National Security Innovation Forum

The Impact of Artificial Intelligence on National Security

How might AI be used to strengthen national security—and how well-positioned is the United States to address potential challenges? On March 17, 2021, global experts gathered virtually at the National Security Innovation Forum to discuss the impact of AI on national security. A collaboration between the UC Institute on Global Conflict and Cooperation (IGCC), the Silicon Valley Defense Group, the National Security Innovation Catalyst, and partners from the United Kingdom, Australia, and Canada, the Forum brought together specialists from government, academia, and industry to address key national security issues raised by AI and potential solutions.

National Security Innovation Forum Speakers:

Stephen Bornstein, CEO, Cyborg Dynamics Engineering

Tai Ming Cheung, Director, UC Institute on Global Conflict and Cooperation

Tobias Feakin, Amb. for Cyber Affairs and Critical Technology, Australia Foreign Affairs

Joe Felter, Former Deputy Assistant Secretary of Defense for South and Southeast Asia; IGCC affiliated researcher; senior research scholar at the Center for International Security and Cooperation, Stanford University

Eric Fournier, Director General for Innovation, Defense Research and Development Canada

George Galdorisi, Director of Strategic Assessments and Technical Futures, Naval Information Warfare Command Pacific

Mike Gibson, Deputy Head Defense Autonomy Unit, UK Ministry of Defense

Bill Greenwalt, Visiting Fellow, American Enterprise Institute

Katharina McFarland, NSCAI Commissioner

Steven Meers, Head of AI Lab, Dstl

Duane Rivett, Co-Founder & VP National Security, Fivecast

Raj Shah, Executive Chairman & Co-Founder, Resilience; Shield Capital

Commander Rachel Singleton, Royal Navy British Defense Staff (US) lead for Maritime C4ISR and AI

ADM(Ret) Scott Swift, Former Commander, U.S. Pacific Fleet

Scott Tait, Executive Director, Catalyst

Sarah Tatsis, Senior Vice President, Advanced Technology Development Labs, Blackberry

Mac Thornberry, Former Chair of the U.S. House Armed Services Committee

National Security Innovation Forum
The Impact of Artificial Intelligence on National Security[1]

March 17, 2021

Understanding the AI Challenge

A new generation of technologies is transforming the nature of warfare, and the Department of Defense (DoD) must change decisively in the next five years to meet the rising challenge of artificial intelligence (AI). The National Security Commission on AI hopes that DoD will be "AI-ready" by 2025, meaning that "warfighters [are] enabled with baseline digital literacy and access to the digital infrastructure and software required for ubiquitous AI integration in training, exercises, and operations."[1] But can DoD reach that goal in just five years? What relationships and capabilities will be needed, at home and abroad, to enable the United States to effectively lead on the new digitized frontier of national security?

To address this challenge, the National Security Innovation Forum convened virtually on March 17, 2021 to discuss the impact of AI on national security. Bringing together perspectives from government, academia, defense, finance, and start-ups in the United States, the United Kingdom, Australia, and Canada, the Forum identified specific, urgent challenges along with concrete solutions.

Participants observed that the democratic ethics and regulations that would ideally govern the worldwide applications of AI are lagging behind its global application. This is due to the fact that many leaders do not yet fully grasp how AI can transform national security. Just in the last decade, AI has advanced from research to reality, finding applications across a range of industries. Its development has not been confined to the borders of one nation, or at the initiative of one government; it has grown independently from the influence of free markets and democratic public policies. Its impact will not only be social and economic, but also political and strategic. The United States needs to work with allies, partners, and other like-minded countries to harness the potential of AI in the pursuit of common interests and shared values.

> ***"Another challenge for all institutions and governments is managing the risks associated with managing the security of our innovation without inhibiting the creativity that drives it."***
>
> *— Dr. Tobias Feakin, Ambassador for Cyber Affairs and Critical Technology, Australia*

The Reality of Great Power Competition

[1] This report was prepared by James Lee, a postdoctoral research associate with the University of California Institute on Global Conflict and Cooperation (IGCC), which is based at UC San Diego.

One participant explained how China has both strengths and weaknesses: its techno-nationalist strategy allows its military to quickly absorb and adopt new technologies, but it struggles to develop novel research and produce indigenous innovation. The United States has the opposite strengths and weaknesses: it excels at research and innovation, but it is lagging behind in adoption.

Perhaps ironically, China's drive toward civil-military fusion is an attempt to replicate the United States' defense ecosystem from the Cold War, when government, industry, and academia worked together on rapid research and rapid deployment. As one participant noted, this system had many achievements: the first nuclear weapons systems, intercontinental ballistic missiles, nuclear submarines, the U-2 & SR-71 aircraft, reconnaissance satellites, geolocation, and stealth technology. Such a productive ecosystem no longer exists in the United States. Today, rigid budgeting and acquisition requirements confound a cumbersome contracting system that forces new technologies into a sometimes decades-long "valley of death" that prevents the rapid and effective application of emerging technologies. Meanwhile, the private sector has continued to innovate at a rapid pace: it took only five years for AI to transition from applied research to production-level applications. If DoD is going to use the cutting edge of commercial technology, it has to keep up with the advancing pace of commercial innovation.

Addressing the Challenge

To meet China's challenge, the United States will have to change how it does business at home and abroad. To be AI-ready by 2025, the United States will need to accelerate innovation and adoption. The government should develop faster pathways for both acquiring and deploying new AI capabilities. Congress will need to provide DoD with enhanced spending flexibility to invest in technology developments, without the two-year projection lag currently required by the Congressional budgeting process. To make funds available as needed, Congress will rightly wish to monitor the use of those funds in real time as opposed to the cumbersome manual review process currently employed by congressional staffs. Interestingly, properly deployed AI tools could be used to remove much of the manual labor associated with this oversight and allow for streamlined real time supervision. Achieving a shift in appropriations on this scale will not only require a massive alignment among Congressional Members, but must also be bolstered by broad cultural change within DoD: without losing focus on the mission, DoD must regain its comfort with rapid and repeated failure as a pathway to learning and advancement. Traditionally, Program Executive Officers (PEOs) have been rewarded for stability. Now they need to be rewarded for disruptive risk-taking and innovation.

> ***"It's not about rewarding those that are embracing AI and embracing risk. Let's start with the easy stuff: let's stop punishing those that fail when they do so. There is such a disincentive for acting in this space on the defense side. On the industry side and the civil side, you're rewarded for it: fail fast, fail early...it's this cultural divide that I think there's an opportunity that SVDG has to bring these cultures together and find those areas of collaboration and progress that can be made."***
>
> *— Ret. ADM Scott Swift, US Navy*

At the same time, the U.S. must deepen its cooperation with allies and partners, starting with the Five Eyes. The U.S. government will benefit from new standards to make it easier to pursue research and development with other liberal democracies. The United States should capitalize on the fact that it has many friends in the world, and reform its export-control policies accordingly. A "free trade zone" among U.S. companies, the U.S. government, and allies and partners, combined with a series of wargames and exercises, could expand the ability of Five Eyes partners to work together to compete with China on shaping AI's future.

Being like-minded does not mean being in perfect agreement. It means that priorities and objectives are the same, though tactics, strategies, and approaches may differ. The need for global leadership, interoperability, and burden-sharing provides a strong reason for collaboration on AI among the Five Eyes, but it is likely that countries will have different approaches to AI ethics. Ethics and standards should remain at the center of discussions surrounding AI deployment, and greater discussion of these questions will promote greater trust and understanding.

> ***"Operating together in the future is likely to require the seamless transfer of data between nations' systems, so that might need a new era of data-sharing agreements. And there may also be questions of which nation's ethical principles a system has been designed to, and whether each nation trusts each other's systems – trusts their anti-bias mechanisms, the testing and evaluation that's been used in their design. So coherence across our approaches to AI ethics is also going to be key."***
>
> *— Commander Rachel Singleton, Royal Navy*

Focus on the Mission

AI will enhance, not replace, human decision-making. Participants stressed that the focus should continue to be on the mission: DoD should identify individual applications for specific programs and not just a general interest in using AI; similarly, technology companies should not represent themselves as "selling AI," but as providing DoD with a discrete capability that will enable it to achieve individual missions. Since the missions of DoD will involve coordination and cooperation with the United States' allies and partners, the development of AI-enabled and AI-enhanced capabilities should also involve coordination and cooperation. The table below summarizes the recommendations that participants at the National Security Innovation Forum offered for the United States and allied countries going forward:

Area	Recommendation
U.S. private sector	• Contracts need to have specific, measurable ways of evaluating performance by technology companies • Find ways to work with start-ups and non-traditional companies • Make it easier for technologists to move back and forth between government and the private sector while maintaining their clearances

U.S. government	• Reform funding and acquisition to promote flexibility • Use real-time analytic dashboards for oversight • Employ AI in military decision-making and training (e.g., augmented reality) • Start with back-office applications where there are real advantages that can be achieved with AI (e.g., preventative maintenance) to build momentum for broader adoption • Give the Department of Defense tools to speed up the validation of AI
Five Eyes partners	• Lower barriers and fast-track for Five Eyes partners (FOCI ("Foreign Ownership Control and Influence") mitigation, facility clearance, CNMC, FEDRAM, reciprocity of security clearances) • Revise ITAR (the export-control process) to create a "free trade zone" between commercial companies, government, and our allies • Establish a collaborative AI laboratory for alliance members to test and evaluate each others' capabilities • Combined series of war games and exercises for AI capabilities