AI Enters the Cyber Attack Realm

Japan prepares for the latest weapons to hit the digital battleground.

and4me/Shutterstock

BY JONATHAN HOBBS

Artificial intelligence is one of the most influential forces in information technology. It can help drive cars, fly unmanned aircraft and protect networks. But artificial intelligence also can be a dark force, one that adversaries use to learn new ways to hack systems, shut down networks and deny access to crucial information.

The challenge is to prepare for a future where autonomous cyber attacks powered by artificial intelligence (AI) will threaten cyberspace and could endanger human life. This prospect is so significant that the Japanese Cabinet Secretariat tasked with developing the country's cybersecurity initiatives has created a research and development focus group to craft plans to counter cybersecurity threats, including those designed with AI.

One reason that Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) is preparing for such mind-bending, cyber-menacing possibilities is that it will host momentous events in the near future. The country will be the site of the Rugby World Cup next year and the 2020 Summer Olympics in Tokyo. Hosting such world-class events shines the spotlight on Japan in many positive ways. But it also makes these events a prime target for cyber attacks.

The center's primary mission is to develop the nation's public and governmental cybersecurity policy. It establishes the standards and operating policies for government and private entities as well as forensic and incident response protocols. In addition, the NISC promotes critical information infrastructure protection. While the NISC makes policy recommendations based on ongoing research, it does not create or impose regulations.

Traditionally, the definition of critical information has been limited to specific government branches, defense forces and certain infrastructure. But the introduction of AI into the equation changes the scope of that definition. AI software can provide powerful solutions for autonomously managing critical systems that can create defenses and reprisals against would-be attackers at lightning speed.

However, the converse also is true. Cyber attacks powered by AI could be potent and far-reaching. For example, the technology in AI-based autonomous cars could be exploited to cause accidents deliberately or to deliver dangerous substances or devices.

NISC Deputy Director-General Ikuo Misumi, who has been working in government cybersecurity in various ministries for more than a decade, says AI is his primary cyber concern today.

Unlike software, AI learns from each experience, improves its strategy and tailors a nearly irresistible lure to attract specific victims. AI cyber weapons can recruit resources, building a

cyber force that does not sleep and never gets sick or injured. It is arguably the most unrelenting force on the planet, Misumi relates.

Countering these kinds of emerging threats is an ongoing process. The NISC works directly with the private sector on a daily basis, and timely incident reporting to the center is critical to addressing vulnerabilities and, when necessary, notifying the organizations that may be affected.

Misumi understands that industry may be reluctant to share cyber incident information with the Japanese government because of possible regulatory retaliation, public embarrassment or competitor exploitation. However, the center assures companies that data regarding cybersecurity incidents is handled with care. Anonymization or sanitization removes information that could identify specific companies and protects personal data.

The introduction of AI to the cybersecurity realm makes reporting cyber attacks all the more important. The deputy director-general considers the threat from AI-based attacks so significant that he created a research and development cybersecurity strategy focus group to develop initiatives and policies to address cybersecurity threats, including those that originate through AI. The challenge is to prepare for a future where AI-powered cyber attacks will autonomously threaten cyberspace, he says.

Although AI-driven cyber weapons sound like science fiction, they have already been deployed with shocking effectiveness. For example, the SNAP_R Twitter phishing tool is an AI-powered social media algorithm that tricks its victims into revealing personal information. When pitted against a human phishing competitor, SNAP_R was nearly seven times faster and lured five times as many victims than the human phisher.

AI cyber weapons represent a significant threat to many countries, including Japan. Education and diligence are paramount, especially in terms of private-sector software, hardware, implementation and consulting solutions. The number of cybersecurity attacks is on the rise, and attacks can be carried out on critical infrastructure, public systems or personal devices.

Ikuo Misumi is the deputy director-general for the National Center for Incident Readiness and Strategy for Cybersecurity (NISC).

The NISC raises cybersecurity awareness through events such as last year's two-day Be Vigilant anime campaign in Tokyo's Akihabara neighborhood. More than 10,000 young people attended.

Building public awareness in Japan about cybersecurity and cyber hygiene is one of the NISC's main missions. Because the nation's younger generation represents the majority of Internet users, one tactic the NISC created is the Be Vigilant anime campaign. A year ago, the NISC held a two-day cybersecurity awareness event in Tokyo's Akihabara neighborhood as part of the campaign. More than 10,000 young people attended.

In addition to raising awareness, these approaches could attract the next generation to explore a career in cybersecurity at the NISC, officials hope.

To address the cyber challenges Tokyo will face while hosting the Summer Olympics, the cybersecurity standards and operations the NISC developed are already being carried out. The center is responsible for assessing the infrastructure that supports the games. The Tokyo Organizing Committee of the Olympic and Paralympic Games will protect systems that directly affect the outcomes of the games, such as time measurement and ticketing systems.

The NISC is working closely with the committee to secure organization of the games in a safe way. The center just completed a second round of the plan-do-check-act risk management cycle. It will carry out the cycle six times before the games begin.

A risk management cycle has been created for the infrastructure of each venue. For example, each location is equipped with three power sources. Two of the power sources, one of which operates as the main power source, are external and independent. In case these two power sources fail, each venue has a backup battery generator to provide on-site power.

In the future, the NISC will need to work more extensively with external partners, Misumi says, to meet its mission of continuing to develop policy for public and governmental cybersecurity and forensic and incident response, as well as protecting critical information.

• • • — • —

Jonathan Hobbs, Ph.D., is the founder and director of Hobbs & Associates, a boutique firm providing intellectual property and cybersecurity solutions for companies developing new technologies in Tokyo. He has a doctorate in neuroscience and physics from Indiana University, and his research focused on developing artificial intelligence algorithms and electronics that approximate biological systems.

To share or comment on this article go to ***http://url.afcea.org/March18***

contact: Jonathan Hobbs, jon@hobbspatents.com