CYBER SECURITY & INFO TECHNOLOGIES

Are We Ready for the Current and Emerging Cyber Threats?

DECEMBER 1, 2023

Information technology dominates the contemporary world. As cyberspace rapidly expands and becomes more integrated into our daily lives, so does the malicious use of this domain. Real-world crimes have infiltrated the digital world; even terrorism and interstate war have found new strongholds in the cyber realm. The increased dependence on technology offers prime opportunities for those with hostile intent to wage a subtle but crippling form of warfare. The world is currently experiencing yet another paradigm shift in how societies wage war. Cyberspace has become a new battleground in modern warfare.

The Russian military invasion of Ukraine constitutes a prime recent example of how cyberspace can be weaponized. On January 14, 2022, Ukrainian government agencies were subjected to significant cyberattacks, which were seen as an attempt to weaken the nation's defense before the invasion began. These attacks continued and targeted two state-owned banks, followed by massive Distributed Denial-of-Service (DDoS) attacks and malware strikes involving ransomware and wipers throughout February. The use of wipers clearly demonstrates that the attacks were aimed at destroying the target's systems and making them inoperable. In effect, Ukrainian businesses and organizations were bombarded with various forms of cyberattacks both before and during the invasion.

Ukraine was not the only target, for Russian state-backed hackers also earmarked several other countries that supported Ukraine. According to Microsoft, these hackers attacked 128 targets in 42 countries. For instance, after Romania declared its support for Ukraine, several Romanian government agencies, including the Defense Ministry, were hit by DDoS attacks. In a similar vein, Russian hackers had used DDoS attacks in 2007 to take down Estonian targets, including critical infrastructure.

Many critical infrastructures today can be controlled digitally, and a cyberattack against these can cause actual physical damage. The recent attack on the Colonial Pipeline exemplifies how state-sponsored hacker groups can exploit digital control mechanisms to disrupt critical infrastructure. In fact, the Microsoft Digital Defense Report of 2022 reveals that 40 percent of all nation-state activities are aimed at targeting critical infrastructure such as communications, transportation, financial services, and the IT sector. According to the report, IT companies are the most common targets of nation-state actors, followed by NGOs, universities, and government agencies. Although the attacks on critical infrastructure have not been unduly destructive, they are still a cause for concern, for they can be used to aid military campaigns in hybrid warfare. In response to these trends, Microsoft has developed a nation-state notification system (NSN) that alerts its customers of observed nation-state activities.

National security is increasingly concerned with cybersecurity. The Biden administration has emphasized the importance of this area on several occasions and pledged to enhance the country's cyber capabilities and deterrence against such attacks. The National Cybersecurity Strategy of 2023 emphasized the importance of defending critical infrastructure from cyberattacks and creating resilience. The document listed the governments of China, Russia, Iran, and North Korea among the malicious actors in cyberspace and offered policies and strategies to deal with threats from these actors.

Further highlighting this new arena of warfare, the Department of Homeland Security's 2020 report identified cyber threats from nation-states and non-state actors as one of the seven major threats to the US, whose government has taken several steps in recent years to improve the nation's defensive and offensive capabilities in cyber warfare. Similarly, businesses increasingly invest more in cybersecurity and become more vigilant against cyber threats. While such efforts are indications of improvement, there still exists a need for a concerted effort to address vulnerabilities, prevent major cyberattacks, and mitigate potential threats.

Yet another crucial area that requires significant attention lies in the impact of AI on cyberwarfare and cybercrime trends. Efforts to create policies to address these growing threats often lag behind the evolving ways in which state and non-state actors utilize them. Therefore, the need to establish effective domestic and international legal frameworks to

tackle these concerns is indeed urgent.

Orion Policy Institute (OPI) is an independent, non-profit, tax-exempt think tank focusing on a broad range of issues at the local, national, and global levels. OPI does not take institutional policy positions. Accordingly, all views, positions, and conclusions represented herein should be understood to be solely those of the author(s) and do not necessarily reflect the views of OPI.