How cyberspace has become the new battleground in modern day warfare

March 3 2022, by Neil Martin

Credit: AI-generated image (disclaimer)

Bolstering cybersecurity is becoming ever more important as nation states wage war in new and complex arenas.

That is the view of two UNSW academics in the wake of a wave of online attacks linked to Russia's military invasion of Ukraine.

As well as the use of tanks and bombs and soldiers on the battlefield, countries are now also waging war in cyberspace in order to weaken their enemies, most notably by targeting crucial infrastructure such as power and communications systems.

For example, in recent days and weeks Ukraine has accused Russian hackers of launching massive denial of service attacks on their government agencies, banks and the defense sector.

The United States government also claims Russia breached the networks of multiple defense contractors and gained sensitive information about weapons-development communications infrastructure.

And back in 2015, a series of power outages across Ukraine were allegedly caused by military hackers in the Russian GRU (Intelligence Agency) Main Center for Special Technologies.

CIA Triad

"Cyber warfare has become a tool by nation states to attack other countries," says Professor Sanjay Jha, deputy director of the UNSW Institute for Cybersecurity (IFCYBER).

"In the modern digital world, by attacking a computer server in the network of some critical piece of infrastructure, you can potentially take down an entire power system and with that, you could paralyze large parts of the economy.

"Other targets might be the banking system or a server that deals with communications systems so these system become unavailable to legitimate users.

"In cybersecurity any system needs to maintain confidentiality, integrity

and availability, aka the "CIA Triad."

"Availability is actually very important, and attackers can affect that by launching what is known as a distributed denial-of-service (DDoS) attack where they just bog down a system with junk data that it has to process.

"Nowadays attackers can draft 20, 30, 50 or 100s of servers all over the world sending packets of information and maybe wasting 99 percent of the server's time dealing with it.

"Just like in conventional conflict, each party wants to maximize the amount of damage and discomfort to the target."

Credit: AI-generated image (disclaimer)

Professor Salil Kanhere, another cybersecurity expert from UNSW's School of Computer Science and Engineering, says finding and then fixing vulnerabilities in computer programs or software is one of the most crucial ways to defend against attacks by state-sponsored hackers and others.

In December 2021, for example, news started to spread of an exploitation in Log4j, a software library that records a wide variety of otherwise mundane information in a vast number of computer systems.

It became clear that attacks on Log4j could allow hackers to submit their own code into the targeted computer and potentially steal information or even take control of the affected system.

"This particular vulnerability was really bad because Log4j software is used in a wide variety of consumer and enterprise services, websites, and applications," says Professor Kanhere.

"The question then becomes, do organizations have the resources to quickly act on the attacks and fix the vulnerability. The big players, and government agencies, will be able to but small-medium enterprises possibly can't react very fast, which means those systems are still vulnerable to attacks.

"What attackers then do is scan the internet, trying to find a system that still has this weakness and then exploit it.

"The major problem is that computer systems nowadays are so complex and intertwined that if attackers find one weak link somewhere, that is enough to gain access into critical systems and steal data or launch further attacks."

Social engineering

On top of all that, cyber attacks can also be cleverly targeted not only at computers themselves but also by the humans who use them.

Phishing attacks can trick users into giving out sensitive information that then compromises security and allows nefarious access into systems.

"Some of the phishing nowadays is so sophisticated," says Prof. Jha. "So much so that even a fairly educated cybersecurity person may be tricked.

"There are also social engineering tactics where people are manipulated into clicking something that then allows an attacker to install malware, or ransomware, or steal information."

In times of war, such as the current Russian invasion of Ukraine, Prof. Kanhere says gaining access to information has the potential to have a huge impact on the success or failure of actual military attacks.

Discovering battle plans, potential maneuvers of troops and equipment, or hacking into secure communications systems used by soldiers and their command could help win wars in the modern age.

"In the past a lot of that information would have been on paper, but now it is all digitized and therefore may be vulnerable," Prof. Kanhere says.

"If you can extract that information then it could certainly give you the upper hand militarily. Traditional wars were fought on land, air, and sea. But now we also have space and cyberspace as the fourth and fifth battlegrounds that are emerging."

And that means that all major governments around the world, not just the Russians, are likely to have cyber experts on hand to play their part in the way 21st-century conflicts are now fought.

"The specific details about that are bordering on national intelligence which I'm not an expert on, but it's not surprising to think that given the importance of information technology and the potential to disrupt networks, that would be a very obvious choice for militaristic efforts," Prof. Jha says.

"It would be reasonable to conclude that all governments, not just Russia, have some sort of cyber units placed in different organizations with the capability of launching offensives if needed."

In terms of bolstering cybersecurity, the UNSW academics say it is a constant game of cat-and-mouse as countries try to secure their systems and fix vulnerabilities faster than the hackers can exploit them.

Artificial intelligence

Prof. Jha is currently conducting research, funded by Cybersecurity CRC, that aims to help develop tools to identify potential security issues in Australia's Distributed Energy Resource Management System (DERMS) that links a range of electrical power industries.

He is also involved in work to improve artificial intelligence models that can identify patterns of cyber attacks and predict future risks using a range of internal and external intelligence.

Prof. Kanhere, meanwhile, is researching the use of machine learning to design network protocol fuzzing tools, which can automatically find vulnerabilities and attack strategies in network routing protocols that are critical to the functioning of the internet.

"The general advice is for systems to be patched to make sure they are secure and for networks to be configured so they can handle any denial-of-service attacks by doing some early detection," says Prof. Jha.

"There is a lot of development in artificial intelligence and machine learning, plus software looking at vulnerability detection.

"But as our dependency on computers keeps increasing, these problems and these attacks are not going to go away. As quickly as we come up with a solution, the bad guys are thinking of another way to attack.

"Now that these vulnerabilities can be exploited during warfare, it's becoming absolutely important that we pay a lot attention to cybersecurity going forward."

Provided by University of New South Wales