Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Strategic Insights
Memo

TO: US National Security Community
FROM: Matthew Kroenig and Anastasia Kazteridis
DATE: October 3, 2018
SUBJECT: Artificial Intelligence and National Security

This Scowcroft Center for Strategy and Security Strategic Insights Memo briefly frames the emerging issue of artificial intelligence (AI) and its implications for national security. It provides:

- A brief primer on AI;
- Its possible applications to national security;
- An analysis of US and Chinese relative advantages; and
- Next steps for US strategy.

Artificial Intelligence 101: A Primer

Artificial intelligence refers to computer automation that gives machines the ability to conduct complex thinking. In the past, humans created the algorithms by which computers operate, but with AI, machines can program themselves. Though this "machine learning" is not new, it has progressed rapidly in the past decade due to an explosion of available data and advances in computing power. The abundance of data and faster computer chips allow machines to better process and analyze data, recognize patterns, and evolve their algorithms accordingly.

Implications of AI for National Security

Artificial intelligence is a general-purpose technology (more like electricity than a nuclear bomb) that is already beginning to have profound implications for many different sectors, including national security. Like most technologies, AI offers many benefits, but it also comes with a dark side.

Economic: AI provides great efficiencies and cost savings for many firms and will continue to be adopted in the private sector. Automation will also, however, disrupt the labor market, creating increased demand for labor in certain categories, but likely resulting in higher levels of unemployment in many unskilled and semi-skilled positions. These economic developments will have significant implications for foreign policy and national security.

Cybersecurity: Commercial technology in AI is viable for military use, lowering the threshold for other actors to acquire it and allowing weaker actors to pose a disruptive and asymmetric challenge to the United States. This is especially true in cybersecurity, where AI capabilities can constantly search for, and exploit or fix, vulnerabilities faster than humans can respond.

Surveillance: Governments collect more data than they can analyze. Footage from drone surveillance is currently used, for example, to gather information about past roadside bomb attacks. AI can review and analyze the vast data produced through surveillance in real-time, which might help spot and thwart attacks before they can be carried out. It could also be employed to improve missile defenses, fighter aircraft, and other defense technologies that depend on rapid sensing.

Military Robotics: The most direct application of AI to national security is military robotics. This includes fully-autonomous drones that could select and engage targets without a human in the loop. The major powers are hard at work on this potential application even as some warn that such "killer robots" should be banned outright as they pose a threat to humans' very existence.

Strategic Deception: Just as AI can analyze data for conclusions, it can also produce data for deception. High-quality forgeries of video and audio are already here, which gives an advantage to those interested in spreading disinformation.

Comparative Advantages of the United States and China in AI

Russia's President Vladimir Putin said, "Whoever leads in AI will rule the world," and at present the United States and China are neck and neck for the title.

US Advantages: The US has a lead in basic research and human capital, an unmatched university system that has trained the world's best AI experts, and is home to abundant sources of venture capital and the most innovative corporations.

Chinese Advantages: China has access to more data due to a larger population and fewer concerns about collecting private information which is critical for developing increasingly effective algorithms, an autocratic political system that can force government-industry cooperation and is better at taking basic research and quickly bringing products to market.

Towards a Strategy for AI

There are several obvious and immediate next steps for US government policy.

- The US must **produce a national artificial intelligence strategy**. The US government published a summary paper from a White House Summit on AI in May 2018 and the DoD has announced plans to establish a Joint Artificial Intelligence Center; these steps do not go far enough. The US needs a whole-of-government approach to innovation, integration, data acquisition and management, and employment of the technology. This could involve the creation of a lead government office that can formulate and implement the strategy. The US will be unable to compete without a more strategic approach.
- The US government should **increase engagement with US technology firms and foster better government-industry integration**. This will enable the US to leverage its advantages in personnel and research, and channel resources toward technologies with national security applications. The US needs to convince companies to cooperate with the government by focusing on the importance of US leadership while warning of the dangers of losing the competition to a potentially-hostile nation.
- The US should **increase AI cooperation with like-minded allies** who are likely to have advanced AI capabilities. The US and its allies have enormous innovative potential if they pool their resources. The US should assume a leadership role through multilateral coordination of allied defense ministries in developing and applying AI technology. It should consider delegating specialized tasks to allies according to their capabilities.
- The US should **identify potential areas of cooperation**, even with competitors, including China. The US and China may be able to work together to establish safety standards and international norms for the responsible use of this game-changing technology.

Matthew Kroenig is Deputy Director for Strategy in the Scowcroft Center for Strategy and Security at the Atlantic Council. **Anastasia Kazteridis** is a Program Assistant in the Scowcroft Center.