SANDIA REPORT

SAND2018-0205 R
Unlimited Release
Printed January 2018

Sandia National Laboratories Strategic Context Workshop Series 2017:

National Security Futures for Strategic Thinking

Elizabeth Kistin Keller, Elizabeth Roll, Munaf Aamir, Diana Bull, Sharon Deland, Chad Haddal, Howard Passell, John Foley, Amber Harwell, Monique Otis, George Backus, Wendell Jones, Michael Bawden, Richard Craft, David Kistin, Jeffery B. Martin, Bradley McNicol, Michael Vannoni, Lawrence Trost, Jeffrey Tsao, and Karla Weaver

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

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

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

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

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

Available to the public from
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/

1. Background

In August 2017, Sandia convened five workshops to explore the future of advanced technologies and global peace and security through the lenses of deterrence, information, innovation, nonproliferation, and population and Earth systems.

Each workshop brought together subject matter experts and leaders from diverse fields to explore potential futures and deepen Sandia's understanding of the evolving global security environment. Workshop participants engaged in structured activities designed to evoke discussion and creative thinking on three key questions:

- What might the global security environment look like in 20 years?
- What are the United States' (US) national security challenges associated with these potential future environments?
- What should the national security enterprise be thinking about now to prepare for these potential future environments?

This summary provides an overview of high-level insights and implications from the strategic context workshops. Appendices A through E contain snapshots of the discussions at each workshop.

2. Future Dynamics

Over the course of the workshop series, participants imagined a range of potential global security futures. While the specific scenarios were diverse and divergent, the imagined futures reflected an increasingly complex and rapidly changing global security environment driven by the confluence of several key dynamics:

- **Technological convergence and individual empowerment:** The evolution and convergence of numerous technologies from previously stove-piped disciplines and sectors will generate a vastly more complex national security threat space. Simultaneously, the connectivity, affordability, accessibility, and magnitude of technology innovations will enable individuals, groups, and institutions to develop and deploy technologies with the potential to produce beneficial breakthroughs and catastrophic consequences globally.

- **Polycentric world with new actors challenging institutions:** Over the next 20 years, the Unites States' superpower status will continue to be challenged. Traditional great power politics between the United States, Russia, and China will collide within a much more complex web of emerging state powers, corporations, non-government organizations (NGOs), and individuals. These entities will challenge and transform the norms and agreements that shape global peace and security.

- **Climate change vulnerabilities and constrained resources**: Changes to Earth systems will make the planet less resilient and expose humans to new health, food, water, energy, and infrastructure vulnerabilities that will exacerbate security challenges arising in other domains. Exponential population growth will drive increased demand for renewable and nonrenewable resources worldwide as availability declines. Interregional disparities will continue to induce migration and cross-boundary responses.

- **Accelerated information diffusion and decision making**: Innovations will continue to transform the information landscape—increasing accessibility, disrupting trust and confidence, and complicating decision making. Concurrently, world events and technology innovation will outpace the capacity of humans and governance institutions to deliberate and respond, contributing to an increase in new machine-assisted decision environments at various scales.

3. Preparing for the Future

Overall, participant discussions about how to prepare for the confluence of these dynamics focused on the importance of increased resilience across the national security enterprise and the need to better anticipate and rapidly adapt to emerging security challenges and opportunities through collaborative innovation and improved communication to inform decision makers and stakeholders:

- Utilize advanced technologies to better **anticipate** emerging threats and opportunities. Advancing anticipatory capabilities will require the rapid integration of capabilities developed globally by the public and private sectors to advance anticipatory intelligence. The integration of advanced computational and social science expertise is also key to gaining a deeper understanding of the complex socio-political-technical systems shaping the global security environment.

- Develop new approaches to **withstand**, **adapt** to, and **recover** from an evolving set of security challenges. Empowered corporations, NGOs, and individuals can act as decentralized threats and as sources for solutions.

- Collaborative **innovation**, to integrate expertise across global institutions, industry, academia, and elsewhere. Organizations should seek opportunities for developing a more collaborative, innovative culture by embracing risk, developing rapid cross-institution partnering models, and attracting and inspiring a diverse and interdisciplinary workforce.

- Advanced decision support tools are needed to bridge the technology-policy divide and **inform** an increasingly wide array of decision makers in industry and government. As the security environment rapidly evolves, new approaches are needed to enable high-speed, high-confidence decisions under increased uncertainty.

Appendix A. Future of Nonproliferation

This appendix provides a snapshot of key themes discussed at the Future of Nonproliferation workshop on 8/10/17.

What dynamics and key questions might shape global security and nonproliferation in 20 years?

Decreased barriers to proliferation shift focus from technology control to understanding and influencing intent

The connectivity, affordability, and accessibility of technology innovations will enable any motivated individual, group, or government to develop and deploy weapons of mass destruction (WMDs). The declining barriers to proliferation necessitate a shift in emphasis from controlling materials, technology, and expertise toward developing enhanced capabilities in anticipating and influencing the motivations of potential proliferators.

- *What combinations of WMD and other technologies (e.g., cyber, conventional) might state and non-state actors pursue to project power and achieve their security goals?*
- *If a nuclear weapon is detonated, how might it spark increased proliferation, increased disarmament, or both?*

Emerging global challenges outpace nonproliferation agreements & institutions

Left alone, the current nonproliferation governance regime is likely ill-equipped to handle emerging global challenges. Innovations in biotechnology and cyber are rapidly outpacing regulatory mechanisms as tensions increase between the nuclear haves and have-nots. The next big norms may not come from a traditional treaty process, but rather through decisions made by select corporations, foundations, or individuals.

- *To what extent will state and non-state actors, including corporations, abide by or alter international norms?*
- *To what extent will the United States engage with other state and non-state actors to address proliferation challenges? Will we see a sustained period of retrenchment or renewed engagement tailored to an evolving world?*

Convergence of emerging technologies challenges and enhances situational awareness of WMD proliferation

The evolution of dual-use technologies, cryptocurrencies, and advanced manufacturing stresses traditional approaches to situational awareness and empowers adversaries. Concurrently, advances in data collection and analysis through ubiquitous sensing, artificial intelligence (AI), and quantum computing may enhance our ability to anticipate and influence proliferation motivations and activity.

- *What tradeoffs might different populations make between privacy and monitoring by the public and private sectors?*
- *What pressures might alter the expansion or decline of the nuclear energy enterprise? How might the United States address its loss of influence with respect to global nuclear energy? How might a collapse of the nuclear energy enterprise shape broader issues of strategic latency and nonproliferation?*

How might the national security enterprise prepare for emerging national security challenges and opportunities?

Utilize advanced sensing, analytics, and social and cognitive sciences to better anticipate emerging threats and opportunities

- Integrate global public and private sector advancements in satellites, sensors, AI, and predictive analytics to advance anticipatory intelligence
- Gain a deeper understanding of the socio-political-technical systems shaping the global security context and influencing WMD proliferation and to build trust in automation and machine-assisted anticipation and decision environments

Develop adaptable regimes and capabilities that are resilient to emerging proliferation threats

- Reimagine the toolset needed to influence proliferator intent when the United States is no longer a sole superpower
- Anticipate, absorb, adapt to, counter, and recover from emerging proliferation threats

Collaborate to enable the innovation of new nonproliferation approaches

- Break down stovepipes separating WMD domains to illuminate opportunities for learning and innovation, while maintaining strong domain-specific expertise
- Craft a risk posture that enables partnering across government, FFRDCs, academia, and the private sector.
- Inspire next-generation leaders who can connect the frontiers in science and engineering to emerging WMD nonproliferation mission challenges

Inform the articulation, pursuit, and achievement of clear nonproliferation goals

- Pursue integrated education efforts and tailored decision support tools to bridge the technology-policy divide through
- Advance research in attribution and combating misinformation

Appendix B. Future of Deterrence & Strategic Stability

This appendix provides a snapshot of key themes discussed at the Future of Deterrence workshop on 8/14/17.

What dynamics and key questions might shape deterrence and strategic stability in 20 years?

Polycentric world creates complex security challenges

International relationships are increasingly blurred beyond expanding numbers of states to include powerful international companies and non-governmental organizations, who can impact a state's security and standing. The relative rise of non-state actors makes the national security space more complex and confounding for current strategic deterrence approaches. Moreover, global interdependencies create challenges for credibility and attribution efforts. These dynamics are set against environmental stressors (e.g., water shortages, human migration, and urbanization) that may eclipse the strategic security priorities of leaders.

- *How might nation-states affect strategic stability in a world with growing strategically disruptive non-state capabilities?*
- *How might increasing global socio-economic interdependence fundamentally alter the tenets of strategic deterrence?*

Technology democratization and technology convergence alters strategic security threats and opportunities

Strategic security threats have broadened from primarily nuclear to include rapidly evolving biotechnology and cyber. The convergence of numerous technologies generates a vastly more complex national security threat space. Moreover, declining technological barriers and the explosion in connectivity and autonomous systems make potential strategic threats accessible to a wide variety of actors across the world. The social benefits provided by these dual-use strategic capabilities will further complicate the security challenge.

- *How might technology advancements help and/or hinder strategic decision-making abilities in an increasingly complex world?*
- *How might technology democratization affect incentives and disincentives for strategic level conflicts?*

Divergent narratives and misinformation prevent effective deterrence

A shared narrative and common perceptions have always been necessary to produce a deterrent effect. But social media and other information mechanisms enable the propagation of fully formed, and potentially fact-free, alternative narratives. Absent the emergence of improved information verification tools, once trusted and secure information will conflict with alternative narratives, thereby diminishing the effectiveness of deterrence and driving up the cost of credible signals.

- *How might informational trust continue to deteriorate, and how will new informational confidence emerge?*
- *To what extent can the global security framework tolerate increasingly disparate and competing narratives and interests?*

How might the national security enterprise prepare for emerging national security challenges and opportunities?

Anticipate destabilizing changes and unintended consequences

- Encourage integrated, multidisciplinary foresight capabilities across the national security enterprise
- Enhance decision maker understanding of threats, policies, and tools through advanced computational and social science techniques and realistic futures exercises

Adapt strategic stability approaches for a complex global security environment

- Invest in more agile, adaptable, rapid, and multidisciplinary anticipation and response capabilities
- Re-evaluate strategic stability approaches that are more resilient and robust to an increasingly fluid fragmentation and reconfiguration of global power structures
- Surrender status quo thinking that nuclear weapons are the primary variable in strategic stability
- Embrace strategic stability as a complex and wicked problem that requires continuous management, recovery, and improvement through prudent risk taking and confidence building measures

Communicate unambiguously to minimize risk and increase public confidence

- Develop innovative analytic and communication systems to clarify intent and minimize the risk of misunderstanding
- Articulate clear strategic security policies and couple them with flexible military, trade, and diplomatic tools
- Invest in new and more trustworthy communications mechanisms that can reinforce public confidence in information

Collaborate to develop integrated and trusted capabilities and partnerships

- Advance trusted detection, attribution, and forensic capabilities for multifaceted web of threats, adversaries, and alliances
- Build and maintain strong cooperative relationships and norms across the spectrum of international actors

Appendix C. Future of Information

This appendix provides a snapshot of key themes discussed at the Future of Information Workshop on 8/17/17.

What dynamics and key questions might shape information and global security in 20 years?

Nations, corporations, individuals, and virtual entities will contest information ownership, access, security, and credibility

Information will continue to be the currency of the realm. Questions regarding who owns, has access to, secures, and ensures the credibility of information will continue. Security will be key to ensuring the value of information; however, the value of information will create motivation for continued exploitation.

- *How might access to and ownership of information impact social inequality, polarization, and international stability?*
- *How might information ownership, access, credibility, and security affect the foundations of democracy (e.g., free speech, privacy)?*
- *To what extent might actors regress to less interconnected or non-digital means in pursuit of security?*

The necessity for rapid decisions under complex, evolving, and uncertain environments will surpass human cognitive abilities

Information-based conflict occurs in microseconds, necessitating a paradigm shift in responses. At the same time the volume of information and disinformation available will increase, complicating decision making and favoring human-machine collaboration. Questions regarding the fairness and trustworthiness of artificial intelligence environments will need to be addressed.

- *To what extent might the intelligence and decision-making processes be consolidated and automated?*
- *To what extent and in what domains might humans relinquish decision-making authority to autonomous systems? What will it take to establish and maintain trust in the autonomous systems?*

Emerging and information domains will be used to challenge US dominance

Nations, corporations, individuals, and virtual entities will continue to challenge US supremacy. Warfare will be pursued in multiple, unrestricted, and nontraditional domains (e.g., cyber/physical domain, human domain), all of which rely on information and information systems. Disinformation will continue to shape the information domain.

- *How might state and non-state actors, including virtual networks and autonomous agents drive the evolution of security norms?*
- *How might emerging and information domains eclipse or transform deterrence, nonproliferation, and innovation strategies?*
- *How might entities trade-off kinetic and non-kinetic means to coerce or harm the United States and allies?*

How might the national security enterprise prepare for emerging national security challenges and opportunities?

Partner to access and share scarce information and emerging domain talent, technologies, and protect key systems

- Encourage sharing of information security and credibility techniques and expertise between corporations, infrastructure owners, government agencies, and allies
- Encourage research and development (R&D) partnerships in the information and emerging domains including human decision making, biological technologies, artificial intelligence (AI), and human interface
- Re-evaluate policies that block collaboration, encourage secrecy, and disallow commercial-off-the-shelf solutions

Redesign the national security apparatus to reflect the expanding threats/vulnerabilities and the need to make rapid decisions

- Co-evolve trusted machine-assisted decision environments that navigate the tension between information assurance, through attribution and credibility, and decision-making speed
- Re-evaluate Titles 10 and 50 relative to adversary norms, processes, and future threat environment
- Explore alternatives to Internet dependence for infrastructure and key system controls

Develop adaptive methods to national security problems that are resilient to diverse threats and future trajectories

- Invest in resilient cyber systems engineering to anticipate, withstand, adapt to, and recover from massive attacks to key national information systems (e.g., financial systems, communications)
- Investigate means of mitigating and preventing problems that could arise from AI, human-interface, and other emerging technologies
- Advance research efforts in quantum computing, communications, sensing, and encryption capabilities
- Foster development of computing paradigms and algorithms that accommodate for data volume and uncertainty

Appendix D. Future of Population and Earth Systems

This appendix provides a snapshot of key themes discussed at the Future of Population and Earth Systems Workshop on 8/23/17.

What dynamics and key questions might shape global security, population, and Earth systems in 20 years?

Climate change, population growth, and resource constraints threaten national and global security, stability, and peace

Climate change, exponentially increasing population, and constrained resources will continue to impact unrest and conflict at multiple scales. Drought, food shortages, sea level rise, and increasing storm frequency and intensity will contribute to the destabilization of social, economic, and political systems. Interdependent dynamics of migration, urbanization, and economic inequality will be complicated by religious and ideological extremism and ethnic conflict. Together, these dynamics will create a global system of unparalleled complexity.

- *How might individuals, societies, and governments balance shifts in resource supply and demand as a way of maintaining security, stability, and peace?*
- *To what extent will increasing resource demand and declining supply create increasingly fragile social and governance systems, the collapse of which further contributes to cascading unrest, insecurity, and conflict?*
- *How might populations, governments, and corporations respond as parts of the world become more accessible or less inhabitable?*

Rapid technological innovation promises solutions, however unintended consequences could exacerbate problems

Public and private sector innovations in sensing and data analytics have the potential to significantly increase our ability to anticipate and understand the complex relationships between Earth systems, population, and conflict. Simultaneously, innovations designed to provide solutions to climate change and resource constraints (e.g., geoengineering, genetic modification, desalination) may create unintended consequences at various scales. The inability of governance systems to keep up with the pace of technological change may create turbulent social and economic shifts.

- *How might advances in autonomy change the nature of work and affect industrialization, inequality patterns, and migration?*
- *To what extent might the combination of technological and governance innovations enable populations to anticipate, withstand, manage, adapt, and recover from emerging challenges?*

Shifting patterns create opportunities for new actors to drive change in an increasingly polarized world

Emerging state and non-state powers will challenge and transform the international norms and agreements shaping global security. Shifting patterns in climate, globalization, industrialization, demographics, and wealth may contribute to the rise of non-state actors driven to address these global problems. All the while, political polarization and mistrust in science erode the capacity of governments to adopt policy and develop technologies that can adapt to future challenges.

- *To what extent, and through what mechanisms, will state and non-state actors, including cities and multinational corporations, cooperate to address emerging security challenges?*
- *To what extent will populations in industrialized and emerging economies choose to and be able to alter resource consumption and reproduction rates?*

How might the national security enterprise prepare for emerging national security challenges and opportunities?

Advance the capacity to collect, integrate, and analyze data, and model complex adaptive systems

- Better understand the interdependencies of disruptions to Earth systems with socio-political-technical systems and how all contribute to instability, insecurity, and conflict
- Improve understanding of uncertainty associated with consequences of population and resource management options and risks

Develop tools and technologies that foster resilience, flexibility, and high speed decisions

- Foster partnerships across multi-disciplinary, multi-sectoral experts and institutions to better understand technical solutions to social- and governance-related challenges
- Build collaborations with academia and industry to assure greater resilience for critical infrastructure, including energy, water, food, and sanitation systems
- Encourage basic research, innovation, and risk-taking in Earth systems research and development (R&D)

Enhance existing approaches and explore new ones for more effectively communicating science & technology insights

- Improve science-based policy making by supporting better assessment of complexities, security options, potential consequences both intended and unintended, risks, and uncertainties
- Strengthen public trust in science through broad education and communication initiatives

Appendix E. Future of Innovation

This appendix provides a snapshot of key themes discussed at the Future of Innovation workshop on 8/30/17.

What dynamics and key questions in innovation are expected to shape the global security environment in 20 years?

Loss of US innovation superiority: The US Government funding of research and development (R&D) is waning. Foreign government investment, private investment, philanthropy, and crowdsourcing are increasing, challenging the USG's asymmetric innovation advantage and influence. Negative perceptions of national security work and the dwindling number of US citizens pursuing relevant disciplines are shrinking the potential national security R&D workforce.

- *To what extent will effective future US national security require technical versus non-technical innovations?*
- *How might greater non-governmental involvement in, and control over, R&D affect US national security?*

Shifting research models: Rapid global connectedness, mobility, rapid prototyping, and informational access are transforming research models, blurring the traditional roles of research institutions, and decentralizing development. Innovation is being fostered in these new models, but with inadequate mechanisms to identify and safeguard against the unintended consequences of their availability. Consequently, growing numbers of cross-cutting, multi-use technologies with highly disruptive applications (e.g., biotechnology, autonomy, advanced manufacturing) require national security attention.

- *What options might entities pursue to manage innovation areas that are evolving too rapidly for effective regulation?*
- *With the rate of technical innovations per capita decreasing, how might evolving research models reverse this trend?*

Interplay of social dynamics and R&D: Innovations are changing social behaviors, interactions, expectations, and outcomes. Rapid global connectivity has altered notions of privacy, generated new social network-based identities, and begun transforming the nature of employment and education. New platforms offer the opportunity to disrupt technological and informational exclusivity, while also potentially further embedding a wealth-skewed distribution of innovation benefits. Emerging technologies may offer mechanisms for overcoming persistent bias (e.g. accent bias) and inclusion issues in communication. Proliferation of disinformation and catered information is elevating the importance of trusted relationships—both human-to-human and human-to-machine.

- *To what extent does the rate of innovation impact socioeconomic stability and, thereby, US national security?*

Evolving human experiences: Innovations are transforming sense-based, relational, and technical experiences. Artificial intelligence (AI) might approach human intelligence, human augmentation could generate unnatural experiences, and virtual reality promises "real" experiences of constructed environments. Human knowledge is increasingly mediated through these innovations, making them both vulnerable to, and proposed solutions for, a growing set of risks, including disinformation campaigns and new warfare. Thus, the means, mechanisms, and expectations for substantiating these experiences will need to evolve for rational inference to be valid. Absent sufficient substantiation, these innovations could be fundamentally destabilizing for individuals and institutions.

- *How might innovations alter the notion of being human?*
- *How might the emergence of decentralized ethical norms affect the intent, function, and evolution of innovations?*

How might the national security enterprise prepare for emerging national security challenges and opportunities?

Develop and support an innovative culture in R&D institutions

- Embrace risk: view failure in research as learning; break the strict unification of resources with achievement; streamline monitoring, reporting and oversight of activities; stimulate creativity and motivation; provide access to resources; encourage cross-fertilization; utilize all sources of emergent global information
- Promote agility, flexibility, and responsiveness: possess a willingness to let go; observe the environment; challenge the role of the institution in the evolving environment; understand the cost vs. value of innovation
- Cultivate the workforce: encourage multiple genders, ethnicities, and religions to join national security fields; embrace social sciences, behavioral sciences, and innovations (chiefly AI) to increase the capacity for security preparedness and effectiveness
- Take an ensemble view of innovation: actively recognize the polarities within the spectrum of innovation (e.g., an existential threat offering the best motivation vs. individual passions)

Ensure innovation advantage through early adoption of global developments

- Continually monitor and engage with global innovation developments that have national security implications
- Exploit national security implications of innovations through their early adoption

Reestablish image of national security innovation work as purposeful and impactful through a nation-wide branding campaign

- Generate a cross-cultural, cross-generational narrative portraying the altruistic aspects of national security work
- Promote individuals who embody a reverence for curiosity, learning, and knowledge


Sandia National Laboratories