Dogs That Haven't Barked: Towards an Understanding of the Absence of Expected Technological Threats
A Workshop Summary

July 6–7, 2016

CGSR
Center for Global Security Research

LLNL-ABS-704446

LAWRENCE LIVERMORE NATIONAL LABORATORY

Table of Contents

This work was performed under the auspices of the U.S. Department of Energy

by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344

LLNL-ABS-704446

Executive Summary

Despite repeated and consistent warnings from government officials and many non-governmental analysts, terrorists or other non-state actors have not turned to more advanced technologies—like man-portable air defense systems (MANPADS) and biotechnology—to attack civilians, instead relying overwhelmingly on more "traditional" terrorist weaponry. In the relatively few cases of actual MANPADS or biotechnology use since the end of World War II, predicted impacts of high mortality rates and significant global economic disruption simply have not occurred. Why? How can these cases inform our analysis of rapidly evolving science and technology (S&T) that holds both great global promise and potential for harm?

Performing analysis and producing assessments of threats arising from the rapidly evolving world of S&T is an important function of the U.S. intelligence community as well as many non-governmental organizations. Since the end of the Cold War, the nature of the analysis problem has changed, requiring new approaches. Providing timely and actionable warning of threats to international security is the *raison d'être* of the intelligence function. However, the S&T threat environment is changing rapidly, from one concentrated on a single, relatively well-understood Cold War adversary to one of many adversaries with diffuse and evolving objectives. Moreover, because many of the emerging capabilities from the world of S&T are not specifically designed as weapons but instead support many applications, possession or development of a technology does not equate to belligerent motives. Consequently, S&T threat assessment today demands a more deliberate analytic process with adversary-specific models. Warning assessments must include characteristics of a technology, capacity of threat actors to adopt, and intent of threat actors to employ technology to do harm.

The history of MANPADS and biotechnology usage indicates that the presence or assessed capability of a specific technology is not a sufficient indicator of threat. MANPADS and biotechnology are very different types of threats that have both been associated with the potential to cause significant loss of life and economic damage for at least the past 30 years. But, in fact, usage of these technologies by non-state actors against civilian targets has been rare, resulting in relatively modest impacts, despite consistently dire warnings.

Accurate threat assessments related to both of these technologies require an understanding of the unique motivations, preferences, capabilities, and objectives of the different groups that may perpetrate an attack. These ultimately will determine specific technologies chosen—or not chosen—by individuals or groups seeking to do harm. Even then, for accurate threat assessment, knowing specifically who is involved and their ability to acquire or absorb requisite technical expertise is critical.

In addition to a more clear understanding of the people seeking to do harm, a better understanding of the people conducting threat assessments and the analytic processes they employ is required in order to improve S&T threat assessments. The hype that normally surrounds new and evolving S&T is vital to discovery and development, but can directly bias assessment. More rigor and a clear recognition of the biases inherent in S&T threat assessment are essential to producing more meaningful and policy-relevant assessments. Moreover, a

multidisciplinary approach that addresses the human factors, sociological factors, and cultural values of adversarial groups is required as part of a credible S&T threat assessment.

Finally, the management of threat analysis, particularly government intelligence analysis, should be scrutinized to determine practical ways in which to improve the analysis of S&T threats. As suggested throughout the workshop, there are many things that *should* be done to incorporate more of the human factors and to use more rigorous analytic methodologies. However, there are real limits to what managers of analytic resources *can* practically accomplish; more study of the limits would be productive. Finally, more discussion on how policymakers respond to the threat assessments they are presented with is needed.

Introduction

Lawrence Livermore National Laboratory's Center for Global Security Research (CGSR) hosted a workshop to investigate why some consistently predicted threats from science and technology (S&T) have not manifested with the impacts to international security as forecasted. During the workshop "Dogs That Haven't Barked: Towards an Understanding of the Absence of Expected Technological Threats," participants used two specific cases to focus the discussion: biotechnology and man-portable air defense systems (MANPADS).

The title of the workshop is a play on a piece of evidence Sherlock Holmes used to ultimately identify a horse thief in the story "Silver Blaze," published in 1894 by Sir Arthur Conan Doyle. In the story, a guard dog in the stable did not bark during the time of the crime, leading Holmes to infer that the dog knew the thief and to posit that the crime was an inside job. This is an example of what would be called a "negative case" in political science terminology. While explaining why nonevents do not occur is difficult, the intent of the workshop was to determine whether there were factors in the negative cases of biotechnology and MANPADS that were generalizable to the topic of S&T threat assessment. Is there something to be learned from negative cases that would lead to improved S&T threat assessment?

Attendees and panelists came from diverse backgrounds in academia, government, and industry from the U.S. and Europe with expertise in science and technology, biotech, stand-off weapon systems, intelligence, military operations, terrorism, and the study of S&T development.

The workshop observed the Chatham House Rule. All presentations and discussions were for non-attribution. Participants were advised that they were free to use the information received, but they could not reveal the identity or the affiliation of the speaker(s), nor that of any other participant in the discussions.

The primary goal of the workshop was to determine whether factors that contributed to the absence of the forecast threats of biotech and MANPADS were generalizable to threats from S&T more broadly. Why haven't threat actors employed biotech and MANPADS to the levels predicted, and, when they were employed, why haven't they had the expected impacts? Is there something we must better understand about the technology that may limit its use and effectiveness? Is there something about the motivations, intentions, and decision-making processes of threat actors that led to them to alternatives in nearly all reported cases? Are

established S&T threat assessment processes and practices flawed in some way that leads to inaccurate conclusions?

The workshop began with a contextual presentation on the role of S&T threat assessment and warning and a brief summary of threat warnings and impacts of biotech and MANPADS.

The workshop was composed of four expert panels to foster discussion:

- Panel 1: Considering the Science and Technology
- Panel 2: Considering the People
- Panel 3: Considering Threat Assessment
- Panel 4: Improving Threat Assessment

This summary is not intended to capture every point of discussion, but does include the range of viewpoints on the issues and seeks to give a general overview of the discussions that took place.

Role of S&T Threat Assessment and Warning

The workshop began with a presentation on the role and importance of impactful assessment of threats and potential threats from S&T.

Key points:

- The S&T threat environment is changing with cumulative effects: a single Cold War adversary threatening annihilation with S&T developed in a highly structured government has evolved to threats of terrorism from numerous adversaries with diffuse objectives and access to globalized, multi-purpose, adaptive S&T; a future threat of information dominance, with threats materializing rapidly with no anticipation, and denial of capabilities without physical force.
- The S&T context has changed: Mere possession of a technology no longer implies or demonstrates capacity to carry out a threat (the impact of dual-use technologies); understanding intent and capacity of potential adversaries is critical.
- Analysis of S&T threats has changed: Cold War adversary decision-making was centralized in small politburo; information scarcity has been replaced by information abundance.
- New issues dominate, bringing new challenges: penetrating “denied minds” not accessing denied areas.
- Today’s technology warning function requires more integrated and holistic analytical processes, not just assessment of emerging technology.
- Warning requires adversary-specific model for each threat actor.
- Warning assessments must include *characteristics* of a technology, *capacity* of threat actors to adopt, and *intent* of threat actors to employ technology to do harm.

The presenter discussed the intersection of technology and policy, stressing the importance of prioritizing specific threats—to include latent ones—instead of just warning of S&T threats broadly, and assessed the changing structure of the S&T threat environment. During the Cold War, assessment of S&T threats was focused on a single adversary: the Soviet Union. Today,

with a focus on non-state/terrorist actors around the world, S&T threat assessments are much broader in scope and concern a globalized threat. Not only has the focus evolved, but assessing intentions of a new diffuse, globalized adversary is much more challenging than the Cold War effort against the intentions of a centralized politburo. The new challenges are penetrating "denied minds" and not denied territories as before, and, as a result, today's intelligence community must contend with fragmentary evidence and sparse intelligence flows, which cannot be contextualized.

Moreover, today mere possession of most technologies no longer implies or demonstrates capacity to carry out a threat. Concepts of adversary intent and capacity are more critical to accurately assessing S&T threats. A computer or a batch fermenter is not indicative of a cyber warfare threat or weaponized microbes. Does the adversary really intend to use the technology in a pharmaceutical application? Does the adversary really have the capacity to acquire and execute a threat from a particular S&T application?

In a brief examination of specific cases, a participant summarized the warnings typically associated with the danger posed by terrorists or other non-state groups acquiring and using MANPADS and biotechnology, as well as the historical record of actual use and impacts. MANPADS and biotechnology are very different types of threats that have both been associated with the potential for causing significant loss of life and economic damage for at least the past 30 years. More recent government warnings make clear that a successful MANPADS "…attack against a commercial airliner could claim hundreds of lives, ground civil aviation for days, and dramatically impact the world economy."[1] Moreover, an effective attack with "…a lethal biological agent…could place at risk the lives of hundreds of thousands of people, [overwhelming] our public health capabilities, potentially causing an untold number of deaths. The economic cost could exceed one trillion dollars for each incident."[2]

MANPADS are a very mature and proven weapon system, under state control in most countries but with many available in the black market or regions of crisis, particularly in recent years. Terrorists or non-state groups have successfully used MANPADS against civilian aviation with varying degrees of effectiveness. According to the US Department of State, since 1975 there have been 40 civilian aircraft hit by MANPADS, causing about 28 crashes with more than 800 deaths around the world.

Biotechnology is a rapidly evolving scientific field with various technical applications and developed technologies, under very little state control globally, with terrorists or non-state groups reportedly interested in bioweapons but using them extremely rarely. According to published reports, there have only been two known successful non-state uses of biological agents since the end of World War II to purposely inflict harm on civilians, resulting in relatively modest impacts.

- In 2001 a reported lone perpetrator conducted an anthrax attack against government and civilian individuals, as well as employees and customers of the U.S. postal service, resulting in five deaths and 17 injuries.

---

[1] See "MANPADS: Combating the Threat to Global Aviation from Man-Portable Air Defense Systems," Bureau of Political-Military Affairs, July 27, 2011. http://www.state.gov/t/pm/rls/fs/169139.htm, accessed August 31, 2016.
[2] National Security Council, "National Strategy for Countering Biological Threats," November 2009, p. 1.

- In 1984, a cult used salmonella to poison food at restaurants in Oregon, resulting in no deaths, but 751 injuries.

What can be learned from cases of threats from these technologies in which actual level of impact is inconsistent with information provided by warnings? Are there lessons that can be generalized to improve future assessments of potential S&T threats?

Panel 1: Considering the Science and Technology

The first panel focused on specific scientific or technological aspects of MANPADS and biotech that might explain why attacks at the scale or impact forecasted have failed to occur. Each presenter outlined the unique attributes of either MANPADS or biotechnology that may make these technologies more or less likely to be utilized by non-state actors.

Key points:

- MANPADS have been specifically engineered to prioritize ease of use, but a successful attack relies on several variables, including the size of an aircraft, its level of fuel, the timing of the attack, and the location of the engines.
- Biotechnology is susceptible to hype and paranoia, but specialized skills and difficulty associated with the process of weaponization make it unlikely to be chosen as a method of attack.
- Successful threat assessments related to both technologies rely on an understanding of the unique preferences, capabilities, and objectives of different groups that may perpetrate an attack. The presence or perceived capability of a specific technology is not a sufficient indicator of threat.

In the first presentation, an expert discussed the responsible use of biotechnology, as well as the types of activities that typically occur within the do-it-yourself (DIY) community in the U.S. He pointed out that success in relation to biotechnology requires multiple instances of trial and error on a scale which is not feasible on a personal, lone-wolf level. Due to the nature of the technology, isolating a pathogen from the environment is fairly straightforward and taught in DIY laboratories. This capability is separated from the weaponization of biological agents, which is extremely hazardous, difficult and requires a high level of expertise. Discussion of the hazards of biotechnology is susceptible to hype and paranoia, especially due to a lack of public education related to its core capabilities and uses. However, biotechnology is not competitive as a method of attack while easier, more accessible attack mechanisms exist.

In the second presentation, an expert contends that MANPADS were temporarily pushed from credible threats to commercial aviation due to the survivability and integrity of modern large commercial aircraft. The success of a MANPADS attack again civilian aviation relies on many variables, including the size of the aircraft, the location of the engines, the amount of fuel available, the precision and function of the specific weapon, and the preparedness and skill of the pilot. Because MANPADS were primarily built to target smaller military aviation assets such as smaller combat jets and helicopters, their explosive charge is much less effective against large jets typical of civilian airlines. While MANPADS can cause—and have caused—severe damage and even destruction, in many cases skilled pilots of attacked aircraft were able to safely land the damaged plane. However, the danger associated with MANPADS against

airliners has become more relevant in recent years, not because of specific technology, but due to a general lack of relevant pilot training. In most cases, the effectiveness of a MANPADS attack against a large commercial aircraft is contingent upon the ability of the pilot to maneuver it to safety during an unpredictable emergency situation. Current training of airline pilots is insufficient, relying on computers to replicate and replace essential know-how. Therefore, overall ability to respond effectively to MANPADS attacks has been diminished due to deficits related to pilot training, according to the panelist.

The final panelists explained that there are many factors that must each be satisfied in order to successfully carry out an attack against commercial aviation using standoff weapons such as MANPADS. These factors include adversary group preferences and beliefs, ability to recruit operatives and deliver weapons to an appropriate attack site, and ability to ensure the functionality of the weapon. Emphasis was placed on assessment of each actor individually, to comprehend the decision-making processes that lead groups to choose MANPADS to attack an aircraft as opposed to suicide bombs or cargo bombs inside the aircraft. These decisions do not take place in a vacuum, and individual factors as well as news coverage and political environment may all weigh on the preferences and motives of an individual group.

Following these presentations, discussion focused first on the use of MANPADS and vulnerable points for MANPADS attack. A direct analogy between MANPADS and biotechnology was drawn, referring to the events that must take place to perpetrate a successful attack, mentioned in the earlier presentation. Training requirements were discussed, particularly the difference in required skill between the two technologies and access to those skills. Although skills related to the weaponization of biotechnology are challenging and hazardous to learn, approximately 80% of the information needed to accurately fire MANPADS is available on Youtube.com. With regard to biotechnology, there is a need to provide more comprehensive public education regarding the benefits and threats. The possibility or ease of weaponizing animal diseases was also raised; this may be easier than weaponizing human diseases in some ways, but is similar in amount of skill required.

Panel 2: Considering the People

Participants on this panel discussed the human factors and motivations behind why the predicted impacts of MANPADS and biotechnology have not materialized. Furthermore, they discussed cases and alternative analytic approaches that could be applied to improve assessment of S&T threats through analyzing human factors related to using these threats.

Key points:

- Intent is the product of a deliberative process that includes a number of factors in deciding whether or not to use MANPADS or biological agents.
- The human factor, such as intent, is often underestimated when analyzing the organization of threats; intelligence analysts often see only what they are looking for, and this shapes analytic output.
- Human factors and technology factors are important, but the motivation and intent behind attacks need to be understood. Understanding how overarching drivers such as regional conflict, high unemployment of young men, and other factors lead to threatening acts is critical to prevention or mitigation of those acts. Without that

understanding, there will only be more threats due to the same motivations, even if specific terror groups are removed from power.

- Identifying actors involved in biological threats and their intents and motivations is crucial. In examining biological efforts, whether by state or non-state actors, intelligence analysis needs to focus on the motivations and intentions of the leadership. Without leadership dedicated to the development and use of biological agents, a program cannot exist. Capability will spring from a leadership dedicated to development and use of biological weapons agents.

This session focused on issues related to the human factor and the importance of understanding the motivations behind actors. The presentations in this session had various perspectives, from analyzing intent and capabilities to understanding the wide capacity of the human motivations for attacks, and included a wrap-up to aid understanding of the skills necessary for biological and MANPAD threats to occur. Some of the discussion addressed the need to build a government and public policy response to the human motivations for terrorist attacks, which include regional conflict and lack of jobs and opportunity, particularly for young men. Emphasis needs to be on improving the conditions potential threat actors live in; the technology is really secondary.

In discussing the specific cases of potential biological attacks, the panel analyzed the factors surrounding the idea of fragile microorganisms, and the three types of people involved in biological weapons attacks—1) novices who have the interest but do not know how to do what needs to be done; 2) sub-experts, or people who have advanced theoretical knowledge and some experience in biology and 3) experts. Thus, knowing who is involved and how quickly they can acquire expertise is important for threat assessment. One presenter argued that a group may possess the motivations necessary, but it is not enough to have scientific skills; you must also know the speed at which individuals can learn. Organization and management are both important.

Subsequent discussion revolved around the importance of analytic workforce management and how to create a more meaningful link between policymakers and scientists. Regarding analytic practices, there was some discussion about how to provide the analytic workforce with better training. What is the proper role of social scientist in S&T threat analysis? What is an optimal (if there is one) organizational construct for the conduct of threat analysis?

Panel 3: Considering Threat Assessment

This panel discussed the challenges in producing a targeted, methodologically rigorous threat assessment, especially those dealing with emerging technology, a lack of primary sources, and insufficient context.

Key points:

- Hype is vital to the process of scientific discovery, but may also create key disconnects concerning the potential capabilities and applications of a technology.

- Framing and biases create direct misunderstandings in terms of the capabilities and prospective threats related to specific technologies.

- More rigorous methodology and an awareness of biases are essential to producing targeted, useful analyses.
- Due to the nature of threat assessments, uncertainty and incomplete information will continue to prove challenging to analysts.

In the first presentation, an expert discussed the shared hype and biases that drive scientific research and discovery. McKenzie's Certainty Trough (Donald McKenzie, 1990) was used to emphasize how a person's affiliation with a particular technology may change their conception of its reliability. Also important here is the relationship between hype and reality. Hype is instrumental in creating a shared vision and expectation of the outcome of a project, but may also create unrealistic expectations concerning the ease of development or dissemination. The presenter discussed a range of biases that affect the way in which decisions are made, such as availability of information, confirmation bias, overconfidence in intuition, and base rate neglect. The subjective nature of decision-making calls for methodological skepticism, in which analysts might draw from a large range of views, be more aware of their own biases, and make their analysis more available to scrutiny.

In the second presentation, an expert considered the discourse surrounding biological threats and identified the key disconnects that negatively affect threat assessments. This panelist pointed out that the term "synthetic biology" frames biology as an engineering discipline rather than a life science. This contributes to a lack of understanding of the science, as well as a lack of nuance concerning where and from whom a potential threat may occur. In reference to DIY biology, the skill level of current experimentation and the supposed breakdown of boundaries between expert and non-expert are grossly overstated, according to the panelist. Moreover, dominant discourse identifies terrorists as the primary source of a possible biological threat. However, attempts by terrorist groups to obtain pathogens have lessened in recent years, even as overall terrorist attacks have increased in frequency. These examples of the disconnected nature of fact and discourse in the case of biological threats directly contribute to a key lack of understanding and nuance in the creation of threat assessments.

In the final presentation of the panel, an expert discussed common methodological problems associated with threat assessments. He referenced the use of small sample sizes, and the danger of using inductive reasoning in place of deductive reasoning to drive research and assessment. Further challenges exist in consulting past trends to inform future events, as trends are not always a reliable predictor. In order to counter these factors, providing adequate context and primary sources is vital to any judgment. An analysis by multiple methods may also provide the most complete picture of a prospective threat, even though time and adequate funding may be difficult to obtain. In closing, the speaker emphasized producing an assessment that is methodologically rigorous, targeted, and helpful.

Discussion following these presentations first addressed the possible danger of publishing research related to biotechnology and how DIY biology communities resist government control in favor of self-regulation. These qualities may be uncomfortable, but self-regulation with FBI observation has proved to be a relatively successful compromise in the U.S. Customer expectations and how a non-technical consumer might guard against scientific bias in presented data were also highlighted. An anonymous review process could be implemented in order to reduce the negative effects of hype and scientific bias.

Panel 4: Improving Threat Assessment

This panel examined ways of improving on the assessment of threats to national security from S&T. The panel also discussed emerging future threats and how they could be addressed using new analytical approaches.

Key points:

- The rise of digital technology has led to new threats that need to be addressed by the intelligence community. Cyber is accessible and easy to develop expertise in.
- Tasks required to achieve terrorist objectives can be broken down using the Benjamin Bloom scale of cognitive dimensions.
- There needs to be a new multidisciplinary approach to technological innovation and threat assessment. There is a lack of expertise and rigor in attempts to understand the impact of technology on society.

One panelist discussed the rise of digital technology as an emerging threat and said that due to its easy accessibility, it will have profound strategic consequences. Considerable effort will be required to accurately assess the threat adversarial actors can have through digital means.

Panelists then discussed the need for a multidisciplinary approach to understand the sociological factors motivating attacks. The panel argued for a horizon-scanning assessment of technological innovations and their societal impacts and national security concerns. The panelists had varying opinions on how this new threat assessment should be established. The first speaker had a narrow view of cybersecurity as a threat that is not well understood. The second speaker discussed a method of assessing whether groups have the capabilities to succeed with an approach using education psychologist Benjamin Bloom's cognitive pyramid as an analytic tool.[3] Based on this taxonomy, types of "knowledge" (factual, conceptual, and procedural) and levels of cognitive sophistication can be used to break down and analyze the tasks associated with terrorist objectives. The resulting matrices can then be mapped to assess terrorist capabilities. The third speaker also stressed the importance of a multidisciplinary approach to understanding how technology impacts society. The panel further discussed an emphasis on cultural and social values and how they affect the dissemination of ideas and their role in risk assessment. Cultural and social values can determine whether certain technology will be adopted and others not. The discussion revolved around the weakness of countermeasures—if you control knowledge, how do you make sure the people who need knowledge get it? The panel concluded that protection is dependent on the threat, and most terrorist groups have not had large technology adaptions and persist in settings with low accessibility.

Final Observations

In the final presentation of the workshop, a participant provided an overview and summary of the main ideas discussed during the workshop. When examining bioweapons and MANPADS,

[3] Bloom's Taxonomy is a classification system developed in 1956 to categorize intellectual skills and behavior important to learning.

speakers posited that the complexity of these technologies and the requirements for their use are much more difficult than has been typically expressed. Threat assessments should begin with an understanding of the intent, dynamics, and capabilities of threatening groups rather than the capabilities of technologies. The process of analyzing threats within the intelligence community should also be scrutinized. Several solutions to improve this process were offered, including a more rigorous, interdisciplinary approach to analysis. These suggestions focused on what should be done within the community. However, they neglected to grapple with the more immediate—and challenging—issue of what can be done, taking into account the existing barriers related to infrastructural problems and constraints on available resources.

The speaker posited that these remarks reflect a common assumption of scientists and analysts: if facts are explained clearly and completely enough, the necessary responses will be obvious and actionable. This is not the case in practice, and more discussion should be devoted to how those responsible for managing analytic resources can affect real changes to analytic processes and workflows. Moreover, more discussion on how policymakers respond to the threat assessments they are presented with is needed.

The speaker also examined the meaning of terms often mentioned during the workshop. What constitutes security? What qualifies as a threat? Casualties associated with biological attacks and MANPADS are extremely low when compared to, for example, the amount of deaths on American highways in a single month. In addition to an unclear definition of the characteristics of threat, the presentations focused almost completely on terrorist groups rather than states. Analysts and policymakers often speak as if the United States is very fragile, but acts of terrorism constitute a political threat rather than an existential one. How would the terrorist threat look if considered within the context of state survival?

Concluding, the speaker noted that the measures of success and incentives for intelligence analysis deserve increased attention. The two measures of success seem to be either that the warned event does not occur or that the program gets attention and funding. If the event does not occur, how will analysts avoid the “Boy Who Cries Wolf” effect? Additionally, if the program is funded, there is incentive to go immediately to the “darkest corner of the room.” There is no cost to false positives, so an incentive exists to give a “low signal warning.” This phenomenon could also be thought of as an analyst “predicting fourteen of the last three coups.” Understanding the complexity of technologies related to threat assessments is important. However, this understanding may not produce much improvement if the weakness of infrastructure and day-to-day incentivizing within the analytic community are not also taken into account. Even if threat assessment is perfected, policy response to these assessments is a critical and often ignored aspect of the warning process.

Workshop Participants

Dr. Gary Ackerman
University of Maryland

Ms. Susan Allen
Lawrence Livermore National Laboratory

Ms. Paris Althouse
Lawrence Livermore National Laboratory

Mr. Eric Arnett
Central Intelligence Agency

Cadet Katie Brechbuhl
United States Air Force Academy
Lawrence Livermore National Laboratory Student Intern

Mr. Shawn Cantlin
Lawrence Livermore National Laboratory

Dr. Glenn Cross
Federal Bureau of Investigation

Mr. Brian Cullen
United States Department of State

Dr. Zack Davis
Lawrence Livermore National Laboratory

Dr. Patrik D'haeseleer
Lawrence Livermore National Laboratory

Dr. Mona Dreicer
Lawrence Livermore National Laboratory

Dr. Carolyn Floyd
Weapons and Counterproliferation Center

Dr. Holly Franz
Lawrence Livermore National Laboratory

Dr. Bruce Goodwin
Lawrence Livermore National Laboratory

Mr. Mark Hanna
Central Intelligence Agency

Dr. Michael Hopkins
University of Sussex

Dr. Steve Johnson
Cranfield University

Mr. Nicholas Jones
Loyola Marymount University, USAF ROTC
Lawrence Livermore National Laboratory Student Intern

Dr. Filippa Lentzos
King's College London

Dr. Melissa Marggraff
Lawrence Livermore National Laboratory

Mr. Kevin McCarthy
Moonraker Associates

Dr. Rand McEachern
Lawrence Livermore National Laboratory

Dr. Caitriona McLeish
University of Sussex

Dr. Michael Nacht
University of California, Berkeley

Dr. Emile Nakhleh
University of New Mexico

Dr. Tony Olcott
Michigan State University

Dr. Sonia Ben Ouagrham-Gormley
George Mason University

Dr. Don Prosnitz
Consultant, Lawrence Livermore National Laboratory

Mr. Brian Rose
The George Washington University
Lawrence Livermore National Laboratory Student Intern

Ms. Mallory Roseman
North Carolina State UniversityLawrence Livermore National Laboratory Student Intern

Ms. Beverly Neale Rush
Central Intelligence Agency

Dr. Brian Shaw
Defense Intelligence Agency

Mr. C. Wes Spain
Lawrence Livermore National Laboratory

Cadet Robert Stelmack
United States Air Force Academy
Lawrence Livermore National Laboratory Student Intern

Ms. Anita Street
National Intelligence Council

Cadet Conner Thomsen
United States Air Force Academy
Lawrence Livermore National Laboratory Student Intern

Dr. Kathleen Vogel
North Carolina State University

Mr. Jack Weller
Stanford University
Lawrence Livermore National Laboratory Student Intern

Mr. Christian Westermann
United States Department of State

2LT Noah Young
United States Army
Lawrence Livermore National Laboratory Intern

Ms. Fareeda Zikry
University of North Carolina, Chapel Hill
Lawrence Livermore National Laboratory Student Intern

Acronyms

Acronym	Definition
CGSR	Center for Global Security Research
DIY	Do it yourself
IC	Intelligence Community
MANPADS	Man-portable air defense systems
S&T	Science and technology