SCHAR SCHOOL OF POLICY AND GOVERNMENT
Center for Security Policy Studies
at George Mason University

Fourth Annual Symposium on International Security

"Technology and the Future of Warfare"

September 24, 2021

Panel 1: "Tools: Identifying the New Technologies being Integrated into Defense Capabilities"

Changing Concepts/Definitions of War and the Challenge of New Technologies – Forrest Hare

Dr. Forrest Hare is a cyber operations solutions developer at SAIC and adjunct professor at George Mason University. Prior to his retirement, he served 28 years in the U.S. Air Force and had assignments in targeting, signals intelligence, information operations, and cybersecurity policy. He earned a PhD in public policy from George Mason University,

Bio Technologies – Stephanie Rogers, acting assistant director for biotechnology at the Office of the Undersecretary of Defense for Research and Engineering

Dr. Stephanie Rogers is the acting assistant director for biotechnology at the Office of the Under Secretary of Defense for Research Engineering. She previously served as vice president of IQT Labs Operations and Bioinformatics and vice president and deputy director of B. Next at In-Q-Tel. She holds a PhD in plant pathology from Oklahoma State University.

Evolving Debates about Cyber as a new form of Warfare – Mark Montgomery, Cyber Solarium

Mark Montgomery is the executive director of the Cyberspace Solarium Commission. He previously served as policy director at the Senate Armed Services Committee under the late Senator John McCain. He served in the U.S. Navy for 32 years as a nuclear trained surface warfare officer before retiring in 2017 as rear admiral.

Moderator: Forrest Hare, GMU and SAIC

Dr. Forrest Hare opened the panel with remarks regarding technology's revolutionary impact on the nature of warfare. Key examples illustrate this point over time, from the introduction of nuclear weapons to the development of space capabilities to the dawn of the internet age and the challenges of cyberspace.

Cyberspace has changed the nature of warfare in two important ways: First, cyberspace has democratized access to powerful technology. Critical technological capabilities, once available exclusively to rich and powerful nations, are now ubiquitous. Second, Cyberspace has itself become a domain of conflict.

Dr. Stephanie Rogers and Biotechnologies

Rogers opened with two general points. First, she highlighted ways in which the Department of Defense may utilize biotechnology to better execute its mission; second, she underscored obstacles that undermine US biotechnological superiority.

Biotechnology is an engineering discipline that uses living things to bolster the production of food, tools, and textiles. The Department of Defense seeks to apply biotechnology to augment the warfighter's capabilities. For example, Dr. Rogers outlined how biotechnology can enable servicemembers stationed in forward operating bases to produce their own food, thus reducing the burden on the supply chain. Other applications include enhancing thermal technology, developing cutting-edge medicines, and increasing access to potable water.

Dr. Rogers outlined four issues that undermine US biotechnological competitiveness. First, the difficulty in retaining, training, and recruiting an effective workforce—from PhDs to those with trade skills. Second, overcoming infrastructure difficulties. US laboratories are well -resourced and highly effective; however, the US manufacturing base is lacking (a reality made clear by the COVID-19 supply chain problems). Third, derisking investment to better engage private industry. Fourth, protecting technology from intellectual property theft, thus preserving the US advantage.

China's five-year plan includes large investments in biotechnology. Those who lead the bio revolution will hold a critical advantage. In the words of Dr. Rogers, "it will take an all-of-nation approach."

Mark Montgomery and Cyber as the new form of warfare

Montgomery illustrated how cyber may be better integrated into a broad deterrence strategy. It's clear that the US must do a better job defending in cyberspace. The US responses to cyberattacks are generally slow and mute, particularly with respect to attacks that are below the threshold that would generate a military response. The US economy, for example, lost roughly one trillion dollars in potential GDP over the course of a decade due to intellectual property theft, but the US government does not respond to this as a form of warfare.

Two factors explain the slow US response: first, adversaries have become experts in "grey zone" operations (operating just below the threshold that would provoke a kinetic US response); second, democracies by their nature struggle to counter grey zone warfare. As autocrats authorize grey zone operations, democratic leaders must attain a higher threshold of consensus to respond. Democratic systems require a level of consensus that autocracies do not. The dangers are clear. Failing to counter cyberwarfare puts critical medical, informational, and electoral infrastructure at risk.

Current US cyber deterrence is not working, but Montgomery outlined a three-part strategy that can:

- First, we must defend ourselves. Banks generally have the strongest, best-resourced cyber security, but local and state governments suffer from outdated systems and a chronic lack of funding. Policymakers must figure out how to increase the cyber budget for these underfunded entities. To achieve these ends we must better organize the cyber security complex, which includes raising funds for the Cyber Infrastructure Security Agency; we must also build better system resiliency so victims can more quickly rebound.
- Second, we must increase cooperation between the public and private sectors. Roughly 85 percent of critical infrastructure is owned by private industry or local government. One recommendation is to elevate the cyber security ecosystem, helping all stakeholders.
- Third, we must leverage law enforcement, economic, military, and diplomatic tools to impose greater costs on attackers. This includes working with international partners to promote norms in cyberspace.

Noah Zoroya, CSPS Student Fellow, MA candidate in International Security