ARMY CYBER INSTITUTE

Weekly Threat Report

ACI – THREAT ANALYSIS CELL for 1 FEB 17 to 15 FEB 17

Fake News Morphs into Information Warfare.

Item of Interest: Information Warfare / Spear Fishing / Social Engineering

The "weaponization" of information exploded during the recent U.S. presidential campaign, prompting U.S. intelligence agencies to conclude that Russian meddled in the American presidential election. While one analyst insists that "fake news" is "old news" as its relates to sophisticated nation states and cyber adversaries, he also warns the impact of malware delivered via a single click on a fake news story or "spear phishing" campaigns could eventually knock out critical infrastructure and undermine security. What's more, argues James Scott, a senior fellow at Center for Critical Infrastructure Technology, cyber-terrorists also are "beginning to leverage news and fake news lures." >> The New Information Warfare.

AI Software Learns to Make AI Software.

Item of Interest: Artificial Intelligence / Machine Learning

Leading researchers are finding that they can make software that can learn to do the task of designing machine-learning software. The availability of computing power and the advent of deep learning are what's making the approach work. But it requires such extreme computing power that it's not yet practical to think about lightening the load, or partially replacing, machine learning experts. >> Dawn of Replacing People?

China's New Microwave Weapon Can Disable Missiles and Paralyze Tanks.

Item of Interest: Energy Weapons / Electronics Counter-measures

This weapon, which can pump out high-powered microwaves from a relatively small platform, could be the start of a new chapter in Chinese electronic warfare. Said another way: it's small enough to be convenient, but powerful enough to totally down enemy electronics. A microwave weapon like this could even be fitted to a missile (like the U.S. CHAMP electronic warfare missile) or drone. >> New Chinese Energy Weapon.

China's Intelligent Weaponry Gets Smarter.

Item of Interest: Artificial Intelligence / AI Weapons / Next Generation Weapons

The United States no longer has a strategic monopoly on the technology, which is widely seen as the key factor in the next generation of warfare. The Pentagon's plan to bring A.I. to the military is taking shape as Chinese researchers assert themselves in the nascent technology field. And that shift is reflected in surprising commercial advances in artificial intelligence among Chinese companies. >>Chinese Momentum in AI.

Pentagon Servers Flawed, Easy to Hack.

Item of Interest: Cyber Security / DCO / Network Security

Several misconfigured servers run by the DoD could allow hacker's easy access to internal government systems. That includes foreign actors eager to find a way into U.S. systems, especially since they could easily make it seem as if the attacks originated in the United States. The Pentagon was informed of the problem eight months ago, but no security fix has been deployed to those servers. This is mostly because the vulnerable servers were not part of the scope of the bug bounty program run by the Pentagon, which started about a year ago. >> Marine Corps at Risk?

Hackers Recruiting Insider Threats on Dark Web.

Item of Interest: Insider Threats / Dark Web / Cyber Crime

The insider threat is the worst nightmare for a company, as the employees can access company's most sensitive data without having to circumvent security measures designed to keep out external threats. The rogue employee can collect, leak, or sell all your secrets, including professional, confidential, and upcoming project details, to your rival companies and much more that could result in significant loss to your company. And this is exactly what is happening on Dark Web Marketplaces -- a place where one can sell and purchase everything from illicit drugs to exploits, malware, and stolen data. >> Recruitment for Collusion in Cyber Crime.