The Institute for Foreign Policy Analysis

National Security Update

The Military Applications and Use of Artificial Intelligence

This *IFPA National Security Update* examines artificial intelligence (AI),with a focus on its status, military applications, benefits, and shortcomings; competition with China and Russia to develop AI technologies; the Trump Administration's AI Executive Order; and the need for the United States government to develop strategies and acquisition approaches to harness/leverage more effectively the AI innovations and applications being developed primarily in the U.S. commercial sector.

Key Conclusions and Findings

- Artificial intelligence is a transformative technology. Just as electricity transformed our economy and society, AI will have far reaching implications. AI will be incorporated into a range of devices resulting in smarter, more sophisticated and "cognified" systems. Unlike traditional software which only supports human reasoning, AI draws conclusions from its own experience. The increasing transfer of judgment from humans to machines represents the revolutionary nature of AI.
- AI can be incorporated into most U.S. military systems – intelligence collection and analysis assets, cyberspace systems, command and control, aircraft, ships, submarines, and autonomous vehicles to name only a few. Systems/weapon platforms infused with AI will increase their effectiveness, significantly bolstering the defense capabilities of the United States. AI-embedded systems will:
    - Enable more informed judgments by decision makers facilitating more rapid action/response times;
    - Heighten the capabilities of soldiers by increasing their productivity as these systems assume greater responsibility for routine tasks;
    - Provide faster reaction times and other capabilities to help counter new threats such as hypersonic weapons being developed by Russia and China, directed energy systems, and large-scale cyberattacks;
    - Enable control of networked fleets of AI systems programmed to complete coordinated tasks with minimum human involvement; and,
    - In certain cases, render some weapons platforms of an adversary ineffective or perhaps obsolete by providing less expensive military systems with increased capability.
- However, several AI issues/concerns need to be addressed and resolved. AI applications still have many bugs to be worked out that could result in unpredictable and serious failures, particularly when encountering tasks or situations for which the AI systems were

not trained; AI systems could be susceptible to manipulation and hacking; and, some AI systems cannot explain or provide the details about how they arrived at a solution.

  - The potential for lack of explainability/understanding about why/how an AI system derived a solution presents a problem regarding human control, confidence, and trust in certain AI applications. Consequently, having humans in the loop, making final decisions is a decision-making prerequisite when any AI system is being utilized. This is especially crucial in decisions/actions involving nuclear weapons.

- The United States is in an artificial-intelligence arms race with Russia but especially with China. China has identified AI as a strategic technology for national security and economic prosperity: Beijing's goal is to be the world leader in AI innovation by 2030. China is investing considerable venture capital in U.S. AI start-up companies, causing concern within the U.S. government (USG) about safeguarding the intellectual property and technology of U.S. high-tech firms.

- The Trump Administration issued an AI Executive Order in February 2019 that underscores the critical importance of maintaining U.S. preeminence in artificial intelligence for U.S. national security and economic well-being. The Executive Order calls for increased coordination in AI research and development (R&D) across USG departments and agencies including within the Department of Defense (DOD).

  - The Executive Order also calls for greater collaboration between the USG and the commercial sector where the majority of AI investment, research, innovation, and development occurs. It highlights the critical link between AI and big data and the need to increase access to USG data together with the need to safeguard U.S. technology from theft by foreign powers and to protect AI systems from disruption by cyberattacks.

- DOD must increase funding for AI R&D and applications as well as address the potential problems attending AI usage, i.e., the predictability and explainability concerns cited above. Another top priority of the Department of Defense should be to access and leverage the U.S. commercial sector AI developments. DOD needs to develop strategies and pathways designed to support greater and more effective collaboration with the commercial sector and develop increased public-private partnerships.

  - This effort should include changes to the DOD procurement process to ease/minimize cumbersome regulations and requirements that discourage and impede many commercial high-tech companies from bidding on DOD R&D and procurement opportunities.

- Implementation of the Administration's EO will require sustained leadership and commitment from the White House and the cooperation of Congress to maintain the U.S. lead in artificial intelligence.

- Congress needs to maintain funding support for legislation to ensure U.S. leadership in artificial intelligence, support the Administration's AI Executive Order by authorizing/appropriating additional AI funding, and push for/legislate DOD acquisition reform that encourages and facilitates collaboration with the U.S. AI commercial sector and makes it easier for commercial companies to work with the Defense Department.

Introduction

We have entered a "fourth industrial revolution,"[i] characterized by fast-paced and converging advancements in artificial intelligence, robotics, the Internet of Things, quantum computing, nanotechnology, biotechnology, and 3D fabrication and other technologies. In particular, artificial intelligence is a critical and rapidly growing field of technological development that holds major military/national security and economic implications.

AI will likely be the centerpiece, the most transformative technology of the fourth industrial revolution. For example, AI makes it possible to automate a wide range of tasks by enabling machines to play an increasingly important and decisive role in drawing conclusions from data and then taking action. Unlike traditional software which only supports human reasoning, AI draws conclusions from its own experience. The increasing transfer of judgment from humans to machines represents the revolutionary nature of AI.

Since the start of this decade, a breakthrough in machine learning – a method of AI engineering – has enabled the development of increasingly capable AI applications. For example, AI experts have compared the transformative potential of AI to that of electricity noting that just as most everything became more useful when it was "electrified," most everything will have greater utility when it is "cognified."[ii]

This suggests that any type of military system/device equipped with AI software, whether it be conventional, cyber, or nuclear, would be able to handle larger volumes of data more efficiently and become smarter and more capable. It is therefore not surprising that in the military/national security realm, advances in AI have produced countless expectations: many defense officials believe that AI holds the potential to revolutionize military strategy, decision making, and operations. In fact, the Department of Defense is developing and beginning to field AI applications in a wide range of its activities.

Growing DOD R&D funding to develop advanced AI applications is expected to drive the increased adoption of AI-driven military systems in the military sector. AI technology and applications have the potential to expedite autonomous operations, allow improved and speedier decision making, and thus increase both the pace and scale of military action, providing an unambiguous military advantage.

For example, AI military research is taking place in intelligence collection and analysis, surveillance, reconnaissance and target recognition, cyberspace functions, battle management and command and control, autonomous vehicles, training and simulations, logistics, and transportation, to name only a few areas where AI applications are being explored. AI tools can be applied to relatively mundane and human-intensive tasks such as computer vision and data analysis. Today, AI applications as part of Project Maven (more below) are being used in Iraq and Syria in U.S. military operations to accelerate the identification of Islamic State (ISIS) targets.

The use of AI, however, presents several potential pitfalls and associated uncertainties. Military AI systems have a number of limitations and concerns from an operational, strategic, legal, and/or ethical perspective. For example, AI can be susceptible to manipulation and hacking, and pose challenges to human-machine interaction. A main concern is that the military might misjudge or even ignore the limitations of current AI technology. Although AI-powered

applications can accomplish considerable undertakings they remain somewhat fragile or brittle in their design and consequently could falter dramatically when facing tasks or operating environments that are different from those for which they were trained.

Moreover, as will be discussed in greater detail later in this *Update*, the workings of AI systems can be unpredictable; in many of the more advanced AI systems a cause for concern is that they are unable to explain or demonstrate how a particular solution was derived. This presents a potential serious issue regarding the understanding and control of AI applications.

An important issue that could hamper DOD's development and fielding of AI-infused tools is that, unlike the development of most previous revolutionary military technologies, the lion's share of AI R&D and applications is taking place not in the defense sector but in the commercial and academic sectors. This has major implications regarding how effectively the bureaucratically and culturally hidebound DOD procurement system can tap into and access the AI innovations in the commercial sector.

This becomes particularly important because both China and Russia have made the development of AI a major military priority. In fact, China has singled out AI as a strategic technology with the objective of becoming the world's preeminent trailblazer in AI innovation by the end of the next decade. Russian President Vladimir Putin has declared that whoever becomes the leader in AI development "will be the ruler of the world."[iii]

What is Artificial Intelligence?

The term "artificial intelligence" was coined in 1955 by John McCarthy, a computer scientist, to describe the focus of a proposed workshop on computers as thinking machines. To this day, however, no commonly accepted definition of AI exists within either the commercial/academic- or the U.S. government (USG)-AI communities. In part, this is because of the diverse approaches to research in the field of AI. For the purposes of this *Update*, the definition advanced by two companion bills passed by the Senate and House of Representatives in December 2017 is used.

In these bills, AI is defined as "Any artificial system that performs tasks under varying and unpredictable circumstances, without significant human oversight, or that can learn from their experience and improve their performance. Such systems may be developed in computer software, physical hardware, or other contexts not yet contemplated. They may solve tasks requiring human-like perception, cognition, planning, learning, communication, or physical action."[iv]

The mid-1950s saw the beginning of research in artificial intelligence. However, AI research exploded at the beginning of this decade because of the confluence of three factors: the availability of sources of big data; advances in machine learning; and the rapid growth in the processing power of computers and development of AI algorithms.[v] This surge in AI-R&D advanced the capabilities of what is called Narrow AI (NAI) which addresses problems such as image recognition and self-driving vehicles. The majority of present-day AI techniques are considered NAI.

A key component of NAI is machine learning involving algorithms which replicate human cognitive tasks that "learn" by evaluating large training data sets to accomplish tasks it has not

previously encountered. As will be described in greater detail later in this *Update*, the availability of voluminous data sets is critical to the development of AI capabilities.

The next stage beyond NAI is called General AI or GAI. GAI refers to AI systems that are capable of human-level intelligence spanning an extensive range of undertakings and tasks. However, experts are largely in agreement that it will be several decades before GAI capabilities are achieved. That said, the burgeoning capabilities of NAI have occasioned a surge of investments by the U.S. commercial sector with funding in 2016 estimated at approximately $30 billion; according to some projections total AI commercial investment could approach $126 billion by 2025.

In stark contrast, the unclassified funding for AI by the Defense Department was a mere $600 million in 2016. Underscoring the growing realization of the importance of AI for military operations, however, is the fact that in Fiscal Year 2017 DOD allocated $7.4 billion to AI-related efforts including AI applications, big data research, and cloud computing.[vi]

Also indicative of the growing military priority of AI, on June 27, 2018 the Defense Department created the Joint Artificial Intelligence Center (JAIC). Designed to be DOD's AI Center of Excellence, the JAIC will have primary oversight of practically all high-budget AI efforts in both the military services and DOD agencies. The goal of the JAIC is to establish a common set of AI standards, tools, shared data, reusable technology, processes, and expertise to be made available throughout the entire Defense Department.[vii] The JAIC is the focal point for carrying out the Department of Defense Artificial Intelligence Strategy,[viii] published in February 2019, shortly after President Trump released his AI Executive Order.

Several other distinctive features of AI should be considered as AI applications become more prevalent in the military/national security field. These include the fact that AI technology holds the potential to be integrated into numerous objects; many AI applications are dual-use with both military and civil/commercial uses; and, AI applications will eventually be infused into nearly everything humans do.

AI Acquisition Issues

From the Cold War era until recently, the majority of key defense-related technologies and systems, e.g., nuclear technology, precision weapons, space systems such as the Global Positioning System (GPS), and the Internet, were traditionally developed by the USG/DOD which later migrated to the commercial sector. In contrast, today civilian companies are leading AI development, with DOD adapting their tools after the fact for national security functions.

A CRS Report states that to facilitate AI procurements for military purposes, it may be necessary to adapt or modify the Defense Acquisition Process. DOD will also have to adapt and modify many commercial AI applications before they can be utilized for military operations. Moreover, several cultural issues will complicate AI commercial acquisitions, "leading to discord with AI companies and potential military aversion to adapting weapons systems and processes to this disruptive technology."[ix]

The aforementioned Project Maven is a case in point where discord arose between a commercial AI company and DOD. Google, which was supplying AI tools to the Defense

Department for the rapid analysis of large volumes of drone video, decided not to extend this contract because its employees were opposed to working with DOD on ethical grounds. Google's action called into question DOD's ability to build a strong relationship with Silicon Valley to access advanced technologies such as AI.[x]

International Competition: An AI Arms Race

As the use of AI for defense functions continues to expand in scope and complexity and the military utility of AI has become clearer, USG officials in the Executive Branch, DOD, the intelligence community, members of Congress, and the broader defense community have become increasingly concerned about the international competition in artificial intelligence. A particular concern is that the United States may be falling behind key competitors, particularly China, but also Russia with serious negative consequences for U.S. national and economic security.

For example, in the 2018 *Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community*, Daniel Coates, then-Director of National Intelligence, states that "The widespread proliferation of artificial intelligence (AI) – the field of computer science encompassing systems that seek to imitate aspects of human cognition by learning and making decisions based on accumulated knowledge – is likely to prompt new national security concerns;"[xi] A number of analysts, including Robert Work, former Deputy Secretary of Defense in the Obama and Trump Administrations, have described the rapidity of AI development as a potential "Sputnik Moment" that could ignite a global AI arms race.[xii]

China's AI Goal: World Leader by 2030

As indicated above, China is far and away the most serious competitor to the United States in the AI arena. Two documents, *Next Generation AI Development Plan* released in July 2017 by China's State Council and the 2015 *Made in China 2025*,[xiii] form the foundation of Beijing's AI strategy. Spelling out in greater detail China's plan for AI first outlined in *Made in China 2025,* the *Next Generation* document states that "AI has become a new focus of international competition. AI is a strategic technology that will lead in the future; the world's major developed countries are taking the development of AI as a major strategy to enhance national competitiveness and protect national security."[xiv]

The document sets forth a three-step plan:

1. To keep pace with the leading global AI technologies and applications by 2020;
2. To achieve AI breakthroughs by 2025; and,
3. To be the world leader in artificial intelligence by 2030.

China's development of military AI applications is based largely on the belief that increased military usage of AI is inevitable and therefore must be pursued aggressively, together with a fear that U.S. AI capabilities could outstrip those of China producing a widening technological and operations gap favoring the United States.

Chinese AI development focuses on AI tools to enhance battlefield decision-making by exploiting a large volume of collected intelligence data to deliver a complete picture of the battlespace and to recommend to decision makers the appropriate military

actions/responses.[xv] It has also been reported that Beijing is conducting AI research on cyber-defense and attack options.[xvi]

Unlike in the United States, there are few boundaries or cultural roadblocks extant in China that prevent collaboration between China's commercial companies, academic research labs, and China's military and central government. To illustrate, in 2017 the Military-Civil Fusion Development Commission was created by the government with the goal of accelerating the transfer of AI technology and systems from Chinese commercial firms and academic research institutions to the Chinese military.

This unified, near-seamless AI effort in China allows the government the means to guide/dictate AI development priorities and funding. China is also leveraging its collection of large data bases accumulated by both the commercial sector and the government. Access to such data bases is essential for machine learning, training AI systems, and other advances in NAI. It is projected that China will possess 20% of the global share of data in 2020 and capture more than 30% by 2030.[xvii] As will be discussed in greater detail below, the United States is taking steps to access more effectively USG-generated data to enhance AI learning and capabilities.

Not surprisingly given the objectives set forth in the *Next Generation AI Development Plan* and *Made in China 2025* documents cited above, Beijing has pushed Chinese companies to invest in American start-ups to access technologies such as AI and robotics to augment the military capabilities of China as well as to boost its economy. For example, between 2010 and 2017 Chinese venture capital investments in U.S. AI companies totaled approximately $1.3 billion.[xviii]

The Defense Department is concerned by Chinese investments in U.S. high-tech firms, stating in a White Paper that USG controls designed to safeguard critical technologies such as AI are falling short. Specifically, Chinese investors could press U.S. AI start-ups to establish partnerships, make licensing or hiring decisions allowing China access to the start-up's intellectual property, computers, and technology being developed.[xix] Another major U.S. concern is China's long record of effective industrial espionage resulting in the unlawful transfer of pilfered U.S. AI technology to Beijing.

The Trump Administration and lawmakers have been raising numerous concerns about China's economic relationship with the United States. Several Executive Branch and members of Congress have called for tighter regulation of foreign takeovers by China by giving a broader mandate to the Committee on Foreign Investment in the United States.

President Trump has also banned the sale of U.S. technology to the Chinese tech giant Huawei whose goal is to become the global leader in the development of the 5G-Internet network. President Trump has also tried to persuade other nations not to purchase Huawei technology and its 5G-infrastructure products. Administration officials believe that Huawei is "a Trojan Horse for Beijing's cyberspies."[xx]

Russian AI Efforts and Capabilities

Russia also represents a serious rival to the United States in the competition for military AI applications, albeit to a lesser extent than China. Even though Russian AI investments currently trail those of both the United States and China, Moscow is taking several steps to address this

gap. Russia's military is researching and developing a number of defense applications for AI, with a heavy emphasis on autonomous vehicles and robotics, two areas that require AI applications to be successful.

In 2016, Russia established the Foundation for Advanced Studies, a defense research organization focusing on autonomy and robotics. Russia's goal is to have 30% of its military equipment to be robotic by 2025.[xxi]

Despite Russia's ambitious AI goals, however, it could be hard for Russia to allocate substantial funding for such efforts. The Russian economy is not as strong as those of the United States and China and it is almost totally dependent on oil exports. For example, although the price of oil has rebounded somewhat from its lows of about $27/barrel in the 2015-2016 timeframe to approximately $56/barrel in mid-August 2019,[xxii] Russia has had to slow the pace of its defense spending over the past several years, even though it still likely remains the third highest defense spender behind the United States and China.

In comparison with global trends, the Russian private sector is only slowly beginning to focus on AI and machine learning. In Russia, universities and scientific research institutes produce the bulk of AI-related research and applications. AI research is primarily driven/funded by the state and state-owned businesses. As a rule, AI applications developed by Russian startups are deemed inferior to those produced by similar U.S. and Chinese start-ups. This may change, however, given Russia's pool of qualified specialists for AI projects with over 200,000 individuals trained in data analysis, machine learning, speech and image recognition, computer linguistics, and related fields over the past five years.[xxiii]

The AI Executive Order released by the Trump Administration, and discussed in an upcoming section, addresses several of the issues related to international competition, especially with China.

AI in Military Operations: Opportunities and Challenges

AI features incorporated for use in the defense/national security realm present several clear-cut opportunities and specific challenges that differ from current military systems. Such AI features include: autonomy, speed, scaling, information dominance, predictability, and explainability.

AI is the Path to Autonomy

The dominant driver and approach to achieve autonomy and autonomous systems is artificial intelligence. Autonomy was the principal objective of the Third Offset Strategy spearheaded during the Obama Administration by former Under Secretary of Defense Robert Work to maintain the technological advantage of the U.S. military. Autonomous systems would be able to augment and, as the technology progresses, eventually replace humans, thus liberating them to perform more complicated, demanding tasks.

Examples of autonomous systems include those able to conduct long-duration intelligence collection and analysis, robotic systems that clean up environments contaminated by chemical weapons, and unmanned systems that sweep a route for improvised explosive devices. By performing such labor-intensive tasks, the autonomous systems would significantly reduce costs, mitigate risks to warfighters, and free up personnel to carry out other activities. However, autonomous systems do not mean that humans will be "out-of-the-loop." DOD

requirements maintain that people will be monitoring and making all final decisions regarding solutions produced by AI/autonomous systems.

The Key to Military Success: Speed

AI offers the opportunity to accomplish tasks more rapidly providing an unequivocal advantage in military operations. For example, in the missile defense mission, AI could help provide the quick reaction times (less than 180 seconds in most cases) needed to identify, track, target, destroy, and provide kill assessment of a ballistic missile in the boost phase of flight. Systems outfitted with AI technologies will be able to react rapidly increasing the overall pace of combat, particularly if AI is widely embedded in other military systems.

The reaction times supplied by such systems would also help counter new threats such as the hypersonic weapons being developed by Russia and China, directed energy systems, and large-scale cyberattacks. AI systems could enable decision makers to make informed judgments more rapidly by providing the capability to analyze and integrate copious amounts of data facilitating far quicker action/response times than those offered by existing battle management and command and control devices. As a result, speedier reaction times fueled by AI systems could overwhelm the ability of an adversary to understand the environment and respond accordingly, particularly if the adversary is relying exclusively on human judgment.

Obviously, and as will be discussed in more detail below, the dramatic increases in decision-making speed for combat operations have potential downsides. It could conceivably result in an operating environment where AI-infused systems are working at such rapid rates that they undermine a human's capability to comprehend or control events.

Scaling AI Systems in the Defense Enterprise

Systems equipped with AI tools offer the potential to provide both force-multiplying and cost-saving scaling impacts as they are extensively scaled, i.e., deployed throughout the DOD enterprise. AI-infused systems will heighten the capabilities of soldiers by increasing their productivity as these systems assume responsibility for routine tasks. AI devices will also enable control of networked fleets of AI systems programmed to complete a coordinated task with a minimum of human involvement.

AI applications may also render some current weapons platforms ineffective or perhaps obsolete by infusing less expensive military systems with increased capability. For example, hundreds of low-cost, interconnected and swarming drones equipped with AI software may be able to overcome a much more expensive, high-value system such as a Russian or Chinese advanced fighter aircraft providing a significant cost-saving advantage.

Information Superiority: Winning the War with Faster/Higher Quality Data Analysis

AI-infused tools and devices promise superior analysis of the expansive volume of collected data now available. It has been reported that each one of the approximate 11,000 drones DOD flies records high-definition footage every day equivalent to over three seasons of NFL football (i.e., at least 768 games). DOD does not have enough personnel nor currently field the requisite computational/analytical devices necessary to sort through this massive trove of data to provide decision makers with accurate, timely, and implementable intelligence.[xxiv] Given that the volume of data available will only continue to grow, in part because of a proliferation of

data-gathering sensors and other collection devices, the problem of bulk data analysis will likely worsen.

However, the fielding of AI-equipped intelligence systems portends considerable improvements in intelligence analysis. They will be capable of scrutinizing vast volumes of data gleaned from different sources to identify the most useful information. AI-infused intelligence systems hold the promise of providing a higher quality of information resulting in superior and speedier wartime decision-making.

The Predictability of AI Outputs

AI systems have often produced unpredictable results causing concern about their application in military systems. Dr. Arati Prabhakar, a former Director of the Defense Advanced Research Projects Agency (DARPA), stated that "When we look at what's happening with AI, we see something that is very powerful, but we also see a technology that is still quite fundamentally limited."

Image analysis highlights some of the current limitations of AI. Although AI systems are better statistically than humans at correctly identifying images because they can scan thousands of images in seconds, Prabhakar stated that "the problem is that when they're wrong, they are wrong in ways that no human would ever be wrong." Prabhakar highlighted one case where an AI system identified a picture of a baby holding a toothbrush as a baby with a baseball bat. Prabhakar went on to state that "this is a critically important caution about where and how we would use this generation of artificial intelligence."[xxv]

Prabhakar's warnings about such unpredictable AI inaccuracies could produce major risks if the systems are fielded at scale. Normally, human mistakes are made on an individual basis and are usually different in each circumstance. However, given their programming, AI systems have the potential to fail both simultaneously and in the same way every time.

If DOD fields AI-infused devices before gaining a thorough understanding of their random, unpredictable occurrences, it may incur what is called a "technical debt," i.e., deployed AI systems would have negligible risk individually but that risks/dangers become significantly compounded by the fielding of every additional new AI system.[xxvi]

Explainability: Understanding How AI Systems Derive Solutions

Explainable AI will be critical if decision makers are to understand, trust, and manage AI systems. Explainability creates concerns in the military realm because the "unexplainability" of AI reasoning/solutions may engender either too-great or too-little levels of confidence in an AI system's output.

Given this uncertainty, it is reasonable to expect that decision makers may be reluctant to base their choices solely on AI-derived analysis they do not understand. The key to creating necessary trust levels in AI-infused systems is to augment explainability. Having humans in the loop to make final decisions is a decision-making prerequisite when any AI system is being utilized. This is especially crucial in decisions/actions involving the use of nuclear weapons.

The twin concerns of explainability and predictability challenge the ability to test and confirm the performance of an AI system prior to deployment, a process through which all DOD systems must successfully pass. While established DOD verification and validation procedures assume

tested performance will reveal a system's future behavior, the majority of AI systems demonstrate so-called "emergent behavior," meaning that AI software will adjust when it encounters new stimuli.

The ability of an AI system to adjust to a complex environment would normally be considered a positive feature of a military system. However, in the case of AI systems, it bumps up against present DOD guidance requiring that autonomous and semi-autonomous systems must undergo a thorough verification/validation process to guarantee that the system will perform as anticipated in realistic operational environments against adversaries able to adapt. It is highly impractical, however, to believe that the military can envision the range of possible realistic operational environments or adversary reactions that an AI system might encounter.

To address the explainability problem, DARPA is conducting a five-year research effort to manufacture explainable AI tools, and other research organizations are attempting to analyze AI software/algorithms to garner a clearer picture of how they function.[xxvii] DOD is also developing a methodology to investigate AI system lifecycles and test AI systems in varied environments with complex human-machine interactions.[xxviii]

The Trump Administration's Executive Order on Artificial Intelligence

On February 11, 2019, the White House took concrete steps to address many of the AI issues/concerns cited above when it issued the *Executive Order on Maintaining American Leadership in Artificial Intelligence*. The Executive Order (EO) underscores the fact that "Continued American leadership in AI is of paramount importance to maintaining the economic and national security of the United States and to shaping the global evolution of AI in a manner consistent with our Nation's values, policies, and priorities." It makes AI a priority for all federal departments and agencies and establishes a comprehensive, whole-of-government framework for the Executive Branch to implement the Administration's AI policy.[xxix]

The EO sets forth several key provisions. It emphasizes the need for increased coordination in AI R&D and funding across the USG departments and agencies and within the DOD and military services. Importantly, the EO directs USG AI R&D agencies to "explore opportunities for collaboration with … the private sector; academia; non-profit organizations,"[xxx] where the majority of AI funding, innovation, development, and applications is taking place.

The EO also addresses the critical link between AI and data and the understanding that AI software/algorithms "learn" by access to data: the more data available the more learning can occur. A key strategic objective of the EO is to "Enhance access to high-quality and fully traceable Federal data, models, and computing resources to increase the value of such resources for AI R&D, while maintaining safety, security, privacy, and confidentiality protections consistent with applicable laws and policies."

The United States must keep pace with our competitors in the AI/data collection race, particularly China, which as noted earlier, has in place an intensive – and in many cases repressive – data-collection program focusing on the activities of its large population together with its theft of data from other nations. Consequently, the AI EO is correct to urge USG departments/agencies to make more of their data available to AI developers within the United States.

In addition, the EO states that "protecting our critical AI technologies from acquisition by strategic competitors and adversarial nations… is essential for the long-term national security and economic well-being of the United States." It also addresses the need to safeguard the integrity of AI technology from a physical and cybersecurity attacks and disruptions to ensure that AI systems work as intended.[xxxi]

The EO does not establish a specific figure for AI funding but instead instructs federal agencies to prioritize AI-related spending and develop funding requests for the Office of Management and Budget for future fiscal years. Given that the Administration can only request funding for programs such as AI, it must work with Capitol Hill to authorize/appropriate substantial AI funding. Implementation of the AI EO will require sustained leadership and commitment from the White House and the cooperation of Congress to maintain the U.S. lead in artificial intelligence.

Conclusions

Artificial intelligence is a transformative technology. Just as electricity transformed our economy and society, AI will have far reaching implications. Unlike traditional software which only supports human reasoning, AI draws conclusions from its own experience. The increasing transfer of judgment from humans to machines represents the revolutionary nature of AI. AI will be incorporated into multiple devices resulting in smarter, more sophisticated, and "cognified" systems.

AI can be incorporated into most U.S. military systems including intelligence collection and analysis assets, cyberspace systems, command and control networks, aircraft, ships, submarines, and autonomous vehicles to list but a few. Systems/weapon platforms infused with AI will increase their effectiveness, significantly bolstering the defense capabilities of the United States. AI-embedded systems will:

- Enable more informed judgments by decision makers facilitating speedier action/response times;
- Heighten the capabilities of soldiers by increasing their productivity as these systems assume greater responsibility for routine tasks;
- Provide faster reaction times and other capabilities to help counter new threats such as hypersonic weapons being developed by Russia and China, directed energy systems, and large-scale cyberattacks;
- Enable control of networked fleets of AI systems programmed to complete coordinated tasks with minimum human involvement; and
- In certain cases, render some weapons platforms of an adversary ineffective or perhaps obsolete by equipping less expensive military systems with increased capability.

However, several AI issues/concerns need to be addressed and resolved. AI applications still have many bugs to be worked out that could result in unpredictable and serious failures, particularly when encountering tasks or situations for which the AI systems were not trained. AI systems could also be susceptible to manipulation and hacking by adversaries. Another

problem is the fact that some AI systems cannot explain or provide the details about how they arrived at a solution.

The potential for lack of explainability/understanding about why/how an AI system derived a solution presents a problem regarding human control, confidence, and trust in certain AI applications. Consequently, having humans in the loop, making final decisions is a decision-making prerequisite when any AI system is being utilized. This is especially crucial in any decision/actions involving nuclear weapons.

The United States is in an artificial-intelligence arms race with China and Russia, but especially with China. China has identified AI as a strategic technology for national security and economic prosperity: Beijing's goal is to be the world leader in AI innovation by 2030. Toward this end, China has established a direct, near-seamless relationship with its commercial AI companies, academia, and the military establishment to develop AI. China is also investing considerable venture capital in U.S. AI start-up companies, causing concern within the USG about safeguarding the intellectual property and technology of U.S. high-tech firms.

The Trump Administration issued an AI Executive Order in February 2019 stating that the United States must undertake a concerted national effort to maintain preeminence in artificial intelligence for U.S. national security and economic well-being. It calls for increased coordination in AI R&D across USG departments and agencies including within DOD, and importantly, greater collaboration between the USG/DOD and the commercial and academic sectors where the majority of AI investment, research, innovation, and development occurs.

It also highlights the critical link between AI and big data and the need to increase access to USG data, safeguard U.S. technology from theft by foreign powers, and protect AI systems from disruption by cyberattacks.

For its part, DOD must increase funding for AI R&D and applications as well as address the potential problems attending AI usage, especially the predictability and explainability issues/concerns discussed earlier. Another key priority of the Department of Defense should be to access and leverage the range of AI developments happening in the U.S. commercial sector. DOD needs to develop strategies and pathways designed to support more effective collaboration with the commercial sector and deepen public-private AI partnerships.

This effort should include changes to the DOD procurement process to ease/minimize the cumbersome regulations and requirements that discourage and impede many commercial high-tech companies from bidding on DOD R&D and procurement opportunities.

Finally, implementation of the Administration's EO will require sustained leadership and commitment from the White House and the cooperation of Congress. Congress needs to maintain funding support for legislation to ensure U.S. leadership in artificial intelligence, support the Administration's AI Executive Order by authorizing/appropriating additional AI funding, particularly for the Department of Defense, and push for/legislate DOD acquisition reform that encourages and facilitates collaboration with the U.S. AI commercial sector and makes it easier for commercial companies to work with the Defense Department.

Endnotes

[i] Devon McGinnis, "What Is the Fourth Industrial Revolution?" *Salesforce (blog)*, December 20, 2018 at https://www.salesforce.com/blog/2018/12/what-is-the-fourth-industrial-revolution-4IR.html.
[ii] "The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk," Volume I, edited by Vincent Boulanin, SIPRI, May 2019, p. 3. See https://www.sipri.org/sites/default/files/2019-05/sipri1905-ai-strategic-stability-nuclear-risk.pdf.
[iii] "Putin: Leader in artificial intelligence will rule world," CNBC, September 4, 2017. See https://www.cnbc.com/2017/09/04/putin-leader-in-artificial-intelligence-will-rule-world.html.
[iv] "H.R.4625 - Future of Artificial Intelligence Act of 2017," December 2017, pp 3-4 and "S.2217 – Future of Artificial Intelligence Act of 2017," December 2017, pp 3-4. See https://www.congress.gov/115/bills/hr4625/BILLS-115hr4625ih.pdf and https://www.congress.gov/115/bills/s2217/BILLS-115s2217is.pdf, respectively.
[v] Big data can be defined as large sets of data analyzed computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions. Machine learning is a branch of artificial intelligence that has been defined as an approach to data analysis that automates analytical model building and is based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention. Algorithms are a specific set of software to perform a specific function – essentially the brains of AI.
[vi] Tejaswi Singh and Amit Gulhane, "8 Key Military Applications for Artificial Intelligence in 2018," *Market Research* (blog), October 3, 2018. See https://blog.marketresearch.com/8-key-military-applications-for-artificial-intelligence-in-2018.
[vii] "Establishment of the Joint Artificial Intelligence Center," DOD Memorandum by Deputy Secretary of Defense Patrick Shanahan, June 27, 2018. See https://admin.govexec.com/media/establishment_of_the_joint_artificial_intelligence_center_osd008412-18_r....pdf.
[viii] "Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity," Department of Defense, February 2019. See https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.
[ix] Daniel S. Hoadley and Nathan J. Lucas, "Artificial Intelligence and National Security," CRS Report, April 26, 2018. See https://www.a51.nl/sites/default/files/pdf/R45178.pdf.
[x] Drew Harwell, "Google to drop Pentagon AI contract after employee objections to the 'business of war'," *Washington Post*, June 1, 2018. See https://www.washingtonpost.com/news/the-switch/wp/2018/06/01/google-to-drop-pentagon-ai-contract-after-employees-called-it-the-business-of-war/.
[xi] Daniel R. Coats, Director of National Intelligence, *Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community*, p. 12, February 13, 2018. See https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.
[xii] Tom Simonite, "For Superpowers, Artificial Intelligence Fuels New Global Arms Race," *Wired*, September 8, 2017, and Colin Clark, "Our Artificial Intelligence 'Sputnik Moment' is Now: Eric Schmidt & Bob Work," *Breaking Defense,* November 1, 2017. See https://www.wired.com/story/for-superpowers-artificial-intelligence-fuels-new-global-arms-race/ and https://breakingdefense.com/2017/11/our-artificial-intelligence-sputnik-moment-is-now-eric-schmidt-bob-work/, respectively.
[xiii] China State Council, "Made in China 2025," July 7, 2015. See http://www.cittadellascienza.it/cina/wp-content/uploads/2017/02/IoT-ONE-Made-in-China-2025.pdf.
[xiv] "Full Translation: China's 'New Generation Artificial Intelligence Development Plan,'" New America, August 1, 2017. See https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.
[xv] Elsa B. Kania, "Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power," Center for a New American Security, November 2017. See

https://s3.amazonaws.com/files.cnas.org/documents/Battlefield-Singularity-November-2017.pdf?mtime=20171129235805.

[xvi] Ibid.

[xvii] Ibid.

[xviii] Daniel S. Hoadley and Nathan J. Lucas, "Artificial Intelligence and National Security," CRS Report.

[xix] Paul Mozur and Jane Perlez, "China Bets on Sensitive U.S. Start-Ups, Worrying the Pentagon," *The New York Times*, March 22, 2017. See https://www.nytimes.com/2017/03/22/technology/china-defense-start-ups.html.

[xx] David Sanger, "Trump Wants to Wall Off Huawei, but the Digital World Bridles at Barriers," *New York Times*, May 27, 2019. See https://www.nytimes.com/2019/05/27/us/politics/us-huawei-berlin-wall.html.

[xxi] Tom Simonite, "For Superpowers, Artificial Intelligence Fuels New Global Arms Race."

[xxii] "WTI Crude Oil Prices - 10 Year Daily Chart ," *Macrotrends*, August 19, 2019. See https://www.macrotrends.net/2516/wti-crude-oil-prices-10-year-daily-chart.

[xxiii] "Artificial Intelligence (AI) in Russia," *The Netherlands Embassy in the Russian Federation*, 2019. See https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=12&ved=2ahUKEwiC8-X_o8bkAhXtt1kKHel2DR4QFjALegQIBRAC&url=https%3A%2F%2Fwww.netherlandsworldwide.nl%2Fbinaries%2Fen-nederlandwereldwijd%2Fdocuments%2Fpublications%2F2018%2F11%2F09%2Fartificial-intelligence-in-russia%2FArtificial%2Bintelligence.pdf&usg=AOvVaw3zLIikqpEZcjpEu4YGI6hx.

[xxiv] Jon Harper, "Artificial Intelligence to Sort Through ISR Data Glut," *National Defense*, January 16, 2018. See https://www.nationaldefensemagazine.org/articles/2018/1/16/artificial-intelligence-to--sort-through-isr-data-glut.

[xxv] Mark Pomerleau, "DARPA Director Clear-Eyed and Cautious on AI," *Government Computer News*, May 10, 2018. See https://gcn.com/articles/2016/05/10/darpa-ai.aspx.

[xxvi] "Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DOD," The Mitre Corporation, January 2017. See https://apps.dtic.mil/dtic/tr/fulltext/u2/1024432.pdf.

[xxvii] David Gunning, "Explainable Artificial Intelligence (XAI)," DARPA, November 2017. See https://www.darpa.mil/attachments/XAIProgramUpdate.pdf.

[xxviii] Daniel S. Hoadley and Nathan J. Lucas, "Artificial Intelligence and National Security."

[xxix] "Executive Order on Maintaining American Leadership in Artificial Intelligence," The White House, February 11, 2019. See https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

[xxx] Ibid.

[xxxi] Ibid.

The Institute for Foreign Policy Analysis
http://www.ifpa.org

Robert L. Pfaltzgraff, Jr., President
RLP@ifpa.org
Jack Kelly, Senior Staff
kell@ifpa.org

September 16, 2019 Report

The Institute for Foreign Policy Analysis, Inc. (IFPA) develops innovative strategies for new security challenges. IFPA conducts studies and produces reports, briefings, and publications. We also organize seminars and conferences. IFPA's products and services help government policymakers, military and industry leaders, and the broader public policy communities make informed decisions in a complex and dynamic global environment. To find out more about IFPA's work and publications, visit www.IFPA.org.