing bioweapons.
- What keeps you up at night when you think of the trajectory of biotechnology (and convergent technologies such as artificial intelligence [AI]) ?
- How can we reduce the risks of such developments?
- Do we need to develop globally accepted norms and standards?
- How can innovations in biotech spur new solutions to counter the risks?
- How can industry, academia, and government best lead given the dual-use nature of biological technologies?

3.3.2. Key Technical Developments and Trends

This session began with a focus on specific technical developments and trends. The scope extended from laboratory developments to the commercial use (and drive) of ongoing advances. The conversation then turned to the national environment in which these developments are occurring - interest (and concern) in both government and among the public. This led to discussion of policy

and regulatory issues and needs. The conversation concluded with an articulation of the need for U.S. technical leadership.

The world is seeing a revolution stemming from the biological sciences that must be embraced in order to significantly mitigate bioweapons threats. The group discussed several aspects of this revolution, and capabilities available today and those that may be available in the near future. Conversation tended to focus on gene editing and synthetic biology, but it was generally understood that the revolutionary advances result from "convergence" of biological technologies with other technologies such as artificial intelligence, robotics, and nanotechnology.

Genome Editing and Synthetic Biology: The group discussed several specific tools and technologies relevant to present and future bioweapons threats. This included gene editing, high throughput gene synthesis, synthetic biology, rapid enzyme discovery, genetic analysis of large populations, and implications of advances in artificial intelligence. CRISPR-Cas9, a breakthrough area of genome editing technology, can be used globally to precisely manipulate genomes through gene knock-out (gene inactivation). Within the next 10 to 15 years, any genome change, including a knock-in (substitution or insertion of DNA sequence information) will be possible. Uses include dialing up or down the expression of genes to create transient changes, detecting or responding to specific molecules in disease treatment via CRISPR enzymes, and more.

Technology today is limited by a lack of knowledge of what to edit. That is, we only know of some of the genes that play an obvious role in human health. Concerns such as using methods developed for personalized medicine to attack individuals may be further into the future. However, this knowledge will improve in the coming years, allowing (for example) analysis of large populations to identify a small group of people susceptible to a specific disease.

It is now easy to access genome editing tools globally in labs. However, this generally does not yet extend in significant ways outside of laboratory environments. While there have been breakthrough advances in genome editing, knowledge regarding what to edit for specific effects and determining the unintended off-target effects is still nascent today.

Use of synthetic biology to engineer organisms is rapidly maturing as evidenced by the large number of companies, both large and small, involved. Using large sequencing databases and bioinformatics tools, it is routine now to design and test thousands of genes for the purpose of making a novel molecule.

Artificial intelligence will play a large role in future biotechnology advances. Advanced manufacturing and robotics technologies play key roles in how the bio-economy is evolving, and big-data analytical and prediction capabilities will be increasingly prominent. Automation allows scaling and enables lesser-skilled people to work more effectively while standardization can offer levels of control and security in biotech operations. Notably, these fields are progressing at different paces which will have implications for how they influence the biothreat environment and enable more effective responses to bio events. And though tools that might be used for enhancing or creating new bioweapons are advancing, commensurate changes in the technologies for delivering them effectively may not evolve at a commensurate rate.

While advances in biotechnologies represent a risk, these advances have been and will continue to be critical for rapidly developing countermeasures, and for designing and synthesizing genes for more rapid prototyping and testing. Some workshop participants believe viruses (e.g., influenza) may be a good target for testing how new approaches could help with increasing the speed of countermeasure development.

3.3.3. The Technology Development Environment

Across all of these areas, U.S. leadership and proactive policy making are imperative. This requires maintaining a competitive edge in science and technology in ways that help set global norms and standards. There must be stronger norms for deployment of new techniques and tools as they are developed. The less this is the case, the greater the chances are that the U.S. will be hit with more surprises (such as the premature release of a gene drive, or activities carried out by another country or entity which U.S. experts deem irresponsible or dangerous). Other countries are rapidly catching up to the U.S. in spending research and development dollars for biotechnology and the field has become truly democratized and global. An example is the recent move of the International Genetically Engineered Machine Competition (iGEM), the largest synthetic biology community and the premiere synthetic biology competition for university and high school students, to Paris.

A number of participants expressed concerns that some facets of work in advanced bioscience and technology are leading to skepticism among some of the public and concern from government entities. One participant cited a recent instance in which government participation in a synthetic biology meeting was restricted. On the other hand, another person mentioned recent meetings with senators and representatives who exhibited considerable positive interest and curiosity about technical advances and their implications.

These observations led to a more general discussion that seemed to reflect a sense that academia and industry, along with other groups working in biotechnology, need a coordinated and proactive approach to help educate government stakeholders and the public regarding implications of developments in bioscience and technology. While there were various opinions as to who should be responsible for such messaging, participants offered several thoughts on the nature of that messaging. It should be spearheaded by individuals and groups that can serve as trusted advisors. Communications should be transparent, with an open articulation of potential risks and negative consequences. Engagement with stakeholders and interests outside traditional groups may be very important. And further engagement with political decision makers needs to be pursued. It is important that this effort begin early because of the danger that individuals or groups with contrary interests might begin to control the conversation with negative messaging or even misinformation.

Finally, a number of participants expressed concerns that actions to make bioweapons obsolete might lead to U.S. policy and regulatory changes that would severely inhibit or even prevent technical advances. This risk is amplified by the potential that concerns from the public based on limited or incorrect information could create pressures to drive such changes. Some felt that this community must be proactive in helping shape policy developments in ways that provide safeguards while minimizing unwanted and unneeded regulatory changes. Such changes could jeopardize U.S. technical leadership and thereby preclude an effective U.S. role in influencing international norms in advanced biotechnology while also hurting the competitive standing of the U.S.

3.4. Workshop Discussions: What Solutions are Needed?

3.4.1. Objective

This session focused on discussing solutions based on our understanding of the threats and risks (to what, by whom, what would it look like), the strategy for defending against these threats, current/near-term actualization of that strategy, and gaps and possible ways of addressing those gaps, and possible solutions, both policy-based and technological. It asked the following questions to guide the discussion.

- Do we develop solutions that have wide applicability for eliminating or countering the risks?
- Where is the biggest return-on-investment - not just in technologies, but in policies and processes?
- Absent a clear market driver, how do we engage industry?

3.4.2. Strategy and Focus

The group's conversation on solutions was particularly wide-ranging and the discussion touched on everything from very specific needs (such as items to support wide-scale delivery of medical countermeasures) to knowledge gaps in aspects of fundamental cellular biology. Much of the conversation revolved around medical countermeasures.

The issue of focus and scope of an effort to "make bioweapons obsolete" was again implicitly raised with discussion of how an emphasis on infectious disease fits within the objective. Participants pointed to historical successes (and near successes) in this domain as providing exemplars for meeting such an objective while also providing a focus that could generate support within the government and the public. One contrary perspective voiced was that focusing too narrowly on public health needs tends to relieve the national security community of responsibility and minimizes needed critical contributions and utilization of capabilities of national security-focused agencies.

3.4.3. Technologies

As mentioned, discussion of needs was very wide-ranging. Specific needs mentioned include methods to rapidly discriminate between natural and human-made bioagents and medical countermeasures for specific pathogens. Needs in basic science mentioned included "faithful physics models of cells" and a detailed understanding of common patterns in viral pathogens that might lead to improved approaches to the development of antivirals. There was mention of the need for funding agencies to more systematically support development of "tooling" - the scientific and technical tools needed to support research in biology and biomedicine.

One topic that generated much discussion was the role of AI (and the data sets that would help enable AI). Many participants were excited about how AI might be used in developing medical countermeasures (especially broad scale antivirals or antibacterial agents). AI as a tool to aid rapid discrimination between natural disease outbreaks and adversary action was also mentioned.

Many participants see a huge opportunity to expand data sharing, and they believe any new national strategy to counter biothreats should double down on it. While other countries are aiming to develop the largest datasets on certain aspects of genetics and diseases, the U.S. could expand on its efforts to date to become the world's leader in opening data to broad access. American companies have much to contribute to this, and some participants believe that there are promising ways to do this focusing on the significant volumes of pre-competitive data they generate.

Differences in views regarding data quality/resolution and many other variables will require significant analysis. Expanded open data systems would also require better policy maker and public understanding of what open source really means in the biosecurity context. If successful, more open access to data can help make the case for continuing investment in making bioweapons obsolete, for example by enabling analysts to more accurately determine the public health costs and savings that stem from specific government investments.

Security will be paramount, and huge questions remain regarding who should be in charge of managing and securing data that can be considered a strategic asset. While security will be a challenge and specifics will depend on which actors are charged with data management, the Amazon Web Services (AWS) government cloud deal shows that the nuances of data security can be worked out.

3.4.4. Capabilities

Making bioweapons obsolete is much more than a technical or research and development (R&D) issue. In particular, capabilities to facilitate test and evaluation of candidate countermeasures are necessary (along with a regulatory environment that will embrace new technologies).

The ability to produce and deliver countermeasures at scale was the topic of a significant amount of discussion. There are important lessons from past cases in which the U.S. government invested in capabilities that were later upset by business dynamics. The U.S. government previously contributed to breakthroughs and created advanced development and manufacturing capabilities for medical countermeasures (e.g., to create domestic capacity to produce sufficient influenza vaccine to protect the nation), but several have been taken over by non-U.S. entities or are no longer operating. This experience underscores the fact that key capabilities must be sustainable - simply funding their establishment can lead to a "second valley of death" that challenges continued viability of the capability.

The question of production locations extends to supply chains, many of which are international for American companies, even if their primary facilities are located on U.S. territory. These variables have major bearing on costs for feedstocks and other inputs. How this is accounted for may be pivotal to the ability of U.S. companies to contribute optimally.

The group discussed the various ways that establishing and sustaining U.S. capacity against bioweapons threats could occur. Some participants believed strongly that domestic production capacity was critical for many reasons, including for demonstrating the active ability to mitigate bioweapons threats. Other potential approaches included creating dedicated biofoundries in government spaces that can be ramped up for surge capacity when the government needs it but are otherwise used for experimentation or commercial purposes. The possibility of relying on distributed capabilities in which critical aspects are located and controlled domestically, while support capabilities are not necessarily domestic, was mentioned.

Ownership and management of critical capabilities (public versus private) is another factor. There may be benefits to government-owned and operated facilities of various kinds, with other advantages to capabilities existing in the private sector if it is clear they can be called upon as reserve capacity when needed. The group also encouraged thinking beyond bio-specific facilities in this regard; as the bioeconomy expands, capabilities normally used for the production of energy or bio-based products may become useful when surge capacity is needed for national response.

3.5. Workshop Discussion: Path Forward

3.5.1. Objective

To guide the discussion, the following questions were posed to the participants.

- How do we develop a plan to defend against the evolving biothreat in a shifting national security climate?

- How do we highlight and adequately prioritize biodefense in an integrated national defense strategy?
- How can we better communicate both the threats and opportunities?
- How do we engage academia and industry in a national dialogue and promote better public-private collaboration on this grand mission?

3.5.2. Moving from Vision to Specifics

The group discussed many components that would be important in effectively working toward a vision of making bioweapons obsolete. This included the importance of balancing near-term practical steps and quick wins with resourcing ideal medium- and longer-term solutions.

A moonshot-type vision for U.S. biosecurity efforts can help in focusing effort, accelerating progress, creating unity among public and private actors, and making the case for resources commensurate to both understanding emerging bioweapons threats and mitigation opportunities.

The group noted the need for concerted expert discourse on what types of capabilities would be needed and desirable for making bioweapons obsolete. What tools are needed, how are they used, and by whom? Is there a future single-box solution we could envision? Coupled with evolving means of production, is it feasible to think one day people or distribution entities will be able to download the specs for therapeutics and make them in a fully distributed manner and, if so, would this hold implications for increasing the risks of similarly-distributed bioweapon production?

Thinking in great leaps may help in driving toward specifics. One participant recommended considering, for example, what we would want to give someone going to live on Mars in order to detect, characterize, and treat whatever biological dangers they faced.

3.5.3. Communication and Stakeholder Engagement

For any specific approaches to implementation questions, effective communication will be critical. This begins with articulating an ambitious national vision regarding biothreats but does not end there. Concise and compelling problem statements must be developed in order to help new stakeholders truly understand bioweapons threats. From there, stakeholders must believe that progress is achievable and understand how that may happen. Strong and easy-to-understand messages will be required to gain buy-in and resources for even the most practical steps - let alone for the larger leaps that may be desirable.

As U.S. policy evolves, public communication that aims to minimize backlash resulting from lack of information (or misinformation) will be equally important and may be challenging. There are already signs of legitimate public concern over the use of personal health and genomic data, genetic modification of organisms, and vaccines, to name a few. Public sentiment against specific steps to implement a plan to make bioweapons obsolete could be fueled by fear and misinformation. Addressing this challenge will require trusted messengers for various stakeholder communities and proactive planning. It will also require honest presentation of risks and trade-offs regarding specific technologies and methods to ensure transparency. Listening to diverse audiences will be crucial.

Similarly, a strategy for communication with government decision makers and other stakeholders will be critical.

Effective communications (and implementation broadly) must include ongoing preparation for surprises. These may arise in tech developments, the application of new technologies, misinformation, and more. Shifts in public perception can be rapid, requiring proactive communication strategies that envision and prepare for a range of potential surprises.

3.5.4. Roles of Various Entities

The U.S. government's capacities for countering biothreats extend far beyond funding research. It has important mechanisms for supporting and incentivizing solution creation by the private sector, and many ways to leverage private-sector innovation. It also has a strong history to build upon: the U.S. government has succeeded in finding cures for fatal diseases in cases when the private sector has not, and it has in countless ways advanced national biosecurity assets.

Moreover, U.S. government laboratories across many departments hold critical national capacities in its people and physical infrastructure that must be fully utilized. The U.S. national security laboratories also serve important roles in matchmaking among stakeholders with common interests but who may not be communicating or collaborating (especially as a conduit between government and academic experts).

Still, there are areas for improvement. The U.S. government has made historic strides against biological threats, but gains can still too often be hindered by episodic funding. There may be ways to create greater leverage or common purpose with companies in which the government invests in order to increase the odds they will continue contributing to a united national vision.

The U.S. government will need to build additional safeguards for intellectual property and protecting American innovation and investment. We have the Committee on Foreign Investment in the United States (CFIUS) and other mechanisms, but many of them only come into play when it is already too late to fully protect U.S. interests.

Other changes may be warranted. As we enter an age of personalized medicine, some regulations may be outdated. Accelerating clinical trials during outbreaks may be important. Additionally, the U.S. scientific community and economy have seen great successes from its investments in basic research in the biological sciences and related technical fields; this could imply the need for U.S. government investments to either continue or to shift toward later-stage development, testing, evaluation, scaling, and deployment.

Additionally, progress to date must be recognized and leveraged. For the DoD, for example, biotechnology is now designated as an enabler of the future force. While the specifics are yet to be determined, this should trigger examination of the department's balance of investments and evaluation of whether additional authorities should be granted to take maximum advantage of this designation.

Workshop participants have seen (and in many cases driven) major successes in public-private partnerships and collaboration for reducing bioweapons threats. Their experiences should continue to be mined for lessons and ideas.

There are areas where improvements can potentially be made. Fostering more interaction with start-ups and ensuring government programs create an even playing field for small companies, will remain important. The direct and opportunity costs of private companies and academics collaborating with the government may need to be lowered; for example, some small grant programs require more work value just to apply than the equivalent value of the funds provided.

For the private sector, funding and financing dynamics may also need to shift. Many entities providing significant financial resources relevant to making bioweapons obsolete have calculations for return on their investments that may make meeting national security goals difficult. Rising international investment in U.S. companies will likewise require attention. Driving a sense of national mission must be part of any implementation plans for significantly mitigating bioweapons threats; market forces alone will not be sufficient.

This page intentionally left blank.

4. CONCLUSIONS

Overall, many participants expressed great urgency in moving forward on the ideas and questions raised during this workshop. There is a window now to shape the emerging bioeconomy in terms of factors like control, market concentration versus distribution, and protection of individual rights. Furthermore, there are worrying signs of declining U.S. leadership in biotech and biosecurity, including rising influence by China, various European countries, and others.

A united, ambitious national vision of making bioweapons obsolete will help in meeting the urgency of the moment and in materially altering the landscape of biological threats. It must be clearly articulated that a national effort toward making bioweapons obsolete will protect America, reduce the nation's vulnerabilities, and increase its competitiveness. Meeting this ambition will take commitment, time, resources, and perhaps most important, leadership.

4.1. Summary and the Next Steps

A meeting was convened for the workshop organizers to discuss the workshop report and synthesize a few summary observations and the next steps. These ideas are those of the workshop organizers and should not be assumed to be a consensus of the workshop participants.

4.1.1. Scope

While the title implies focus on man-made threats, the workshop discussed the threat from a much more comprehensive perspective that included natural outbreaks and accidental releases/events. Discussion of man-made events caused by terrorists, quasi-state actors, and state actors were all mentioned. While we agree that it is useful to consider the threats holistically, a concern is that the focus immediately shifts to natural threats simply because they are ever-present. This leads to a gap in our security posture because not all solutions for defending against natural threats are applicable to man-made threats. We recommend that the next workshop focus on man-made WMD threats.

4.1.2. Technology Trends

It was evident from the discussion that the advances in biotechnology and their convergence with other technologies are poised to create breakthroughs in human health, agriculture, and consumer commodities. However, there is a "dark side" to this similar to information technology advances. The great power competition, advances in biotechnology, global spread of bio capabilities, and convergence of biotechnology with others such as AI can create risks that we have not encountered before. We believe that we need to look at the technology advances holistically by paying attention to both sides - as a source of "technology surprise" by our adversaries but also as a source of innovative solutions to current and future threats. *We recommend that we focus separately on the two sides of technology trends at the next workshop by inviting more participants from industry and academia.*

4.1.3. Solutions

Considering our emphasis on reducing the scope to man-made biothreats, we propose focusing on solutions relevant to the specific threats. Specifically, how to develop a defense-in-depth approach to countering threats posed by quasi-state and state actors. This should include elements such as anticipation of technology surprise, deterrence, threat awareness, prevention, mitigation, response, and recovery. This will also include both policy and technology solutions and hence, will need engagement of more policy experts as well as academia, industry, and national security

stakeholders. *We recommend that we focus on both policy and technology solutions specific to man-made WMD threats and invite a diverse set of experts in both.*

4.1.4. Building a "Moon-shot" Initiative

Based on the discussion, we recommend two topics to be discussed at the next workshop: a) how to build a community that is more diverse than the traditional biodefense community by including academia and industry at a much larger scale, and b) how to develop a better and more effective communication strategy at the national and international level to inform the various stakeholders including elected officials, potential sponsors, and non-governmental organizations. *We recommend multiple lines of effort to deeply develop key aspects of a "moonshot" initiative and corresponding teams of participants and stakeholders.*

APPENDIX A. WORKSHOP AGENDA

Making Bioweapons Obsolete

August 27, 2019

9:00am	Welcome *Doug Bruder*
9:10am	Introduction and Expected Outcomes *Andy Weber and Anup Singh*
9:30am	Making Bioweapons Obsolete: Setting the Vision *Moderator: John Vitko* *Remarks by John Vitko followed by group discussion*
11:00am	Technology and Market Changes: What to Expect? *Moderator: Anup Singh* *Remarks by Jennifer Doudna and Patrick Boyle followed by group discussion*
12:30pm	Lunch (continue discussion)
1:15 pm	What solutions do we need to defend against the threats? *Moderator: Robert Kadlec* *Remarks by Robert Kadlec followed by group discussion*
3:00pm	How to Move Forward *Moderator: Christine Parthemore* *Remarks by Andy Weber followed by group discussion*
4:30pm	Closing Notes & Adjournment by Anup Singh, Sandia *Andy McIlroy*

This meeting will be UNCLASSIFIED and held under the Chatham House Rule.

This page intentionally left blank.

APPENDIX B. WORKSHOP PARTICIPANTS

Natasha Bajema
Founder and CEO
Nuclear Spin Cycle, LLC

Tom Bates
Program Leader, Biosecurity Center
Lawrence Livermore National Laboratory

Catherine Branda
Sr Manager, Applied Biosciences
Sandia National Laboratories

Luciana Borio
Vice President, Technical Staff
In-Q-Tel

Patrick Boyle
Head of Codebase
Ginkgo Bioworks

Ben Brodsky
Manager, Risk Management Department
Sandia National Laboratories

Doug Bruder
Global Security Associate Labs Director
Sandia National Laboratories

Jim Carney
Manager, Advanced Materials Laboratory
Sandia National Laboratories

J. Bradley Dickerson
Sr Manager, Global Chemical and Biological Security
Sandia National Laboratories

Jennifer Doudna
Professor of Chemistry
Professor of Biochemistry & Molecular Biology
University of California, Berkeley

Drew Endy
Associate Chair of Bioengineering, Stanford
President, BioBricks Foundation

Julie Fruetel
Manager, Homeland Security and Defense Systems
Sandia National Laboratories

Jennifer Gaudioso
Sr. Manager, Global Security Strategic Future
Sandia National Laboratories

Deborah Gordon
Executive Director, Preventive Defense Project
Stanford University

David "Chris" Hassell
Senior Science Advisor to the Assistant Secretary for Preparedness and Response
U.S. Department of Health and Human Services

Matthew Hepburn
Joint Program Lead for Enabling Technologies
Joint Program Executive Office-Chemical and Biological Defense
U.S. Department of Defense

Robert Kadlec
Assistant Secretary for Preparedness and Response
U.S. Department of Health and Human Services

George Korch
Director, Department of Homeland Security National Biodefense Analysis and Countermeasures Center
President, Battelle National Biodefense Institute

Brett Lambert
Managing Director
The Densmore Group, LLC

Duane Lindner
Consultant

Jason Matheny
Founding Director
Center for Security and Emerging Technology
Georgetown University

Andrew McIlroy
Associate Labs Director
Energy and Homeland Security
Sandia National Laboratories

Christine Parthemore
Director, Center on Strategic Weapons
Council on Strategic Risks

David Rakestraw
Science and Technology Advisor in the
Director's Office
Lawrence Livermore National Laboratory

Laura Regan
Senior Military Advisor to the
Director of the Office of Net
Assessment
U.S. Department of Defense

Joe Schoeniger
Manager, Systems Biology
Sandia National Laboratories

Anup Singh
Director, CBRN Defense and
Energy Technologies Center
Sandia National Laboratories

Andrew Snyder-Beattie
Program Officer
Open Philanthropy Project

Rajeev Surati
Inventor, Entrepreneur, and Investor

Kenneth Turteltaub
Division Leader
Biosciences and Biotechnology Division

John Vitko, Jr.
Consultant

Stan Wang
Non-Resident Senior Fellow
Council on Strategic Risks

Andy Weber
Senior Fellow
Council on Strategic Risk

COUNCIL ON STRATEGIC RISKS

The Council on Strategic Risks (CSR) is a nonprofit security policy institute devoted to anticipating, analyzing and addressing core systemic risks to security in the 21st century, with special examination of the ways in which these risks intersect and exacerbate one another. To further this goal, CSR currently hosts non-partisan institutes on climate and security (The Center for Climate and Security) and strategic weapons risks (The Center on Strategic Weapons), as well as a program designed to study converging, cross-sectoral risks (The Converging Risks Lab).

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2020-2472R.

NNSA National Nuclear Security Administration