SANDIA REPORT
SAND2020-8392
Printed August 2020

Potential Academic Research Topics of National Security Relevance

Jarret Lafleur, Ph.D.
Patricia Hernandez, Ph.D.
Bradley Steinfeldt, Ph.D.
Eva Uribe, Ph.D.
Lonnie Carlson, Ph.D.
Paul Nielan, Ph.D.
Nerayo Teclemariam, Ph.D.

Systems Research and Analysis, Homeland Security and Defense Systems Center
Sandia National Laboratories, Livermore, California

Prepared for Collaboration with the SciPol Scholars Program

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

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

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

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

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

ABSTRACT

Since even before its establishment as an independent national security laboratory in 1949, Sandia has been devoted to an overarching mission of developing advanced technologies for global peace. These technologies have taken a variety of forms, and they exist in and must address an ever-changing global security environment. An understanding of that global security environment and its possible or likely evolution is therefore critical to ensuring that Sandia can maintain its focus on strategic technology investments that will benefit the nation in the next 20-30 years.

Sandia sustains multiple Systems Analysis organizations whose responsibility includes maintaining an understanding of the global security environment as it applies across multiple mission domains. The topics below include two from Sandia's emerging threats and biodefense mission, three with relevance to Sandia's cyber defense mission, and four of particular but not exclusive relevance to Sandia's nuclear deterrence mission. All are intended to spur independent academic thought that could assist Sandia as well as the broader national security community in anticipating and adapting to a continually changing world. Sandia anticipates periodic interactions between Sandia Systems Analysis staff and SciPol Scholars Program faculty and students who choose to expand upon these topics in order to provide opportunities for feedback and communication throughout 2020-2021.

1. RISKY BUSINESS: RISK ANALYSIS OF EMERGING BIOTECHNOLOGY

As biotechnology advances, so do the potential threats to US economic and security interests. Biological threats have the potential to cause world-wide catastrophic events, and while risk assessment processes exist for determining the threats and vulnerabilities associated with biological agents, there is not a clear methodology for understanding the risks associated with biotechnology. There is a continuing need for exploration of correlations between areas that drive biotechnology development and the potential impacts on national security. Associated research questions include:

- What methodologies might be effective for evaluating and prioritizing risks associated with emerging biotechnology? How must such methodologies differ from risk assessments of biological agents alone?
- What key factors and metrics may be indicators of technologies that could impact national security?
- How could stakeholders within this space be effectively engaged, domestically and internationally, to mitigate these effects?

2. THE EVOLVING LANDSCAPE OF GENOME SECURITY

Genome security is an evolving space that the involves the prevention, detection, and response to accidental or malicious use of genome analysis or genome editing that may lead to WMD-like effects. There are several key technical advances, including DNA sequencing, DNA synthesis, genome editing, and increased automation, that have increased the production rate and accessibility of biotechnology products. The revolution in biotechnology holds immense promise for addressing human disease, creating biotechnology solutions for bioenergy, understanding basic biology and advancing the drug-discovery field. The cost of DNA sequencing and de novo DNA synthesis has decreased exponentially, and advances in genome engineering has enabled precisely targeted genome modifications in a variety of organisms. Unfortunately, explosively growing use of gene editing tools also raises profound dual use concerns. Detection and surveillance of potential concerns within genomic systems and/or genetic tools, both accidental and malicious, will require a novel and multidisciplinary approach. Below are several research questions that begin to address concerns within this space:

- What fundamental properties of genomic systems make them uniquely vulnerable to novel or unexpected concerns? What novel or unrecognized concerns are created by advances in genomic systems technologies?
- What are the indicators that a technology (or actor/institution), or convergence of technologies, can produce a concern, and how can the severity of the concern be accurately assessed?
- What are the implications of policies and programs on regulation of research?: How much would that help overall risk? What would the negative effects be on research and innovation? Is it even feasible to consider such restrictions, or is it too late?

- What are the implications of not detecting a genome security-based event?

3. MODELING THE EFFECTS OF POLICY AMBIGUITY ON DETERRENCE AND ASSURANCE

One enabler toward the reliable operation of nuclear deterrence and assurance is an accurate description of the rules and principles by which a nation will act in the event of provocation, as described by declared policy. However, while policy declarations should be accurate, rarely are they precise. This lack of precision, or prevalence of ambiguity, is typically intentional. A policy that is too precise and prescriptive might not allow a decision-maker sufficient leeway in adapting to new circumstances, and it could help an adversary devise strategies to exploit specific policy gaps.

Reasoning in the Thomas Schelling school of thought on deterrence, ambiguity can enhance deterrence by introducing more uncertainty in the mind of the adversary. On the other hand, the Herman Kahn school of thought might suggest that too much ambiguity indicates to an adversary a weak and indecisive leadership and even prompt an attack. When it comes to assurance, a different trend might be hypothesized: In order to be assured, an ally or partner might care to drive policy ambiguity as low as possible, indicating clear nuclear umbrella defense plans and commitments, provided that the policy allows discretion for adapting to unforeseen circumstances.

Based on simple considerations like these, one might hypothesize that the strength of deterrence and assurance vary with policy ambiguity as in Figure 1. A model even as notional as Figure 1 can provide helpful insights. For instance, if accurate, it highlights that highly ambiguous policies have weakening effects on both assurance and deterrence, and that policy trades should only be made in the space to the left (or less ambiguous side) of the degree ambiguity that provides peak deterrence.

However, this model is indeed notional. Before it can be used to guide decisions about future declaratory or other policies, research and study are needed to clarify, substantiate, and investigate this line of thought. For instance:

- What past research has been executed and what literature has been written on the relationships between deterrence, assurance, and ambiguity?
- Does existing literature, including historical examples or human studies, corroborate or refute the trends hypothesized in Figure 1, and for what reasons?
- How might ambiguity be quantified or qualified (e.g., into descriptive tiers of increasing declaratory policy ambiguity)? How might the strength of deterrence or assurance be quantified or qualified?

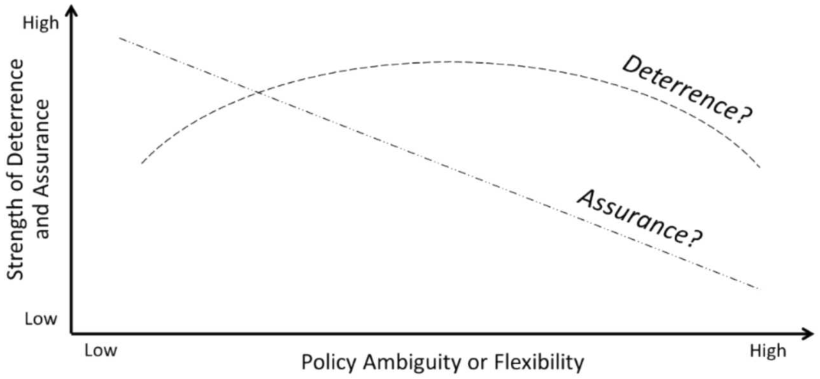

Figure 1. Hypothesized Variation of Deterrence and Assurance Strength with Policy Ambiguity.

4. ANTICIPATING CHALLENGES TO GLOBAL NUCLEAR NORMS

The 2018 Nuclear Posture Review recognized the dramatic and rapid deterioration of the global strategic threat environment since 2010. In addition to rogue state nuclear threats, the review noted that Russia and China have added new types of nuclear capabilities to their arsenals, increased the salience of nuclear forces in their strategies and plans, and engaged in increasingly aggressive behavior across multiple strategic domains. Among the most concerning developments was Russia's "escalate to de-escalate" doctrine that suggested its belief that coercive nuclear threats or limited first use could paralyze the United States and NATO and thereby end a conflict on terms favorable to Russia.

Soon after the NPR's release, President Putin highlighted concerning nuclear capabilities under development during his March 1, 2018, state of the nation address, including a nuclear-armed underwater drone, nuclear-powered cruise missile, and hypersonic systems. Russia's violation of the Intermediate-Range Nuclear Forces (INF) Treaty beginning in 2014 and its failure to return to compliance has now also prompted U.S. withdrawal and termination of the nearly 32-year-old treaty.

These developments have spurred national thinking about the ongoing role of nuclear deterrence in U.S. security strategy, with its public recognition as the highest priority mission of the Department of Defense. These developments have also drawn attention to the potential fragility of long-held nuclear norms, prompting questions such as:

- How fragile are long-held nuclear norms, and what implications does this have on the establishment or preservation of stable nuclear norms in the future?
- What blind spots exist in nuclear deterrence planning, and what global nuclear norms might credibly be at risk in the coming decades?

5. BRIDGING THE TECHNOLOGY READINESS "VALLEY OF DEATH"

The U.S. Department of Energy National Laboratories conduct a mix of both basic research and the development of systems for deployment by the nation's armed services. Consequently, the laboratories are in a position to shepherd new technologies from concept to the field. Nonetheless, the laboratories are not immune from the Technology Readiness "Valley of Death" (Fig. 1) that looms over many organizations and industries. This "valley" describes the tendency for organizations to well-resource both system development (e.g., according to the DoD 5000, NNSA 6.X, or NASA Project Life Cycle processes) and basic research but under-resource development in the transition region, typically around Technology Readiness Levels (TRLs) 4-6. This TRL 4-6 region involves technology validation beyond the laboratory but short of integration into a flight system, and consequently is one in which a technology is too advanced for further basic research but too risky for a flight program to adopt.

The laboratories would appreciate academic insight into questions such as:

- What strategies or policies have other industries or government sectors adopted to solve this problem?
- Which strategies and policies have been successful in maximizing technology transfer to flight programs?
- Are there new strategies that may be worthy of consideration and testing?

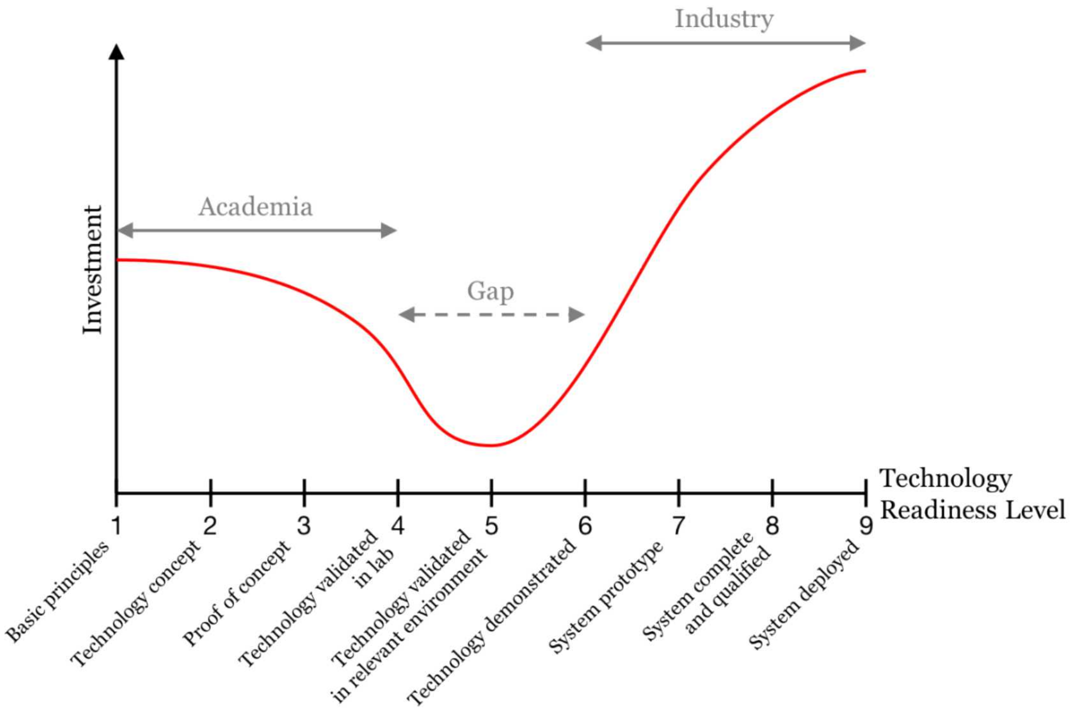

Figure 1. Example Illustration of the Technology Readiness "Valley of Death". *Image Credit: https://blogg.pwc.no/digital-transformasjon/bridging-the-technological-valley-of-death*

6. MODELING THE EFFECTS OF SYSTEM RELIABILITY VARIATIONS ON WARGAME DETERRENCE

In the 1960s, Thomas Schelling challenged the evolving school of thought on deterrence, which had posited that deterring the Soviet Union required the threat of a certain and overwhelming retaliatory response to strategic attack. Rather, Schelling pointed out that even the reasonable *possibility* of an overwhelming retaliatory response could be enough to deter. This idea of resting the nation's security on this assumption has caused at least one author (Payne 2008) to call it *The Great American Gamble* on which America rested large portions of its national security during the Cold War.

This idea that deterrence may rest on the possibility, rather than the virtual certainty, of a retaliatory response raises interesting questions that span both policy and engineering realms, among them: What is the deterrent-optimal reliability for a weapon system? This question is itself multifaceted, with at least one facet related to the marginal opportunity cost of designing incremental reliability increases into defense systems. Perhaps an even more interesting facet can be investigated in a wargame or simulation setting, namely how participant decision calculus and tendency to engage in or avoid conflict changes with the reliability of the deterrent systems in the game. Does an empirical relationship exist, and what is its strength? On what factors (e.g., conventional vs. nuclear, small- vs. large-scale conflict) does the strength of this relationship depend?

7. THRESHOLDS IN CYBER CONFLICT

The Law of Armed Conflict is often invoked when discussing cyber conflict. Several years ago, the UN Group of Governmental Experts (GGE) agreed that the Law of Armed Conflict still applies in cyberspace, but the group has subsequently failed to achieve consensus on how it applies, i.e. what type of cyber attack would constitute a "use of force" that would justify an armed response. In 2018, the U.S. National Security Council articulated two end states for cyber deterrence, including "a continued absence of cyber attacks that constitute a use of force" and "reduction in destructive, disruptive, or destabilizing cyber activities against U.S. interests below the threshold of the use of force" ("Recommendations to the President on Deterring Cyber Adversaries," 2018). At the same time, USCYBERCOM recognizes that "adversaries operate continuously below the threshold of armed conflict to weaken our institutions and gain strategic advantages" (USCYBERCOM Command Vision, 2018). In other words, some adversaries use cyber means specifically to gain strategic benefits without triggering the "use of force" threshold. Compelling questions deserving of exploration include:

- Is the "use of force" threshold appropriate for cyber conflict? Are there more nuanced thresholds concepts that might more accurately capture how our adversaries conceive of thresholds in cyber conflict?
- How have conflict thresholds and norms been developed historically, and can we extend those experiences to cyber conflict?

8. THE ROLE OF UNCERTAINTY IN DETERRING CYBER ADVERSARIES

Scholars of deterrence theory have long recognized the importance of uncertainty for deterring an opponent. Schelling described deterrence by a "threat that leaves something to chance," (Thomas Schelling, *Arms and Influence and The Strategy of Conflict*, 1966) in which actors intentionally exploit risk and uncertainty to influence the decisions of their opponents. Many scholars have pointed out the inherent differences between cyber conflict and nuclear conflict that make deterrence of cyber adversaries more difficult, if not impossible. Cyber attacks abound in uncertainty – the extent and impact of effects may be uncertain, the accuracy and timing of attribution is uncertain, the ability to detect attacks is uncertain, and norms of acceptable behavior in cyberspace are debated and uncertain. How do these and other sources of uncertainty influence our ability to deter actors from attacking us using cyber means? Are there ways we can leverage the uncertainty in cyber conflict to our advantage in order to deter cyber actors?

9. CAN WE DETER CYBER ATTACKS THROUGH DEFENSE AND RESILIENCE?

When we think of deterrence, we typically think of deterrence by punishment, in which a threat of retribution creates the prospect of unacceptable costs that causes an adversary not to take some proscribed action. An alternative mechanism is deterrence by denial, in which one party can “deny the other party any gains” from their actions (Glenn Snyder, *Deterrence and Power*, 1960). This could be achieved either by bolstering defensive capabilities or by demonstrating the ability to mitigate or recover from the primary effects of an attack. Our ability to defend against or recover from massive nuclear war is limited. However, deterrence by denial may play a larger role for other types of conflict, including cyber. Gerson has discussed the importance of deterrence by denial for conventional conflict, noting that the point of defense is not to completely remove opponents’ ability to attack, but rather to convince them that “the only alternative is protracted war” (Michael S. Gerson, “Conventional Deterrence in the Second Nuclear Age,” Parameters, 2009). Others have discussed the greater relevance of deterrence by denial for even the most motivated actors, who “may be willing to give their lives, but not in futile attacks” (Robert W. Anthony, “Deterrence and the 9-11 Terrorists,” 2003). Questions of interest to the cyber defense community include:

- Are there historical examples of deterrence by denial succeeding in dissuading warring parties?
- What does deterrence by denial look like for cyber conflict?
- How can we measure effectiveness of these deterrence mechanisms relative to deterrence by punishment?

This page left blank

DISTRIBUTION

Unclassified Unlimited Release

This page left blank