# Competitive Symposium

## A Model for Interactive Learning and Policy Innovation


Center for the Study of WMD Weapons of Mass Destruction

Program for Emerging Leaders
Winter Workshop
2-3 March 2017

**Center for the Study of Weapons of Mass Destruction**
National Defense University

MR. CHARLES LUTES
Director

MR. JOHN P. CAVES, JR.
Deputy Director, Distinguished Research Fellow

Since its inception in 1994, the Center for the Study of Weapons of Mass Destruction (WMD Center) has been at the forefront of research on the implications of weapons of mass destruction for U.S. security. Originally focusing on threats to the military, the WMD Center now also applies its expertise and body of research to the challenges of homeland security. The center's mandate includes research, education, and outreach. Research focuses on understanding the security challenges posed by WMD and on fashioning effective responses thereto. The Chairman of the Joint Chiefs of Staff has designated the center as the focal point for WMD education in the joint professional military education system. Education programs, including its courses on countering WMD and consequence management, enhance awareness in the next generation of military and civilian leaders of the WMD threat as it relates to defense and homeland security policy, programs, technology, and operations. As a part of its broad outreach efforts, the WMD Center hosts annual symposia on key issues bringing together leaders and experts from the government and private sectors. Visit the center online at http://wmdcenter.ndu.edu/

**Cover Photo:** Katie Lewis, National Defense University

# COMPETITIVE SYMPOSIUM

## A Model for Interactive Learning and Policy Innovation

Program for Emerging Leaders
Winter Workshop
2-3 March 2017

Justin Anderson and Natasha E. Bajema

National Defense University
Washington, D.C.
October 2017

# Table of Contents

# Introduction

## What is a Competitive Symposium?

Chuck Lutes, Director, Center for the Study of Weapons of Mass Destruction (WMD Center)


The threat posed by weapons of mass destruction (WMD) remains one of the nation's most pervasive national security challenges. As nation states and terrorist organizations seek ways to challenge America's global role, they will increasingly pursue unconventional and asymmetric means to threaten U.S. interests. The potential for nuclear, chemical, biological, or radiological weapons to create unmatched devastation and effects marks WMD as an existential danger to our nation. It is vitally important that we maintain a vibrant community of education and scholarship that understands the destructive nature of these weapons and the tools available to counter them.

Throughout its history, the WMD Center has maintained a broad mandate for education, research, and outreach and has been on the frontlines of policy innovation on pressing and emerging WMD issues, such as interdiction, elimination, consequence management, deterrence, and escalation management.

The Competitive Symposium held on 2-3 March 2017 is a new initiative of the WMD Center designed to leverage the three components of the Center's mandate together with our WMD expertise on staff and growing cadre of next-generation military and civilian leaders with knowledge of the WMD threat—the Program for Emerging Leaders (PEL) and the Countering WMD Graduate Fellows Program. The goals of the Competitive Symposium are to foster innovative thinking for responding to the dangers of WMD, to strengthen collaboration across the U.S. government in countering WMD, and to build a strong community of future leaders for countering WMD.

What is a competitive symposium? The following report provides a detailed overview of the structure, implementation and outcomes of our first competitive symposium. As a working definition, we propose a competitive symposium to be an interactive, competitive, collaborative, substance-driven workshop designed to generate policy innovation and creative ideas for solving the critical WMD challenges facing the United States. We expect the concept to evolve as the Center proceeds with this initiative in the future.

As a Center, we brainstormed three complex challenges to test the creative mettle of PEL members and CWMD Graduate Fellows: Do-It-Yourself WMD, Cyberattacks against Critical Infrastructure, and the Nuclear Deterrent for the 21st Century. Twelve teams competed to

develop innovative proposals addressing one of these important challenges, and one team won the CSWMD Policy Innovation trophy. We offer our congratulations to **Team 11: Beautiful Strategy**!

## A Model for Interactive Learning

Natasha E. Bajema, Senior Research Fellow, WMD Center

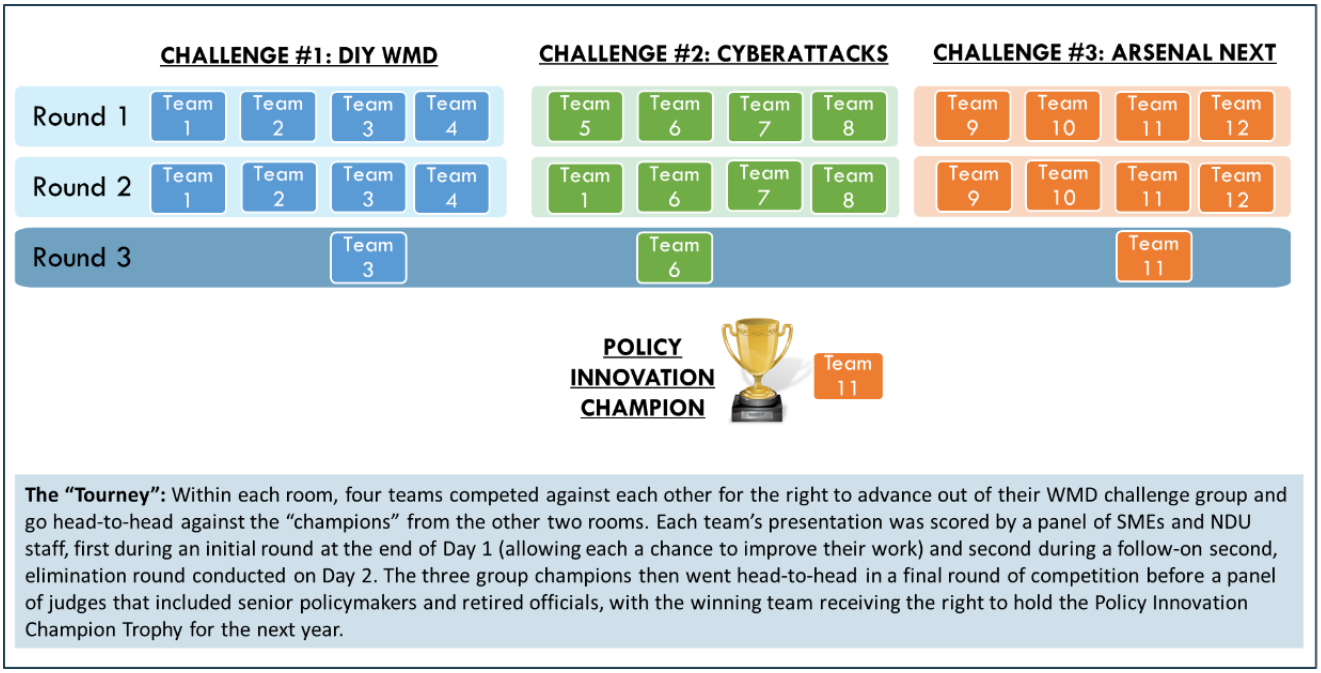

Given the major focus of the WMD Center on education, we gave careful thought to designing the **Competitive Symposium** as a new model for interactive learning on WMD issues. As a Center, we established several key objectives up front. We aimed 1) to challenge participants with complex topics; 2) to provide an opportunity for participants to advance their professional skills; and 3) to offer a chance for next-generation leaders to think outside the box. In other words, even before we hashed out the logistical details, we set high expectations for the event.

The Competitive Symposium was in itself an innovation for the Center (and perhaps more broadly for the academic community), and our event design began from scratch. The WMD Center brainstormed three timely and complex WMD-related topics to intellectually challenge the participants: DIY WMD; Cyberattacks against Critical Infrastructure; and a Nuclear Deterrent for the 21st Century.

To achieve all of our ambitious objectives, we focused on three main criteria for the event design. We sought: 1) to maximize participation; 2) to minimize repetition; and 3) to provide opportunities for improvement. The competition was structured into three rounds. All teams advanced automatically to round two and received an opportunity to improve their proposals and presentations.

In order to **maximize participation**, we needed to ensure that eliminated teams remained engaged until the conclusion of the event. For this reason, we asked the judges in the final round to assess and critique the proposals, asking tough and probing questions as they would ask of their own staff in their government positions. In this way, participants in the audience gained insight into the experience of pitching a new proposal to U.S. government senior leaders.

In terms of the event design, we struggled to **minimize repetition** over three rounds of competition, i.e., hearing the same briefing more than once (albeit improved versions). Originally, we considered structuring the competition using a bracket approach, but we eventually settled on two competition rounds in breakout groups and a final round in plenary due to the time limitations of the two-day event. In the end, we agreed that participants could still learn something by watching their competitors present the




same idea over multiple iterations, each improving on the previous.

Beyond the substantive component, however, we also wanted participants to have a chance to hone their professional skills, e.g., articulating and presenting a new idea. For this reason, we prioritized providing an opportunity for participants to improve their proposals. We invited SMEs to assist during the brainstorming and proposal formulation sessions. We also invited former senior government officials to serve as Senior Mentors and provide advice on formulating policy and finalizing presentations.

Early on, we decided that the pilot effort would be integrated into the programming for PEL and CWMD Graduate Fellows and chose the two-day PEL Winter Workshop as the ideal opportunity to test the new concept. This approach offered both advantages and disadvantages for the event's design. On the positive side, it allowed the Center to leverage our growing community of future leaders with knowledge of, and interest in, WMD. It also allowed us to build upon our current educational efforts. However, the two-day event imposed some constraints on the Competitive Symposium as originally conceived. Initially, we wanted to allow teams to form in advance (based on certain criteria) and give them time to develop their own proposals for addressing a pressing WMD challenge. Teams would then submit these proposals for admission to the two-day competition.

Future symposia may take this approach. Due to time constraints, the pilot effort focused on a two-day competition without advanced preparation. As a result, participants were compelled to develop their proposals and compete against other teams as part of a whirlwind two-day event. Although participants signed up in advance for their preferred WMD challenge, they met their teams (8-10 people each) for the

first time at the event. To prepare participants for the substantive component in advance, we developed introductory papers and reading lists on each of the three WMD challenges.

After a brief plenary session, participants headed to one of three rooms, each devoted to a different WMD challenge. In each room, participants divided up into their pre-assigned teams. We kicked off the proposal development phase with briefings by subject matter experts (SMEs).

Following this substantive introduction, the teams began brainstorming and formulating their proposals. Throughout the competition, SMEs and Senior Mentors remained on hand in each of the WMD challenge rooms. Teams were required to interact with them regularly as a way to improve their approach to a complex WMD challenge, but also to simulate the need to consult experts in a real-world environment.

At the end of the first day, teams gave an initial presentation to a panel of SMEs, who offered a (gently) critical initial evaluation intended to help them get ready for the next day's competition. The second day started with an opportunity for teams to review and improve their presentations with assistance from SMEs and Senior Mentors, followed by two rounds of competition. The second day culminated in the "winning" team from each room presenting before a panel of esteemed judges and live audience in NDU's Lincoln Auditorium.

The judges critiqued the proposals based on accepted policy analysis criteria such as technical feasibility, political viability, efficiency, effectiveness and equity. Proposals were also judged for their innovation, quality of presentation and evidence of teamwork. Every person in the auditorium had a chance to vote for the competition winner. Our Center Director awarded the CSWMD Policy Innovation Champion trophy to the winning team, "Beautiful Strategy."

The Competitive Symposium offered next generation military and civilian leaders a unique opportunity to think outside the box, to develop fresh ideas in the CWMD mission space, and to engage senior leaders beyond normal day-to-day activities.

## A Model for Policy Innovation

Justin Anderson, Research Fellow, WMD Center

In addition to its focus on education, the Competitive Symposium represented a pilot effort of the Center for the Study of WMD to encourage the innovative development of policy proposals addressing simulated real-world challenges during a two-day event. In planning the Competitive Symposium with policy innovation in mind, we sought to develop an event with the following elements:

1. **A critical, compelling challenge for all participants.** Necessity is the mother of invention and innovation. We worked to develop WMD challenges that presented the symposium's teams with a compelling, complex problem set, while also deliberately limiting the time and resources available to develop a solution.
2. **A positive, problem-solving environment.** Innovation is also fostered within an environment where all members of a team, project, initiative, or office are encouraged to introduce new ideas, develop new ways of conceptualizing a problem, and can collaborate to develop a solution. We sought to balance the imposition of time and resource constraints by providing a setting that encouraged the open sharing of ideas and creative brainstorming.
3. **A (friendly and structured) competition between teams.** We also designed the event to feature a friendly competition between the participant teams. Competition can also catalyze innovation, particularly if there is some form of incentive involved.

To create a positive environment for policy innovation, we sought to integrate all three concepts into the design and development of the competitive symposium.

### *A Critical, Compelling Challenge*

**Each of the teams was assigned a cross-cutting WMD problem.** Each of the WMD challenges was developed in a manner where the policy issues raised, the areas of responsibility and authority involved, and other elements of the challenge cut across different areas of expertise. None of the challenges, for example, was purely a military problem. Different challenges required teams to consider variables such as the needs of domestic constituencies or the concerns of foreign allies, simulating the complexities inherent in contemporary WMD challenges faced by the U.S. government.

**The teams also faced built-in time and resource constraints.** Proposed policy solutions require resources to become reality. Resources, however, are always finite. Many challenges also unfold along tight timelines. Teams had to work against a deadline of a few hours to develop a proposal—and an accompanying presentation—to address their assigned challenge. All three challenges also included some form of fiscal constraint or budgeting requirement, with teams asked to either remain under a cap or provide a detailed explanation of how they planned to allot resources to develop a new initiative, program, or technology to address their WMD challenge.

*Fostering a Positive, Problem Solving Environment*

**The symposium was designed as a free and open environment for introducing new ideas and developing new approaches to address policy challenges.** We sought to establish an environment where all participants were encouraged to offer their ideas and experiment with new and different ways to address WMD challenges—within certain parameters, such as a requirement to meet a number of designated policy objectives. Throughout the event, the organizers and invited SMEs communicated the message to participants that new ideas and hypotheses could and should be shared freely within their teams. The WMD challenges were also written in a manner intended to provide space for participants to develop their own unique solutions to the problem(s) at hand. In addition, SME evaluation of each group's initial presentation of their policy proposal focused on ways to further develop the new and innovative elements within their presentations instead of solely critiquing their content or presentation style. Overall, we worked to ensure that participants were encouraged to offer new and different ways of looking at, and attempting to resolve, difficult challenges—and could do so without feeling they would be penalized if their ideas seemed unorthodox.

**The event also sought to model and encourage Interagency collaboration.** The development of "whole of government" policy solutions requires knowledge and skill sets resident within different departments, offices, and agencies of the U.S. government. The Competitive Symposium assigned all participants to teams that included representatives from different parts of the government in an attempt to reflect the diversity of the Interagency process (each team was also a mix of civilian and military personnel). In addition, the different WMD challenges did not lend themselves to straightforward solutions, requiring the teams to work together as a "mini-Interagency" to develop a proposed way ahead that included resources and expertise drawn from across the U.S. government.

*A (Friendly and Structured) Competition of Ideas and Solutions*

**The symposium was developed as a (friendly) "peer-to-peer" competition.** Competition also fosters innovation; the symposium sought to foster a friendly competition between peers that would incentivize new and creative policy proposals. The event was structured as a two-tiered competition, with teams within each WMD challenge grouping competing against each other in order to advance to the next round and the opportunity to square off against the "champions" from the other two WMD challenges. This competitive structure was intended to help keep all participants interested, motivated, and engaged as they sought to work with their teammates to develop proposals that would compete with proposals from other teams made up of their PEL or CWMD Graduate Fellow peers. During the event, participants needed to balance an interest in developing and honing their presentations in order to score well with the SME evaluators while also remaining collegial with the other teams.

**The symposium also included SME mentoring and assessment.** Another key element of the competition was the involvement of outside SMEs. Teams had access to these SMEs throughout the development of their proposals, and many took the opportunity to ask questions that helped inform and refine their proposals prior to evaluation by expert panels. The presence of these SMEs, to include senior officials who had developed policy on the topics featured within the challenges, also served as an additional incentive for participants to put together—and put forward—the best possible proposals and presentations.

## The WMD Challenges

### Challenge #1: Do-It-Yourself WMD

Natasha E. Bajema, Senior Research Fellow, WMD Center

In the first challenge, entitled "Do-It-Yourself (DIY) Weapons of Mass Destruction", four teams wrestled with the growing risk posed by a variety of emerging and broadly accessible technologies that could be used to develop new and novel forms of WMD. In the past, governments have primarily developed, invested in, owned, and employed advanced technologies. Today, private companies and individuals are making advances in domains that were once the exclusive territory of governments. The "democratization of science" has led a broad range of emerging technologies increasingly driven and controlled by the private sector and private individuals rather than national governments.

In recent years, sophisticated technologies such as synthetic biology, additive manufacturing (3D printing) and advanced robotics (commercial drones) have all experienced growth, largely beyond the purview of governments. These new technologies have given rise to DIY communities in fields that were once the exclusive domain of trained scientists and manufacturers. This trend has produced new challenges for governance, especially for emerging technologies that involve significant consequences if the technology were used for nefarious purposes related to WMD.

In fact, emerging technologies may be leading to a meaningful paradigm shift in how policymakers view the threat of WMD, how to counter WMD, and potentially what could be defined as WMD. Most of the tools and approaches to counter WMD have been around for decades, and even the more current approaches are not designed to account for risks associated with such emerging technologies. Moreover, many of the policymakers responsible for developing policy to counter WMD have little to no insight into, or impact on, the life cycle of emerging technologies that may impact the WMD space.

For this challenge, teams played the role of an interagency working group, jointly sponsored by Office of Science and Technology Policy (OSTP) and the National Security Council (NSC) at the White House. Teams were tasked with developing an innovative proposal for the President with recommendations for managing the risks of DIY WMD, particularly those posed by additive manufacturing, unmanned aerial vehicles and synthetic biology.

In order to prepare the teams to address the complex range of policy and strategy challenges inherent to their task, participants received three briefings from subject matter experts. Ed You from the

WMD Directorate of the FBI provided an overview of the DIY Bio community and the FBI's outreach efforts. T.X. Hammes, a Distinguished Research Fellow at NDU described the threats posed by emerging technologies such as drones and 3D printing. Mallory Stewart, former Deputy Assistant Secretary of State in the Bureau of Arms Control and Verification briefed the group on the governance challenges associated with emerging threats.

During the brainstorming process, each team resolved a number of issues before formulating their proposal. First, teams decided whether to focus on one or all of the emerging technologies of interest to the President. Teams that selected the former were then required to develop a justification for their decision to prioritize a single emerging technology.

Second, teams considered the appropriate policy intervention points for each emerging technology. The technology life cycle begins with basic scientific research and advances through different stages including lab experimentation, research to prove concept feasibility, early technology development, prototyping and technology demonstration, systems testing and deployment/commercialization. Once commercialized, policymakers can intervene upstream (manufacturing), midstream (supply chains) and downstream (end-uses) to shape policy outcomes. An intervention point is an opportunity in the development (technology life cycle) or production process where specific actions taken by policymakers can bias outcomes toward legitimate rather than illegitimate ends and/or lead to technology solutions which mitigate the potential risks.

Third, teams examined existing governance on emerging technologies and determined whether they planned to close a gap in existing governance or devise new ways to mitigate the risks of DIY WMD. Fourth, teams developed a detailed implementation plan that assigned and distributed responsibilities, included engagement of the private sector, and estimated the costs of their proposal.

The four teams on the DIY WMD challenge presented their proposals to subject matter experts over the course of two days. One team from this challenge advanced to the final round of the competition to face off with finalist teams from the other two challenges.

## Policy Proposal, Challenge #1: "Federally Funding Ingenuity: Incentivizing Threat Reduction in the DIY-Bio Community"

Sarah E. Davenport, Stephen Hummel and Habi Mojidi

For decades, access to biotechnology expertise and equipment necessary to alter genetic material was limited to major universities and pharmaceutical companies, mainly due to the enormous costs involved. Recently, however, the technology to conduct such experiments has become significantly cheaper. In addition, "biohackers" have pioneered creative alternatives to lab equipment and processes in their small garage-style labs, often making these technologies widely available via open source media, leading to a democratization of synthetic biology.

Do-It-Yourself (DIY) biologists and community laboratories have sprouted up in nearly every major American city, forming a massive and flourishing DIY Bio Community. Researchers with minimal formal education now have access to technical platforms and mentorship to enhance their knowledge of biology and genetics and discuss and apply experimental methods. DIY labs supply members with advanced equipment such as centrifuges, gene sequencers, and CRISPR (Clustered Regularly Interspaced Short Palindromic Repeats) kits, which enable genetic editing. Many of these biohackers are actively engaged in advancing biotechnology, which combines hands-on bench work with methodological analysis performed on various equipment with specific computer programs. This research provides a new potential opportunity for the federal government to gain access to insight and innovation outside the traditional laboratories.

The democratization of biology has several implications, some beneficial to society and others potentially threatening to U.S. national security. Advancements facilitated by the ease of genetic manipulation may lead to cures for diseases, many of which are not funded at the national level through accredited laboratories. Conversely, potentially harmful pathogens once relegated to secure and tightly monitored environments could be unintentionally released due to unsafe/unmonitored practices in DIY labs or easily synthesized or enhanced for nefarious purposes.

Today, DIY Bio takes place everywhere across the country—from makeshift setups in a closet or garage to community makerspaces and labs such as Baltimore's Under Ground Science Space (BUGSS), Boston's Open Source Science Lab, and Sunnyvale's BioCurious. The current biosecurity architecture is not well equipped to identify and ameliorate the vulnerabilities in the DIY Bio realm. Unlike the additive manufacturing space where the federal government has implemented standards and requirements mainly through the National Institute for Standards and Technology (NIST) and in collaboration with industry leaders, regulating synthetic biology is not easily encapsulated.[2] Regulating this complex multifaceted domain is not solely a law enforcement, commerce, or a counterterrorism issue, nor can it be accomplished by the myriad of federal

health agencies that lack enforcement mechanisms.

The U.S. government can adopt valuable lessons for DIY Bio from its efforts to regulate other emerging technologies. For example, the Department of Defense currently collaborates with industry leaders and academia to fund and regulate aspects of additive manufacturing. This collaboration has yielded funding for researchers and allowed the U.S. government to exercise influence in that arena. In the same way, if the U.S. government were to fund DIY bioresearch, it could set terms for the conduct of such research—to include biosafety measures, biosecurity and standardized reporting, etc. This arrangement would not only mitigate risks associated with lax safety procedures, it would allow the government to proactively identify new technologies that might have the potential to affect biosecurity, for good or bad. DIY Bio labs, receiving federal funding, would ensure that participants are registered in a database and that their research meets minimum safety regulations.

We propose that the U.S. government monitor DIY Bio practitioners and their projects through an incentivized self-identification platform—by replicating the "Kickstarter" model and creating public-private partnerships. Typically, the U.S. government utilizes contract support to fund research and development projects; however, the typical contracting process is arduous and extremely lengthy. Kickstarter is a crowd-funding website where would-be inventors or businesses pitch their ideas via short videos or media presentations. Members can invest in the project as little or as much as they desire, usually contributing at pre-established levels to eventually get an award. For example, an inventor may post a project to manufacture electric cars. This front-end crowd-funding enables companies to get start-up capital based on the quality of their ideas. Inventors offer incentives for members to invest early, for example, a significant reduction on the final market price.

The creation of a federal website and mobile app similar to Kickstarter would present an innovative platform where DIY Bio researchers and community labs could post proposals to be funded by government agencies. Agencies could use their formal or discretionary budgets to bid on proposals that meet their requirements. Not only would this approach streamline the arduous grant-writing and research, development, and acquisition (RDA) processes, saving time and money on staffing and review, but it would encourage greater participation—and therefore greater transparency into the DIY Bio community for the U.S. government. Throughout the process, the U.S. government should strive to maintain impartiality and enable novel solutions to unidentified problems. Once this process is fully implemented it would increase innovation while decreasing the costs, enhancing the use of the funds provided to the agency by U.S. Congress.

The Kickstarter format is one that is familiar to the DIY Bio community, which is largely comprised of young, tech-savvy and pop-culturally versed millennials. In fact, several DIY labs have used Kickstarter to fund themselves—this is a tested and vetted model. BioCurious funded a project through

a Kickstarter campaign in which 239 backers gave a total of $35,319 to create a Bio-Safety Level 1 lab open to the public.[1]

Engaging with the DIY Bio community on its level would reap several benefits. The government could post high-priority technology needs, and individual labs or DIY Bio researchers could bid on them like a contract. This approach would attract innovative solutions and decrease the cost of the request-for-proposal acquisition process. If well-received, this platform would allow the government to steer the future of DIY biotechnology and drastically cut costs and time for the research, development, and acquisition processes.

The Kickstarter approach would offer the U.S. government a proactive eyes-on approach to monitor new developments in the DIY Bio community and encourage contacts that may have been avoided with a purely law-enforcement/counterterrorism approach. The initial response to science conducted outside the laboratory has been one of both interest and fear—often labeling the DIY Bio community with a reputation somewhere between "nerd" and "terrorist." This stigma has left many in the DIY Bio community reticent to proactively identify themselves to government officials, and many reject the idea of registration of any kind. The U.S. government is not likely be successful in addressing risks posed by the DIY Bio community by treating potential assets as criminals. By allowing the DIY Bio practitioner to initiate a relationship with the U.S. government through the Kickstarter-esque app or website, the government would reap the benefits of information, vetting, and reporting while leveraging the DIY Bio Community to solve pressing challenges.

## Challenge #2: Defending Critical Infrastructure against Cyberattacks

Harrison Menke, Research Analyst, WMD Center

In the second challenge, four teams were tasked with assessing whether some cyber-attacks (e.g. against critical infrastructure) should be considered the same as WMD attacks and developing actionable solutions designed to mitigate the risks posed by cyber. In the 21st century, societies will become increasingly dependent on networked information systems. While these technologies enhance efficiency and accessibility of information, they also create new vulnerabilities that could be exploited by potential adversaries seeking to create devastating damage—leading some to suggest that high-end cyber-attacks against

[1] BioCurious Kickstarter, https://www.kickstarter.com/projects/openscience/biocurious-a-hackerspace-for-biotech-the-community, accessed on 25 April 2017.

[2] GAO Report 3D Printing Opportunities, Challenges, and Policy Implications of Additive Manufacturing Kickstarter, http://www.gao.gov/assets/680/670960.pdf, accessed on 24 May 2017.

critical infrastructure could produce severe political, psychological and, in some cases, physical effects similar to a traditional WMD event.

Critical infrastructure provides the foundation for modern American life, from electric power to telecommunications to clean water. To manage these resources, governments have increasingly adopted networked systems to improve their efficiency, accessibility, and reliability. But the growing connectivity of these critical infrastructure systems have created new risks and increased their vulnerability to a devastating cyber-attack. If a legitimate operator can remotely access a key component of one of these critical infrastructure systems to conduct routine operations, then an actor with malicious intent may be able to exploit the same connectivity to inflict harm.

Damage from cyber-attacks can range from minor and temporary to massive and enduring. U.S. critical infrastructure presents a lucrative target for potential adversaries armed with cyber weapons. The comprehensive nature of this threat demands close interagency coordination to ensure effective policies for prevention, protection, response, and recovery.

During this challenge, teams assumed the role of a special interagency task force reporting to the Homeland Security Advisor. Teams were directed by Presidential guidance, which sought to strengthen the nation's critical infrastructure structure defense against large-scale cyber-attacks intended to cripple U.S. society and economy by creating massive disruption and destruction. Each team was asked to prepare and present a proposal which would examine whether and how cyber-attacks against infrastructure should be considered to be a WMD attack, and present policy recommendations designed to mitigate the risks of a WMD-like cyber-attack.

In order to prepare the teams to address the complex range of policy and strategy challenges inherent to their task, participants received three briefings from subject matter experts. Seth Carus, Distinguished Research Fellow at NDU, discussed the challenges associated with treating cyberthreats like WMD. Brandon Wales from the Office of Cyber and Infrastructure Analysis at DHS, discussed the diverse range of cyber vulnerabilities of critical infrastructure systems. Alex Crowther, Senior Research Fellow at NDU, briefed the group on the spectrum of cyberthreats facing the United States and the challenges of countering them.

Each proposal responded to three focused questions. First, teams contemplated whether cyber-attacks against critical civilian infrastructure that cause significant damage and/or casualties should be explicitly considered WMD attacks. Teams then needed to assess the policy, legal, and resource implications of doing so.

Second, teams questioned whether the Executive Brach and the broader intergovernmental structure (federal, state, local) was effectively organized to develop and execute a cutting-edge set of solutions to protect critical infrastructure. Teams sought to identify seams and gaps in U.S. policy and structure, providing and justifying

new concepts to redress current vulnerabilities.

Finally, teams considered the key features of an innovative national, strategic-level campaign to develop guidance to mitigate the risks posed by cyberattacks directed at civilian infrastructure. Thus, it was necessary to first review current policy approaches such as Presidential Policy Directive 41 and then assess whether it was necessary to either develop new policy, readjust some elements within current policy, or simply maintain the current approach.

The four teams on the Cyber-WMD challenge presented their proposals to subject matter experts over the course of two days. One team from this challenge advanced to the final round of the competition to face off with finalist teams from the other two challenges.

### Policy Proposal, Challenge #2 "Strengthening Public-Private Partnership in Cybersecurity"

Bryan Reed and Christina Richards

Existing public-private partnerships are ineffective in combating cyber threats against critical infrastructures. Legal, strategic, and pragmatic obstacles impede effective public-private sector communications, which compound regulatory and civil-liability risks. As such, it is incumbent on both the public and the private sectors to capitalize on each other's strengths. One step would be to incentivize the use of cybersecurity standards.

Cybersecurity standards exist; however, there is little success in applying the standards consistently across both the public and private sectors. There are several possible reasons for this, to include issues with "info sharing" and proprietary information, trust, and agreement on what the standards ought to be. The first step might be to create an organizational-level cybersecurity certification standard; however, even if one were created, could there be sufficient incentive to pursue this type of certification? To address this question, we have to ask "what's in it" for both sectors. For the government, protection of national security interests by increasing private sector resilience is of primary concern. In the case of industry actors, the facts on the ground are becoming increasingly clear; as U.S. Cyber Command Commander Navy Adm. Mike S. Rogers said in November 2016: "It's unrealistic to expect the private sector alone to withstand the onslaught of activity that is

being directed against them by nation-states and other actors."[2]

With that in mind, there is one approach that might prove valuable: to conceptually develop a widely recognized, positive standard of certification similar to the Leadership in Energy and Environmental Design (LEED). To briefly summarize, organizations that are building construction projects (at all phases of development) can pursue a LEED certification. An organization earns points across several areas that address sustainability issues. Based on the number of points achieved, a project then receives one of four LEED ratings levels: Certified, Silver, Gold, and Platinum.[3] These certifications have value as they relay to the consumer that LEED buildings are resource efficient, use less water and energy, reduce greenhouse gas emissions, and save money.

Why not apply the LEED concept to provide a similar certification for cybersecurity? Where LEED focuses on sustainability, we could focus on particular elements of cybersecurity such as data loss prevention, privacy, stronger access controls, etc., with higher levels representing the achievement of a certain level of points across elements. Participants, both in public and private sectors, would obtain a certification signaling a higher level accreditation; this could be considered a weighted factor in contract award decisions. For example, a cybersecurity credential awarded to an organization would signify that the company is both a leader in the field and an active participant in pursuing better means and methods for cybersecurity. By putting forth the possibility of a monetary reward for higher cybersecurity standards—through increased consumer confidence, which could lead to increased business— one incentivizes the private sector in familiar financial terms. Additionally, similar to programs such as having a Project Management Professional certification, the proposed cybersecurity certification standard provides value over time as the ongoing maintenance of the certification continues to signal to consumers—both private and corporate—that the industry partner has an established focus and has developed trust in the highest levels of cybersecurity.

Moreover, the certification standard provides a familiarization for industry and government actors in terms of responding to a cybersecurity incident as key players would have established points of contact, protocols, and procedures in a crisis. Additionally, in conjunction with the incentives of the certification program, legislators could reciprocally roll back applicable insurance regulations, facilitating the market for insurers to offer data loss coverage to companies, further incentivizing industry adoption of a strong cybersecurity certification. These insurers would be underwriting policies worth millions of dollars and they would impose very rigorous cybersecurity standards upon those companies they insure. The better your

---

[2] Cheryl Pellerin, *DoD News, Defense Media Activity,* "Cybercom Commander: Public-Private Partnerships Needed for Cybersecurity," 16 Nov 16, https://www.defense.gov/News/Article/Article/1006807/cybercom-commander-public-private-partnerships-needed-for-cybersecurity, (Nov 16, 2016).

[3] *Better Buildings are our Legacy*, http://www.usgbc.org/leed

cybersecurity posture, the lower your premiums.

Without a true partnership between industry and government, it will continue to be difficult to thwart cybersecurity threats. We recognize there is a need to bolster the existing cybersecurity infrastructure, breakdown stovepipes in public-private cooperation, and incentivize implementation of higher standards in cybersecurity. With advances in technology, the willingness of actors to use cyber as a weapon, the costs associated with mitigation and clean up, and the "non-attribution" aspects of cyber threats are all significant challenges that simply cannot be ignored. By utilizing a LEED model style certification to incentivize cybersecurity standards, both public and private sector actors would have a means to bolster consumer/public confidence, and specifically differentiate, characterize, and recognize cybersecurity behaviors to begin to establish a more level playing field in an already active cyber threat environment.

## Challenge #3: Arsenal Next: A Nuclear Deterrent for the 21st Century

Justin Anderson, Research Fellow, WMD Center

In the third challenge, four teams were tasked with: 1) developing a new U.S. nuclear deterrence strategy that could address current and future nuclear and other WMD threats to the United States and its allies; 2) developing a nuclear deterrent force (offense and defense, the latter in the form of missile defenses) that could fully and effectively implement this strategy; and 3) ensuring this planned force did not break a pre-set budget limit.

The scope of the challenge presented to the teams was both global and complex in nature, requiring teams to assemble a force that could deter four potential adversaries (each equipped with a different WMD arsenal) while also fulfilling nuclear extended deterrence guarantees to allies in three separate geographic regions (Europe, Asia-Pacific, and the Middle East). The teams were also asked to consider a number of other critical factors, to include what mix of offensive and defensive forces would best deter adversary efforts to intimidate, coerce, or commit aggression against the United States and its allies, and—with regard to their offensive forces—what force structure they would choose to employ (to include whether to retain the current U.S. "triad" of long-range nuclear platforms (intercontinental ballistic missiles (ICBMS), submarine-launched ballistic missiles (SLBMs), and long-range bombers).

While a number of specific details of the scenario were fictionalized, the diverse range of policy and strategy requirements were derived from real considerations faced by U.S. policymakers and strategists working on nuclear deterrence issues. The potential synergies or trade-offs between different offensive and defensive systems—each bringing different capabilities to the U.S. military, and each having a different price tag—were also drawn from past and present debates on the U.S. nuclear deterrent. The scenario was also a topical one, as the United States is presently considering a range of options for modernizing and replacing its aging nuclear deterrent force. As such, the scenario was also informed by

contemporary debates regarding how much the United States should spend to upgrade its nuclear forces (and the nuclear complex that supports them) as well as how to respond to challenges such as Russia's comprehensive overhaul of its nuclear forces and North Korea's pursuit of a larger and better-equipped arsenal (to potentially include ICBMs).

In order to prepare the teams to address the complex range of policy and strategy challenges inherent to their task, participants received three briefings from subject matter experts. Ambassador Linton Brooks, lead negotiator for the Strategic Arms Reduction Treaty (START) briefed the group on force structure considerations; Elaine Bunn, former Deputy Assistant Secretary of Defense for Nuclear and Missile Defense Policy, briefed the group on nuclear deterrence strategy; and Amy Woolf, the Congressional Research Service's lead for nuclear force analyses, briefed the group on Congressional perspectives on budget and policy matters regarding the U.S. nuclear deterrent.

The teams then turned to their assigned tasks. In order to facilitate their efforts to build and cost a nuclear deterrent force, the teams were provided with spreadsheets preloaded with number/cost formulas for different platforms and weapons in order to provide them with a running tally of their overall costs (and allow them to ensure they remained below the pre-set cap). Within these parameters, however, the group facilitator and SMEs assisted teams as they worked to address the range of critical policy and strategy requirements their force needed to fulfill. Teams worked to tailor their strategies to address challenges posed by different adversaries while simultaneously balancing geographic requirements that demanded splitting forces between different regions—without losing sight of the requirements for U.S. homeland defense. Teams found that their tasks did not lend themselves to a sequential "build"; instead, strategy and policy requirements had to be considered and addressed simultaneously, as attempting to resolve any one adversary deterrence or allied assurance challenge on its own inevitably had consequences for other challenges.

Each of the four teams delivered their briefings to a SME panel, received feedback, and had the opportunity to brief a second time. Each of the teams presented a unique strategy and force structure, include proposals to change the geographic balance of the U.S. nuclear deterrent and re-considering previously retired systems to address specific new and emerging adversary challenges.

### Policy Proposal, Challenge #3: "A Flexible Force Posture"

Steve Cooper, Alex Mikulski, Jeanine Frazier, A. Mark Diglio, Thomas Moon, David Herndon, Kelly Shannon, Gregory Watson

Team 11 outlined a new nuclear deterrence strategy for the United States based on the scenario given in the *Arsenal Next* challenge. The challenge provided options to select or modernize various elements of the nuclear triad based on a credit system that represented the actual nuclear defense budget. Our group sought to design a strategy capable of deterring several different types of nuclear-armed

adversaries, to include a nuclear peer and an increasingly risk-acceptant small (but growing) nuclear power, all while keeping within strict budget constraints. Our strategy called for lowering the number of ICBMs and SLBMs from the current baseline. We proposed to invest the cost savings from these ballistic missile reductions in a modernized strategic bomber force, increased missile defenses, and a new nuclear-capable cruise missile for U.S. attack subs. Our rebalance within the triad would provide an increase in overall capabilities, a strategic ability to counter a wide variety of threats from new adversaries, and a modest three percent cost savings to reinvest in additional conventional capabilities or go towards paying the U.S. national debt.

Drawing from deterrence theorists such as Bernard Brodie, Thomas Schelling, Kenneth Waltz, and Herman Kahn, among others, our group anchored our strategy on the assumptions that successful deterrence must be based on credible threats. This includes capabilities, the resolve to employ these capabilities, and the clear communication of a deterrence strategy that can be accurately interpreted by adversaries and allies alike. Our strategy attempts to achieve three objectives: deter our adversaries, assure our allies, and provide maximum flexibility within budget constraints

Specifically, we recommended that the U.S. government reduce our land-based ICBM force by one-third, leaving a total of 300 ICBMs. The 300 ICBM force is sufficient based on the key constraining factor of ICBM employment which is that, to reach many points on the globe, the ICBMs must first overfly Russia. Russian overflight complicates their potential use against other adversaries; however, it does not preclude potential use, especially in large-scale scenarios. Additionally, we recommended that the U.S. government reduce its ballistic missile submarine fleet (SSBN) to six Ohio-Class submarines, and move them to be based in the Pacific area of operations. The SSBNs in the Pacific will still be able to range most potential targets within current nuclear-armed adversaries, and these potential ballistic missile employments can be conducted so they do not overfly Russia, in the case of non-Russian targets. This was deemed critical for avoiding potential conflict or tension escalation with Russia.

The cost savings of the ICBM and SSBN rebalance aided in the procurement of 100 of the United States' planned next generation strategic bomber, the B-21. The cost savings also: allowed for an upgrade to 60 B-52s to extend their service life; procured 100 next generation tankers; procured one national missile defense (NMD) site; and added three theater missile defense (TMD) systems with full armament (per the scenario we had two TMDs without any interceptors). Rounding out the changes, we recommended converting ten Virginia-class attack submarines to become nuclear-capable with ten submarine-launched cruise missiles (SLCM) each, for a total of 100 SLCMs. In addition, 100 modernized dual-capable aircraft (DCA) were funded at the scenario baseline.

Our rebalancing of capabilities ultimately yields more flexible response options than the baseline nuclear force. This is particularly true for lower scale scenarios.

We took comments by Senior Mentors to heart about the importance of reassuring allies. One senior mentor mentioned that there are many options to reassure allies. One tactic is to bring your weapons systems to your allies, describe their capabilities in detail, and outline their advantages. Another senior mentor mentioned that although a mammoth capability like an ICBM or a Trident II missile (from an SSBN) might seem more overwhelming than a lower-yield weapon, there is something to be said with respect to reassurance about parking capabilities in your allies' backyard (in our case, we envisioned utilizing our DCA, nuclear-armed attack subs, and/or TMD in this role).

Our recommendations would allow national leaders more response options, more options in general, and more credibility with proportional response options at every level of the escalation ladder. In particular, the SLCMs provide a survivable capability that can provide proportional options to lower-level threats. Additionally, according to the scenario, we procured a previously non-existent missile defense capability. These missile defenses add an element of robustness to U.S. deterrence strategy for lower-level scenarios and can increase reassurance for allies if the TMDs were placed in a germane area of regional concern. As threats to the United States evolve, our WMD policies, strategies, and defenses must also evolve. Any openness by policymakers to a new mix of deterrence capabilities can yield more capability in key areas while maintaining sufficient strategic capabilities to deter a large-scale first strike. More capability at lower levels of the escalation ladder coupled with strong defensive capabilities would improve our deterrence vis-à-vis new and emerging threats such as North Korea and Iran, while simultaneously increasing our flexibility to respond to lower end scenarios involving potential peer and near-peer adversaries.

## Senior Mentor Reflections

Susan Koch, Distinguished Research Fellow, WMD Center

The Competitive Symposium held in March 2017 was an exceptionally successful, innovative addition to the Program for Emerging Leaders (PEL), the CWMD Graduate Fellows, and the WMD Center lineup. I strongly recommend that it be retained, with only a few alterations to make it even more valuable to the participants.

The three challenges of the 2017 Competitive Symposium were well designed from several standpoints. They all involved vital issues whose importance to national and global security will only increase in the future. The issues covered also were all new and complex, with few if any "off the shelf" productive policy options available; thus they required real innovation by each of the teams. The background information provided to the participants was excellent, giving them a good foundation for their policy discussions. One suggestion: the Do-It-Yourself Weapons of Mass Destruction (DIY-WMD) challenge was very broad; I would recommend that future DIY-WMD teams be encouraged to choose to focus on just one of the three technologies. Each type of emerging technology was sufficiently broad, complex and important to warrant an exclusive focus.

My other suggestion would be to require the teams to present three or four policy options culminating in a recommended course of action. That approach would better reflect the actual policymaking process. It would also give the judges greater insight into each team's process in developing its proposed solution/strategy.

I was extremely impressed by the team members: at how seriously each team took this exercise; at the breadth and depth of their knowledge; at their analytic ability and innovative thinking; and at their ability to work as true teams. The participants were extraordinary, and it was a pleasure to observe them.

Finally, I thought the symposium's use of subject matter experts and mentors was excellent. We had complementary, rather than overlapping, skills and experience, making all of us useful to the teams. At least I hope the teams found us helpful. From this mentor's standpoint, our time was extremely well spent.

I conclude as I began. The Competitive Symposium was terrific – a very important addition to the already valuable WMD curriculum offered by the WMD Center. It enabled the PEL members and CWMD fellows to stretch their considerable talents in new directions, furthering in important ways the program's contribution to their future as leaders throughout the combating WMD community.

## Conclusion

Justin Anderson and Natasha E. Bajema


The Competitive Symposium represented a pilot effort by the WMD Center to provide an interactive learning opportunity on WMD issues that would encourage policy innovation.

The development of the event led the organizers to think hard about what kind of environment and exercise could foster innovation—while seeking to avoid the attitudes and obstacles that can stand in the way of creative thinking and problem-solving. We sought to design the event so that the Symposium could serve as a "policy laboratory" where teams could experiment with ideas, receive information back regarding what did and did not work, and have another chance to develop a solution. While time was limited, and the challenges complex, we were pleased with the results. The teams worked hard and came back with thoughtful, innovative proposals to help address some of the most pressing national security challenges currently faced by U.S. policymakers.

At the same time as encouraging creativity and experimentation, we also hoped to help participants critically review their own assumptions and proposals. The goal was not just innovation for innovation's sake. Some policies endure because they remain effective. But encouraging both creative and critical thinking can help develop the analytic capacity to determine which policy approaches remain vital and which have become ossified.

As our first iteration of this type of event, we also gained several interesting lessons learned for future policy innovation competitions.

First, the time available to participants proved a major constraint on the event. Over the course of one and a half days, team members met each other for the first time, brainstormed and formulated a policy proposal, designed slide presentations, wrote a two-page policy paper and presented their proposal twice to a panel of judges. In the future, we hope to have lead time prior to the competition during which prospective participants form their own teams (based on certain criteria), work together to build a policy proposal and submit materials in advance to apply to the competition.

Second, the role of SMEs and the opportunity to improve the proposals with expert input was an invaluable opportunity for participants. Our post-event survey revealed this aspect as the most beneficial with regards to both education and innovation. In future iterations, we plan to expand on interactions between participants and SMEs.

Finally, we noticed overall more energy among participants compared to

other event formats (e.g., lecture/panel). Part of our motivation for developing the event was an abiding frustration with "static" events where participation is limited to listening to speakers and perhaps having the opportunity to ask a question. There is mounting evidence in education and other fields that this is not an optimal approach for learning new information or developing new ideas.

By contrast, we sought to design the Symposium to ensure a constant level of activity and intellectual engagement. From our own experience in participating in the symposium and from event surveys, we believe we achieved these objective. Most people found the event to be engaging, educational and stimulating and left the event feeling that their time had been well spent.

Our thanks to all of those who helped with developing the event and to everyone who participated in this pilot effort. We are tentatively planning to hold our next Competitive Symposium in October 2018. If you're interested in participating, please check our website for further details or follow us on Twitter @WMDCenter.

For more information on the Program for Emerging Leaders or the CWMD Graduate Fellowship, please visit our website at http://wmdcenter.ndu.edu/

# Event Agenda

## Thursday, 2 March 2017

**0800-0805** **Introductory Remarks**
Mr. Chuck Lutes, Director, Center for the Study of Weapons of Mass Destruction

**0805-0810** **Welcome Remarks**
Dr. Mark Mattox, CWMD Graduate Fellows Program, Center for the Study of Weapons of Mass Destruction

**0810-0830** **Symposium Overview**
Dr. Natasha Bajema, Program for Emerging Leaders, Center for the Study of Weapons of Mass Destruction

**0830-0840** **Break**

**0840-1020** **Breakout Groups**
Subject Matter Expert Presentations & Discussion

**Challenge#1: Do-It-Yourself WMD**
Chair: Dr. Diane DiEuliis, Senior Research Fellow, Center for the Study of Weapons of Mass Destruction
Mr. Ed You, Supervisory Special Agent, WMD Directorate, Federal Bureau of Investigations
Dr. T.X. Hammes, Distinguished Research Fellow, Institute for National Strategic Studies (INSS), National Defense University
Ms. Mallory Stewart, Former Deputy Assistant Secretary of State, Bureau of Arms Control and Verification, State Department

**Challenge#2: Defending Critical Infrastructure from Cyberattacks**
Chair: Dr. Mark Mattox, Senior Research Fellow, Center for the Study of Weapons of Mass Destruction
Dr. Seth Carus, Distinguished Research Fellow, Center for the Study of Weapons of Mass Destruction
Mr. Brandon Wales, Director, Office of Cyber and Infrastructure Analysis (OCIA), Department of Homeland Security
Dr. Alex Crowther, Senior Research Fellow, Institute for National Strategic Studies, National Defense University

**Challenge#3: Arsenal Next: A 21st Century Nuclear Deterrent**
Chair: Dr. Justin Anderson, Research Fellow, Center for the Study of Weapons of Mass Destruction
Ms. Amy Woolf, Specialist in Nuclear Weapons Policy, Foreign Affairs, Defense, and Trade Division, Congressional Research Service
Ms. Elaine Bunn, Former Deputy Assistant Secretary of Defense, Office of National Missile Defense, OSD Policy
Ambassador Linton Brooks, Distinguished Research Fellow, Center for the Study of Weapons of Mass Destruction

| | |
|---|---|
| **1020-1030** | **Break** |
| **1030-1200** | **Team Working Groups**<br>Brainstorming the Policy Options |
| **1200-1300** | **Lunch with Senior Mentors** |
| **1300-1500** | **Team Working Groups**<br>Formulating Policy Proposals |
| **1500-1630** | **Breakout Groups**<br>Round 1 Competition |
| **1630-1645** | **Round 1 - Panel Deliberation** |
| **1645** | **Results & Closing Remarks** |

## Friday, 3 March

| | |
|---|---|
| **0755-0800** | **Opening Remarks** |
| **0800-0900** | **Breakout Groups**<br>Preparation for Round 2 |
| **0900-1100** | **Breakout Groups**<br>Round 2 Competition |
| **1100-1130** | **Break** |
| **1130-1145** | **CWMD Graduate Fellowship Program Update**<br>Dr. Mark Mattox, Center for the Study of Weapons of Mass Destruction |

**1145-1210** **PEL Certificates**
Mr. Chuck Lutes, Director, Center for the Study of Weapons of Mass Destruction

**1210-1230** **Group Photos, Marshall Hall Entrance**

**1230-1400** **Lunch**
Preparation for Round 3

**1400-1600** **Plenary Session**
Round 3 – Finalist Teams Present to Esteemed Panel of Judges

Chair: Dr. Natasha Bajema, Senior Research Fellow, Center for the Study of Weapons of Mass Destruction
Ms. Elaine Bunn, Former Deputy Assistant Secretary of Defense for Nuclear and Missile Defense Policy, OSD Policy
Mr. Phillip Dolliff, Acting Deputy Assistant Secretary of State for Nonproliferation Programs, Bureau of International Security and Nonproliferation, State Department
Mr. James Finch, Principal Director for Countering Weapons of Mass Destruction, OSD-Policy
Ambassador Laura Holgate, Former U.S. Representative to the Vienna Office of the United Nations and the International Atomic Energy Agency
Dr. Steven Wax, Chief Scientist, Research and Development Directorate (J9), Defense Threat Reduction Agency

**1600-1630** **Break**

**1630-1700** **Competition Results**