Data is Fundamental to Artificial Intelligence in Government

Government, Industry, and Congressional Leaders Discuss the Impact of Artificial Intelligence on Homeland and National Security

(Washington, D.C., September 25, 2019) The United States has arrived at a critical inflection point as artificial intelligence (AI) will vastly impact the daily lives of citizens and deliver unprecedented capabilities across the public and private sectors. Within the federal government, agencies are already adopting AI and devising strategies for how to effectively utilize this transformative technology—in particular, the use of AI has been most consequential in supporting the mission sets around homeland and national security. On September 25, 2019 the Center for Public Policy Innovation (CPPI) and Homeland Security Dialogue Forum (HSDF) convened a policy symposium to explore strategies for the development and deployment of AI. The wide-ranging discussion highlighted current use case scenarios, the importance of data to accelerate AI adoption, and the need for industry-government collaboration in the United States to stay ahead of adversaries in this area.

While certain parts of the government have detailed an AI strategy—for example, the Department of Defense (DoD) released their strategy in 2018 and the National Institute for Standards and Technology has issued a plan for guidance around standards development—many questions remain. For example, the rise of computing power has created some narrow AI capabilities in government, but with the amount of data collected by government there are many more possibilities: *How can the government position itself to take advantage of more sophisticated AI capability down the road?* The CPPI and HSDF event brought to light the thinking of experts from Congress, the Department of Homeland Security (DHS), Central Intelligence Agency (CIA), and U.S. Air Force (USAF), along with industry perspectives from Booz Allen Hamilton, IBM, Oracle, Peraton, and ServiceNow.

Congressman Jerry McNerney delivers a keynote address

How Congress and Federal Agencies are Approaching AI Adoption and Dispelling Myths

The keynote speaker at the symposium, Congressman Jerry McNerney, serves as co-chair of the Congressional Artificial Intelligence Caucus. He spoke candidly about the lack of understanding generally in Congress around AI. "Most people in Congress look at artificial intelligence as symptoms [of technology] that are kind of scary. They don't know a whole lot about it and they hear that it will be displacing 40 million jobs in this country. I want to make sure that we get enough information and knowledge out in Congress so that we can use AI to benefit society, rather than displacing a lot of people."

The Congressman mentioned a bill he introduced titled the AI in Government Act of 2019 that has bipartisan support and a companion bill in the Senate. The legislation intends to create an AI Center of Excellence within the General Services Administration and creates a new hiring pathway for AI experts in government. He was adamant about the need for skilled labor and education around this issue for the U.S. to stay competitive in this area.

Congressman McNerney emphasized the need for continued investments in AI technology from both the public and private sectors. "We don't want to fall behind in military technology, history's clear about that. The team that has the best military technologies are most likely to win a competition, whether its lethal or not." He also said the U.S. has an opportunity to "incorporate our values" into the development of AI technology ensuring that privacy and protection of personal liberties are part of the equation, which would distinguish our technology from China where there are no privacy boundaries or many ethical considerations.

When the discussion centered on the panelists, two government experts were able to layout in detail how their specific agencies were approaching AI. The AI advisor for the Cybersecurity and Infrastructure Security Agency (CISA) at DHS, Mr. Martin Stanley, said they have three major considerations when it comes to this technology:

- How emerging technology can be leveraged by our adversaries;
- Understanding the attack surface and how that changes with AI;
- How CISA can leverage the technology inside their program to find greater cyber capabilities and efficiencies, and make their dollars go further.

The U.S. Air Force is approaching AI in a way that will support the 2018 National Defense Strategy. According to Colonel Jason Brown, Director of the USAF Strategic Studies Group, this includes four major lines of effort: expanding the industrial base, developing software at scale, partnering with industry and academia to apply cutting-edge research, and cultivating digital talent.

> "As federal agencies adopt AI technology, it's critical that they do so in a responsible way, and that they are equipped with the expertise and tools they need to succeed. That's why this legislation is crucial. It will help the federal government to harness the full potential of AI while also identifying and reducing potential harmful effects."
>
> *- Congressman Jerry McNerney on the AI in Government Act*

IT Modernization in Relation to AI

Artificial intelligence cannot exist on outdated legacy systems. “It might be easy to jump on the cool factor around AI, but that can’t be a reality without trying to do the hard work of having your data organized, having your data classified, and having modern systems,” commented Jonathan Alboum, Principal Digital Strategist for ServiceNow and former Chief Information Officer (CIO) at the Department of Agriculture. Oftentimes, the government budget focuses on the operational elements within an agency, and then the IT infrastructure and oversight functions at the headquarters level can fall behind—this becomes a major challenge in adopting emerging technology.

Part of the Air Force’s AI strategy centers on organically developing software at scale. According to Colonel Brown, this requires migrating existing infrastructure to the cloud as quickly as possible, and both Kubernetes and DevSecOps are a big part of the equation. He also mentioned the success of several “software factories” started by Kessel Run—the Air Force’s in-house software development group.

The Underlining Importance of Data

One recurring theme throughout the symposium was that AI is all about the data. “There's never been more data than right now, and it’s being created every single day in the national security enterprise. What are we going to do with all that data?” commented IBM’s Don Fenhagen helping stage the discussion to follow.

“Data of all types, of all forms, of all languages come in at alarming rates, alarming variety, and at an ever-increasing pace. We have a finite workforce that has no chance whatsoever of keeping up with the pace, variety, and velocity, and volume of that data without some automation aid,” commented Dr. Raymond Cook, Chief Technology Officer (CTO) for the CIA’s Directorate of Science and Technology.

The Department of Homeland Security collects vast amounts of structured data and the agency is beginning to see “non-obvious connections and patterns when the right computational environment exists,” commented DHS Acting Deputy Under Secretary of S&T Andre Hentz.

Data availability is still an issue for federal agencies both in terms of giving access to analysts and mission operators, as well as interacting with industry partners to develop new solutions and tools. “How do you finesse that data in a way that enables humans to access it in a security-proof way, because everything we do at the CIA is a little bit unique, and is on the high side. We're operating on a very highly-classified and controlled information infrastructure,” said Dr. Cook.

He also discussed data in the context of training automated systems commenting that while the CIA has tons of data, ensuring that the data is “well-labeled, trustworthy, and verifiable” is still a challenge. Then the issue of bias comes to the forefront and the agency is looking at not just how to eliminate bias, but also understanding what the bias is and how to train against biases. As AI systems are developed, there is a great deal of concern in both the public and private sectors that the data being used contains biases around race, gender, and ideology. IBM has done a great deal of research in this area to prevent discrimination in AI algorithims. In addition, the National Institute for Standards and Technology published a report titled "U.S. Leadership in AI" that also discusses the issue of bias as this technology is cultivated.

Steve Escaravage, Senior Vice President of the Strategic Innovation Group at Booz Allen Hamilton, talked about the underlying technologies around machine learning to support AI and the importance of getting feedback from these systems, which enables them as a solutions provider to better support their government customers. One challenge they deal with is around data classification where much of the research and development on these systems uses non-classified information, but the missions themselves deal more on the high-side forcing them to "rethink the infrastructure that's needed to get feedback."

From left to right: Lt. Gen. (Ret.) Kevin McLaughlin, Col. Jason Brown (USAF), Dr. Raymond Cook (CIA), Mr. Steve Escaravage (Booz Allen Hamilton), and Mr. Patrick Sack (Oracle)

Patrick Sack, CTO of Oracle's National Security Group also commented on the importance of a feedback loop with their customers. "We need feedback to make life better for our government customers. Most of the time is spent by analysts finding data. How can we help the data find people instead of people finding data?" He went on to add, "Data has multiple meanings for multiple disciplines and too many times we don't give that data to the right organization to allow them to analyze it. We want to use the same data and enrich it with other data and then apply machine learning. Then we can [create] a better, more secure, and more reliable environment."

Standardization of data was another topic of discussion. Mr. Sack mentioned that each discipline has a different vocabulary to leverage against data, and in some cases, the Intelligence Community and DoD will refer to the same thing using different terms. He suggested that there needs to be a business glossary model that sits on top of the government data to help standardize and uses the appropriate vocabulary to achieve mission outcomes. "That's what leads to fragmentation and ambiguity in all the data because everybody's trying to fit for purpose. We need a way to standardize the data and vocabularies so everybody's using the same data in the right context," he commented.

Dr. Reggie Brothers, CTO at Peraton, pointed to the foundational challenge data presents at an agency like DHS that has a law enforcement mission meaning data can be held up in investigations or for security reasons. Figuring out the proper government protocols for understanding data use and access becomes critically important, and much work remains to be done in this area. The creation of the Chief Data Officer roles across government should help address this issue. Dr. Brothers also raised a point around cultural considerations when it comes to AI, especially in the homeland and national security mission areas, where there are persistent concerns around trusting the data.

"Most of the time is spent by analysts finding data. How can we help the data find people instead of people finding data?"
- Mr. Patrick Sack, CTO,
National Security Group, Oracle

Several of the panelists pointed to data stovepipes that exist across government and the challenge of achieving better data integration and breaking down organizational boundaries. Mr. Sack commented on some of the roadblocks the government faces, "There's authority reasons, there's access control reasons, there's policy, there's legal. There's a whole bunch of reasons, but at the end of the day, if there's data that can be useful for some angle on national security, we should be fully utilizing it. I'm not sure that we are."

Risk tolerance is low when it comes to AI and emerging technology; some use cases are viewed as inherently risky for government. Mr. Stanley commented, "Sometimes we don't know what the risk tolerance might ultimately be for certain solutions, but we do know that expectations on performance are a lot higher." This was a piece of advice for industry when it comes to pilots, to make sure they have their best team in place to hopefully prove out the technology.

Privacy and ethics considerations were raised by the program speakers. While Congress has a role in passing some kind of privacy law, one panelist conceded that the slow pace of the legislature means it will be overcome by related events in this area. It would be preferred to have an ethical framework around AI that agencies, businesses, and individuals can use to guide decisions around this technology.

Investment from Industry and Public-Private Partnerships Are Critical for Success

One of the challenges for DHS S&T is to articulate their specific technology needs to industry, especially since any application needs to link to a specific operator set. Mr. Hentz said they are trying to take a more entrepreneurial approach and discussed the important role that industry can play in helping identify some of the existing technology gaps at DHS.

Mr. Hentz also had some interesting advice for government contractors. He noted that sometimes when solutions are sold to the top of an organization, there can be integration challenges at the back-end and the value of the solution is not fully realized. He suggested that a better way to engage with government is "to work through an integrated solution that is already going to be acquired through FedRAMP, for example."

Mr. Hentz also described how much further ahead China is than the U.S. when it comes to R&D investment in AI. In 2017, China released their AI strategic plan that aims to create a domestic industry valued at nearly $150 billion, outdoing their global rivals in the area of AI. Several of the panelists acknowledged that China is better at making coordinated investments between the public and private sectors when it comes to AI and they also have the advantage of not dealing with the same considerations around privacy and individual rights as compared with other countries.

The Air Force has been working strategically to build-out the industrial base to include start-ups, scale-ups, and small businesses. AFWERX is a good example of this, "They've done an amazing job of establishing various different activities and venues that are bringing the problem-owners at the user-level within the Air Force and getting them in contact with people we don't normally do business with or have never done business with," commented Colonel Brown. They have also been leveraging the Small Business Innovation Research Program (SBIR), making investments in individual companies around $10 million, which is a much larger sum than in past years.

Word cloud from the symposium to illustrate the most common themes in relation to artificial intelligence

The Air Force also has a strategic partnership with the Massachusetts Institute of Technology (MIT) where they have launched an artificial intelligence accelerator program. The Air Force has committed to investing approximately $15 million per year on ten specific AI projects with MIT.

R&D investments from industry are also critical. “Oracle is investing heavily in machine learning to create autonomous systems. It reduces the chance of human error. Now, we are in an autonomous world whether we want to believe it or not and autonomous systems will happen. We cannot be complacent in this world, otherwise we will not be leading and creating advances for the government,” said Patrick Sack.

Steve Escaravage spoke to the need for foundational R&D investments around AI. “There are new generations and algorithms coming out every three months, but we can't get distracted by something that we see today. Foundational investments and having R&D enclaves for machine learning behind the same security architecture at which you conduct operations, that would be the one [very meaningful] thing that would make a difference across the board.”

Dr. Cook observed that five out of the six major cloud players are all U.S.-based companies—this includes AWS, Google, IBM, Microsoft, and Oracle, the only exception being the Chinese company Alibaba. This is a major advantage for the U.S. Government, “[These companies] are spending billions of dollars in driving better IT, bringing machine learning and algorithms to the forefront, working on a daily basis to not only compete with each other, but to change this market and change the world. You have five of the six mega cloud providers available to you that want to change the outcome and invest their dollars in your mission. The government should take advantage of that,” he commented.

AI Use Case Scenarios in Government

From left to right: Mr. Michael Hermus (Revolution Four Group, Mr. Jonathan Alboum (ServiceNow), Mr. Andre Hentz (DHS S&T), Dr. Reggie Brothers (Peraton), Mr. Martin Stanley (DHS CISA)

Panelists highlighted several areas where AI is already in use, or where they would like to see it headed in the near-term.

Jonathan Alboum thought back to his time as a federal CIO and commented that one incredibly useful AI application would be the ability and look at operational data and predict where there is going to be an IT-related outage. "If you can prepare for that outage, you would be the best CIO because you know your systems are never really down."

Mr. Hentz said using AI to address the opioid crisis would be an incredibly valuable application. There are a lot of data points around opioid abuse and drug production ranging from drug monitoring programs, electronic prescriptions, and information on imported materials that can create a fuller picture of abuse patterns and drug origins.

Within the Intelligence Community, there has been a lot of investment already made in using AI and automation for natural language processing and that has been a very valuable asset, according to Dr. Cook.

Oracle's Mr. Sack talked about the benefits of machine learning to understand behaviors and enhance the cybersecurity of systems. The ability to get ahead of the threat is critically important for any organization and enhances resiliency. "Nothing is 100% secure, but you'd better be resilient," he commented.

From a cyber operational perspective, DHS CISA has been evaluating AI solutions and Mr. Stanley commented, "What's good in one particular space and has a narrow application, may not translate to another one. We need good criteria for being able to determine whether a capability is the right fit for a particular mission set." Once that determination is made, there are a number of considerations around the data. For example, firstly, is the data available, and secondly, is the data being used appropriately.

Using AI to address some of the more tedious requirements for defense operations was another point raised during the panel discussion. "Predictive maintenance for the Air Force is a massive project. We have ties to the Joint Artificial Intelligence Center, and there's a lot of great back and forth in this area. This is one of the most mature things we have going on in the Air Force, and it's taken a lot of money."

Workforce Challenges and the Human Element of AI

There's no question that competition for digital talent is a major obstacle for government, and even industry, as emerging technologies drive mission outcomes.

Colonel Brown had some interesting thoughts on this issue, "The reality is that we cannot hire every coder that we need, we're going to have to grow them and make sure we have several different initiatives that relate to getting airmen in every single specialty. We know that every single

squadron in the Air Force is going to have a requirement for digital talent." Part of the strategy includes new boot camps and massive open online courses to get airmen trained.

"We really need to start looking at ways that we can transition [government employees] into new positions and build these human-machine teams that allow the humans to do things that they're good at: dealing with unpredictable, very complex kinds of decisions," commented Mr. Stanley from DHS.

Dr. Cook talked about how the human element around these technologies, "We're getting audio data in different languages from a variety of different places and it's a very important part of the workflow, but it doesn't come close to answering the question and understanding the problem. There's still a human in that loop and a lot of humans in that loop, and there will be a lot of humans in that loop for quite some time." Ultimately, decision-making reasoning still requires a human element, especially when it comes to issues of national security.

"Invest in people. We are not investing enough into cultivating digital talent to the degree that we need, so invest in people, we cannot go wrong," commented Dr. Cook.

Conclusion

Based on the discussion, it is evident that AI is a transformative technology that will have a major impact on mission outcomes in the future. To date, AI has been put to good use for language processing by the Intelligence Community, and maintenance inspections for the Air Force, but it also has the potential to address some of the larger challenges confronting the government, such as battling the opioid epidemic or identifying behavioral patterns of potential terrorist suspects.

Central to any AI effort is the availability and quality of data. Congress passed a law mandating federal agencies appoint or designate a Chief Data Officer (CDO) that will oversee the agency's data inventory and manage the accessibility of data assets. While there are still questions about the precise role of the CDO, they will be essential to creating a data-driven government. IBM's Center for the Business of Government released a report on the role of the CDO and how they can leverage data more effectively.

Another priority is cultivating a talented digital workforce. The government has long struggled to compete with the private sector for talent, and the adoption of more sophisticated technologies only compounds this challenge. For the government, investment in people and training around new AI-related skill sets is necessary to stay ahead of adversaries, especially when it comes to issues of national defense.

Finally, industry plays a vital role in funding AI research and collaborating with government to better serve their needs. This collaboration is critical to help the U.S. maintain a competitive edge against foreign rivals in the global AI marketplace. According to a report from the Congressional Budget Office, industry spends 67% of the national total on R&D. The government's reliance on the private sector to fund R&D for emerging technologies will become increasingly important and speaks to the need for greater public-private sector collaboration. ■

Additional event photos from IBM's Center for Cognitive Government in Washington, DC

About the event organizers:

The Center for Public Policy Innovation (CPPI) is a 501(c)(3) not for profit educational think tank whose mission is to assist government officials in addressing the many challenging issues brought on by the rapid advancement of Information Technology. CPPI provides policymakers with groundbreaking thought leadership on transformational technology, informed policy analysis, and innovative strategies to help ensure American competitiveness in the global economy and comprehensive security on the homefront. CPPI convenes educational symposiums, site visits, and other forums that bring together stakeholders from government, industry, academia, and the civic sector to discuss policy issues in a collaborative environment. For more information visit www.cppionline.org.

The Homeland Security Dialogue Forum (HSDF) was established in 2003 to boost the level of informed dialogue between the public and private sectors on homeland and national security issues and explore the important role of technology in hardening our nation's vulnerabilities. HSDF has organized more than 450 meetings and other special events with top officials from the Department of Homeland Security; other relevant federal, state, and local agencies; and foreign governments. HSDF is supported by a number of leading technology companies and security solutions providers. For more information visit: www.hsdf.org.

Thank you to our event supporters:

Booz | Allen | Hamilton

IBM

ORACLE

Peraton

servicenow