Artificial Intelligence and National Security –
The Race to Build an Information Age Force

At the fourteenth installment of the Asymmetric Threat Symposium this past October at the National Press Club in Washington, D.C., speakers, panelists, and moderators remarked that the return of great power competition to the forefront of national security in the 21st century is happening at the same time the world's powers are locked in Information Age technology competition – specifically, a race to explore, create, and adopt artificial intelligence (AI) and machine learning (ML) tools and technologies.

Today's competition is fundamentally different from those of the past, symposium participants noted. Where national power in the 20th century was often measured by the development of industrial warfare tools to enforce geopolitical might – such as the aircraft, modern radios, submarines, and mobile armored formations – today's Information Age power is far more complex. From defending against crippling cyberattacks, to intelligence analysis, to distributed unmanned aircraft operations, AI and ML is becoming more entwined with the modern instruments of defense and national security as it has with many aspects of modern life from banking to home video streaming services. "I don't see AI as a separate instrument of power. You have the DIME, whether it's diplomatic, information, military, or economic," said Congressman Don Bacon, the U.S. Representative from Nebraska's 2nd District and a retired Air Force brigadier general. "I see AI as embedded in all four of these, and over time, it has to be inherent in each of these four."

In the 21st Century AI will be critical to everything across both peaceful competition and/or armed conflict since it delivers unprecedented speed for a host of activities and capabilities – from intelligence preparation and analysis to information processing and targeting. In this aspect, it is far more transformational than any one military capability, and will require changes to practices, training, and the culture of developing and fielding technologies. "We love talking about AI for national security, but this has... every element of national power involved, probably more than many points in history," said Lt. Gen. John (Jack) N.T. Shanahan, U.S. Air Force (Ret.), who served as the inaugural director of the Department of Defense (DoD) Joint Artificial Intelligence Center (JAIC) from December 2018 to June 2020. America's economic power will depend on how well it embraces AI tools and algorithms, just as much if not more so than the military and national security aspect.

CACI Senior Vice President and Strategic Advisor Lt. Gen. Mike Nagata, U.S. Army (Ret.) noted that according to one recent analysis, the market for AI around the world is expected to grow from $30 billion in 2020 to around $300 billion by 2026. While AI has been under development for decades as computer technology has advanced, it has now arrived at its transformational moment. "Some people recognize it, but unfortunately a lot of people don't either understand it, don't recognize it, or choose to ignore it," Shanahan said. "We don't have that luxury anymore. We have to move."

But it is culture rather than technology that is one of the largest challenges to overcome, several panelists noted. The DoD, the Intelligence Community (IC) and other national security organizations are all shaped by Industrial Age processes and structures, from planning to acquisition to operations. Making a "mental transition from an Industrial Age, hardware-centric force to a digital age, software-centric, more risk tolerant one is hard," Shanahan added.

As an example, Lt. Gen. Karen Gibson, U.S. Army (Ret.), one of the event's moderators, former Deputy Director of National Intelligence for National Security Partnerships, and former U.S. Central Command (CENTCOM) Director of Intelligence, noted that when she was directing intelligence-gathering and analysis operations at CENTCOM, the command had "terabytes of data" on hand from the smart phones of ISIS prisoners. However, her staff had few other means other than manually searching through the information to find what they were looking for. "I would walk back to my hooch at night, picking up my iPhone at the door," she recalled. "I knew that if I had taken a picture that day (at dinner) and I opened it, my phone would say 'is this Jack Shanahan?' with a little square around your face," she explained, using a theoretical picture taken of Shanahan using a common iPhone feature. This was a revelation, she added – in that it shows consumers could easily access a capability she needed badly on the battlefield for common everyday interactions, but as the top intelligence officer in the Middle East, she had no way of applying that capability at CENTCOM to find ISIS leaders.

The example illustrated a problem nearly all participants remarked on, regarding AI and its role in national security. Unlike the advances of World War II and the Cold War, the true innovation and advances in AI and ML today are coming from the private sector. The good news is that there is progress under way in building better relationships, as more and more companies see that there are "natural competitive advantages" to be had by helping the government accelerate a transition from a military defined by industrial processes to one that is comfortable operating in a digital world, Shanahan noted. Government can facilitate, incentivize, and provide some vision, Congressman Bacon added. "But it can't impede the discoveries, and it can if it's not careful." National security leaders and Congress must find a balance between incentives, funding, facilitating and "getting out of the way, so we don't impede what industries and academics find," Bacon said. While much has been written about China's "top down" approach to AI research and its ability to tap into the enormous data pool of its population, that alone does not provide advantage. "We have innovation. We have strength from the bottom up, but we just have to harness it and incentivize it."

The fielding of technology is not just a research and development issue, many observed, but one that involves technology capability, talent, and culture all being modernized for Information Age warfare. The technology sector has accumulated years of knowledge, process, governance, and valuable insight into AI and how it works, said JAIC Chief Technology Officer Nand Mulchandani.

"The places and areas where (AI) has been applied (it has) absolutely revolutionized things, but there are still waves and waves of more coming that ... is still very much in its infancy," Mulchandani said. But when it comes to applying AI to joint warfighting operations or targeting or other "tactical end" aspects of warfare, this is still very far out in terms of both research and the ability for the United States military to deploy the technology and be comfortable enough with the issues involving trust and ethics around it, he noted.

That understanding and expectation gap will be bridged with time. But more and more there is appreciation across the technology sector and in the U.S. Government that AI advances will be for the good of the United States and its allies around the world, several participants noted. "We tend to focus on sort of the weapon systems," Shanahan said. But there is no field that will not benefit in some way from AI – from human resources to personnel management, medical records, and more. The U.S. Government, DoD, academia, and industry working closely is vitally important, and a powerful part of making sure American efforts to lead the way in AI succeed, he added.

Former Army Secretary Ryan McCarthy, who worked for former Secretary of Defense Robert Gates during his tenure, observed that how DoD is approaching AI is already seemingly different from how it built up cyber capability a decade ago – leading to the establishment of U.S. Cyber Command (CYBERCOM) in 2010. The way DoD is approaching AI development is "much more joint," McCarthy said. "It's very encouraging, and I think that if you compare cyber to AI, we've gotten out of the gates better, and the Department is essentially focused on this issue."

Old acquisition practices will have to be significantly reformed or scrapped if the race to integrate AI is to succeed. "If our AI follows the same roadmap as the F-35, we will lose," Bacon said bluntly. Working

on technology like AI, it is no longer sensible to have decade-long acquisition processes built to mature hardware like aircraft and vehicles. However, he noted, there is progress on this front already since the 2020 National Defense Authorization Act (NDAA) contained a provision that gave the U.S. military the authority to jump over some acquisition barriers to develop certain AI-related tools. But a continuing conversation between industry, DoD, and Congress will be important to improving acquisition and increasing the delivery of important capabilities to the servicemembers who need them. Shanahan noted that DoD's JAIC has put in place a new acquisition and contracting model, called TRADEWIND. "This consortium approach to acquisition of emerging tech takes advantage of some hard lessons learned over the past few years. In the digital age, we have to move much, much faster. If we don't, we could lose," he said. "Provide the authorities to allow more agility and flexibility, while still insisting on accountability for how the taxpayers' money is being spent."

Speed is not only essential in acquisition but applying the speed AI provides to a host of information-dependent military capabilities will require wisdom as well, Nagata said. The U.S. has immense capability in collecting information from sensors and systems across the services, but having more information than anyone can use or process is not good and creates a collective "cognitive burden" for DoD. The military services and the IC must be able to amass enough information for "the problem being faced," he said, and as this is done be able to sift through and evaluate the data and separate out what has "operational value" from what is less relevant to immediate need and can be evaluated later.

The U.S. military has invested greatly in being able to aggregate large sums of data, Nagata added, and the fact that now national security leaders can talk about concepts such as cloud-based storage, data lakes, and data reservoirs with ease – all of which are accessed by various forms of AI – "is emblematic of how much emphasis and genuine progress we have made in that aggregation of mountains of data." The next step where investment is needed is to adopt new capability that can "curate and deliver" data in ways that operators and warfighters can use effectively without substantial distraction from their mission. Nagata's point was echoed by the Joint Staff's Director for Command, Control, Communications, and Computers/Cyber and Chief Information Officer Lt. Gen. Dennis Crall, U.S. Marine Corps who said that effectively managing the data load in the best of environments – much less ones where an adversary is actively trying to attack you – is going to prove difficult as tools and algorithms mature. But it is important to not lose sight of the warfighting requirements as AI's use expands in the DoD. "There will be challenges in the electromagnetic spectrum," Crall noted. "There will be challenges with integrity of data to make sure that the idea of reach back models or big pipes to process data may not be available. So, we have to look at how we do this work that we're talking about at the speed of relevance on the tactical edge, and that is no small task."

From balancing capability with the ethics of using AI to make rapid decisions in warfare, to building trust in these new systems and applications, the choices America must make in the years ahead will require industry, government, academia, and others to embrace and nourish a "spirit of ruthless experimentation and substantial risk tolerance" if we are going to reach the goals of unprecedented data curation and aggregation that all national security missions will require, Nagata said, adding that we cannot allow ourselves to become complacent or think our standing as a pre-eminent military power gives any advantage in this new Information Age competition.

Retired Air Force Gen. Paul Selva, the former Vice Chairman of the Joint Chiefs, noted that this era of military competition is distinct from those of the recent past because today, "servicemembers, leaders, and those working on AI in the private sector are dealing with technology that is not as familiar as concepts such as the internal combustion engine or radio was to people in World War II." This technology change is about a capability that "all of us may not completely understand," he added. Even though we carry around capable smart phones and devices, we don't necessarily understand or appreciate how information travels on that device, and how it gets to us and influences us, Selva said.

As AI is studied more, and its effect on warfare scrutinized, we must think about how to understand it in a cultural context, Selva noted. "What I would encourage is a healthy amount of skepticism about the technology, but real enthusiasm about its potential." And when you put those things together, you get a set of dynamics that will allow us the ability to affect the "human dimension" of warfare, empowered by AI, in a way that will truly make us more effective, he said. ■