ASYMMETRIC THREAT SYMPOSIUM XIII

Cyber, Electronic Warfare, and Spectrum Operations: Critical Capabilities for Protecting America

REPORT 1 · AUGUST 2020

Automation and AI in Cyber Operations

Dr. Kevin M. McNeill, SVP, Cyberspace Solutions, CACI International Inc

A rapidly emerging asymmetric threat combines automation and artificial intelligence (AI) applied to cyberspace operations. The threat potential arises from autonomous intelligent behavior of software-defined systems used for either offensive cyberspace operations (OCO) or defensive cyberspace operations (DCO). Asymmetry emerges as autonomous cyber-attack capabilities can rapidly adapt their behavior to circumvent standard cybersecurity tools and operator responses.

The June 2016 Defense Science Board Report on Autonomy provided recommendations directed along three top-level objectives: 1) **accelerating** DoD's adoption of autonomous capabilities by targeting barriers to the operational use of autonomy; 2) **strengthening** the operational pull for autonomy by improving the trustworthiness of autonomous capabilities to build trust in the use of autonomous systems; and 3) **expanding** the envelope of technologies available for use on DoD mission to mitigate a wide range of operational challenges.

We often think of kinetic platforms such as drones or autonomous vehicles when considering autonomy. However, it is interesting to view these recommendations in terms of cyberspace operations. The prescience of the study is evident in authors' consideration of two categories of intelligent systems: those employing "autonomy at rest" and those employing "autonomy in motion." The first operate virtually **in software**, and include mission execution capabilities. The second have presence in the physical world and include **robotics and autonomous vehicles**. Whether these systems are cyber-physical or only cyber, they will be dominated by software-defined functionality based on a software architecture and integrated modules.

Automated systems are primarily rule-based systems whereas **autonomous systems** support intelligent decision-making and adaptation provided by software that models mission objectives, the operational environment, and the policies that apply. In OCO, autonomous systems can change behaviors to evade defenses, while in DCO they can dynamically adjust infrastructure or deploy countermeasures to protect networks. For cyber-physical systems, there will likely be an increase in the cyber-attack surface, including one-time access at any stage in the system development lifecycle from the drawing board to the battlefield, remote network access, maintenance connections, or exploitation of sensor apertures.

Artificial intelligence and machine learning (ML) are key enablers for increasing employment in computing systems and are priorities for cybersecurity research and development (R&D) investment. Autonomous cyber capabilities allow systems to change behavior by learning and correlating data across multiple sensor sources to understand attack behaviors and the corresponding risk to networks – for either OCO or DCO. Autonomous cyber attackers may be engaged by autonomous defenders to create an **autonomy/counter-autonomy battlespace.**

Autonomous threats require new capabilities, operator training, and test and evaluation. DoD cyber ranges must be modernized and instrumented for autonomy/counter-autonomy fights. A further challenge is updating wargaming environments for autonomy to adapt from "human-in-the-loop" to "human-on-the-loop." CACI conducts R&D into automation, AI, and ML, and develops high-fidelity modeling and simulation tools, enabling DoD **range modernization** efforts to incorporate and analyze the potential behavior of intelligent cyber systems.

The accelerating emergence of cyber autonomous systems available to adversaries can enable high impact attacks with lower cost to deploy. Their ability to learn and quickly alter behavior demands autonomous defenses to ensure effective mitigation of these threats. Innovation and R&D investment will be critical to develop solutions. ■