Pentagon Looks To Replace Human Hackers With AI

The Industrial/Military Complex is saturated with Technocrats who have algorithmic solutions for everything, including warfare. WWIII will be fought with AI-driven asymmetric tactics at the speed of light and far beyond human ability to understand what it is doing. TN Editor

Secretive Pentagon research program looks to replace human hackers with AI

The Joint Operations Center inside Fort Meade in Maryland is a cathedral to cyber warfare. Part of a 380,000-square-foot, $520 million complex opened in 2018, the office is the nerve center for both the U.S. Cyber Command and the National Security Agency as they do cyber battle. Clusters of civilians and military troops work behind dozens of computer monitors beneath a bank of small chiclet windows dousing the room in light.Three 20-foot-tall screens are mounted on a wall below the windows. On most days, two of them are spitting out a constant feed from a secretive program known as “Project IKE.”The room looks no different than a standard government auditorium, but IKE represents a radical leap forward.If the Joint Operations Center is the physical embodiment of a new era in cyber warfare — the art of using computer code to attack and defend targets ranging from tanks to email servers — IKE is the brains. It tracks every keystroke made by the 200 fighters working on computers below the big screens and churns out predictions

about the possibility of success on individual cyber missions. It can automatically run strings of programs and adjusts constantly as it absorbs information.
IKE is a far cry from the prior decade of cyber operations, a period of manual combat that involved the most mundane of tools.

The hope for cyber warfare is that it won't merely take control of an enemy's planes and ships but will disable military operations by commandeering the computers that run the machinery, obviating the need for bloodshed. The concept has evolved since the infamous American and Israeli strike against Iran's nuclear program with malware known as Stuxnet, which temporarily paralyzed uranium production starting in 2005.

Before IKE, cyber experts would draw up battle plans on massive whiteboards or human-sized paper sheets taped to walls. They would break up into teams to run individual programs on individual computers and deliver to a central desk slips of paper scrawled with handwritten notes, marking their progress during a campaign.

For an area of combat thought to be futuristic, nearly everything about cyber conflict was decidedly low-tech, with no central planning system and little computerized thinking.

IKE, which started under a different name in 2012 and was rolled out for use in 2018, provides an opportunity to move far faster, replacing humans with artificial intelligence. Computers will be increasingly relied upon to make decisions about how and when the U.S. wages cyber warfare.

This has the potential benefit of radically accelerating attacks and defenses, allowing moves measured in fractions of seconds instead of the comparatively plodding rate of a human hacker. The problem is that systems like IKE, which rely on a form of artificial intelligence called machine learning, are hard to test, making their moves unpredictable. In an arena of combat in which stray computer code could accidentally shut down the power at a hospital or disrupt an air traffic control system for commercial planes, even an exceedingly smart computer waging war carries risks.

Like nearly everything about such warfare, information about IKE is classified. As even hints about computer code can render attacks driven by that code ineffective, minute details are guarded jealously.

But interviews with people knowledgeable about the programs show that the military is rushing ahead with technologies designed to reduce human influence on cyber war, driven by an arms race between nations desperate to make combat faster.

Read full story here…