AI RFI Responses, October 26, 2018

Update to the 2016 National Artificial Intelligence Research and Development Strategic Plan RFI Responses

DISCLAIMER: The RFI public responses received and posted do not represent the views and/or opinions of the U.S. Government, National Science and Technology Council (NSTC) Select Committee on Artificial Intelligence (AI), NSTC Subcommittee on Machine Learning and AI, NSTC Subcommittee on Networking and Information Technology Research and Development (NITRD), NITRD National Coordination Office, and/or any other Federal agencies and/or government entities.
We bear no responsibility for the accuracy, legality or content of all external links included in this document.

Recommendations for the US Government's 2018 AI R&D Strategy Update

Dr. Larry Lewis (703.824.2020/lewisl@cna.org)

Director, CNA Center for Autonomy and AI

National security is inherently connected to technology. Throughout history, the ability to adapt technological advances to warfighting has led to fundamental changes in the character of war and the tools used in its conduct. Examples include the development of the crossbow; gunpowder-powered projectile weapons; chemical weapons in World War I; rockets, jet aircraft, and nuclear warheads in World War II; and stealth, unmanned vehicles, and precision-guided munitions in recent decades. These developments potentially pale in comparison to the potential impact of the rapid and advancing progress in artificial intelligence (AI). Dominated by developments in the commercial industry, the past several years have seen dramatic advances in which machines complete complex tasks and match or exceed human performance.

This development has been noticed by other countries just as the US recognizes it is operating in a new strategic environment of great power competition. Both China and Russia view AI as ways to counter US military strength, and strong national Research and Development (R&D) efforts are a key component of these efforts. This places increased importance on US R&D efforts regarding AI to maintain competitiveness and promote national security.

This fall, the US government is revising its AI R&D strategy, originally written in 2016. This is an opportunity to help the US to sharpen and strengthen its own AI efforts in this competitive and strategic environment. As the US refines this strategy, CNA and its Center for Autonomy and AI offers some areas of potential improvement from the original 2016 strategy that should be addressed in the new version. These areas are: defining the nature of the relationship between industry/academia and government; fast-tracking R&D to applications; working with allies; and ethical, legal, and societal implications of AI.

Defining the nature of the industry/academia relationship with government. For AI, the relationship between government and industry is fundamentally different than it has been in the past. The new reality for AI is that, for the underlying technology, commercial research and development (R&D) efforts will dwarf that of the US government. The US must now rely on developments in the commercial sector as well as its own R&D programs. How does this affect the specific nature of the relationship between government and industry? Should the US government abandon its typical first mover approach and take on a fast follower approach? How should the US prioritize resources and research areas in that new framework? How can it identify and quickly bring on key technologies from industry for its own development and use?

A complicating factor for this relationship is the effect of ethical concerns companies may have regarding supporting national security and defense applications. The recent concerns over Google's support to Project Maven – which applied AI to image classification in full motion video from military drones – highlights how the US may be more challenged in working with

industry than will rival nations such as Russia and China. This is also complicated by the increasing multinational nature of industry, and including corporate concerns about reduced profitability in foreign markets from greater cooperation with the US government. What are some approaches the US can take to promote cooperation in this complex environment?

Operationalizing R&D: moving research to applications. With AI, the majority of R&D is in commercial development, and much of this development will be equally exploitable by many states—and by non-state actors for that matter. This means that the ability to quickly identify developments and integrate them into US capabilities will be critical in this new, rapidly evolving technological environment. This creates challenges for a US military characterized by a slow and deliberate acquisition process. What are some best practices for successfully fielding innovation? What are the requirements necessary for such applications to be effective in the context of US government applications? This includes steps that can be done up front to make research operationalizable as well as including research on how to more rapidly transition basic research to sustainable applications.

Working with allies. Much has been said regarding the emergence of a new AI arms race with China and Russia. Russia has discussed AI as "kryptonite" to foil US military strength while China aims to be the AI world leader by 2030 and to apply that expertise for national security purposes. The US faces some structural and policy challenges relative to those two countries that can by fiat significantly leverage their commercial R&D efforts in AI. But there is one advantage the US enjoys over those two rivals: close allies. Ranging from NATO to its close 5-eyes alliance (US-UK-CAN-AUS-NZ) to other close relationships with like-minded countries, the US can benefit from the collective efforts of these allies. How can the US benefit from AI R&D efforts by allies for mutual benefit?

Ethical, legal, and societal implications of AI. Significant advances in artificial intelligence (AI) over the past decade have changed our way of life and carry a number of benefits. At the same time, the idea of adapting AI to government and military applications has created considerable controversy. There are strong concerns about these technologies, including privacy, safety, and bias, and even speculation that they could lead to the end of the world. Some of these commonly held concerns about AI and autonomy in war, as reported in the media or voiced in international venues, are either out of step with the current state of the technology, or they do not consider the way government and military systems are actually used. These concerns have broad impact, ranging from industry willingness to partner with the government, public support for government initiatives, and the development of international norms and laws that can affect the US. Thus the AI R&D strategy should include a component where these concerns are addressed through dialogue and communication among the government, industry, academia, and the public.

Summary. The revisit of the 2016 US AI R&D strategy is a wise decision to take an iterative approach, building upon the past strategy but looking for ways to improve and refine the overall US approach. This is particularly critical for AI in view of it being a rapidly advancing

technology that is likely to be decisive in national security in the coming decades. Based on insights from the CNA Center for Autonomy and AI's body of work, the above recommendations for the revised strategy are offered as ways to help the US to sharpen and strengthen its own AI efforts in this competitive and strategic environment.