Martian Defense Research: White Paper

Cyberwar and the Effects on Global Security

By @Martian

Security Researcher

Introduction

Cyberwar describes a series of cyber attacks against a nation, state, or international organization seeking to disrupt, damage, or destroy infrastructure using computer viruses, denial-of-service attacks or other methods. Cyberwar typically involves one nation perpetrating attacks on another nation, but sometimes, these attacks emanate from terrorist groups or fascist groups seeking to advance the agenda of an already hostile nation. Although the US Department of Defense (DoD) recognizes the potential dangers of cyberwar, it does not provide an explicit definition of cyberwar. Some experts insist that it should be considered a form of war only if the attack leads to loss of life. Regardless, the harm caused by these attacks can cripple critical government and civilian infrastructure, and this may result in damage to property or even loss of life.

Just a few years ago, tales about cyber warfare were punctuated with bleak prospects: what if state-sponsored hackers blacked out cities across the country? Sabotaged banks and froze all ATMs? Crippled shipping firms, oil refineries, and factories? Shut down airports and hospitals? Today, these events are unraveling. More than ever before, it is evident that these attacks have transcended into physical disruption on a global scale; a feat that could only be achieved through military campaigns and terrorism.

Cyberwar and the Effects on Global Security

Understanding the different types of cyberwar attacks is a step forward in appreciating the impact they can have on global security. There are common types of attacks that constitute cyberwar: Espionage; Sabotage; and Denial-of-service (DoS) Attacks. This paper will explore each of these attacks; their potential impact on global security; and their real-world examples.

Espionage

Espionage involves monitoring governments or other entities to steal crucial information. Also called spying or intelligence gathering, espionage employs botnets or spear-phishing to infiltrate computer systems before extracting crucial information. The primary goal of a cyber espionage attack is for the attacker to collect as much intelligence as possible to facilitate a cyber war attack. Therefore, they have to remain hidden for as long as possible. The tactics used in cyber espionage include: [1] exploiting the vulnerabilities of websites or browsers [2] spear-phishing emails [3] malware, Trojans, and worms [4] supply chain attacks directed at the target's business partners, and [5] compromising updates for the commonly used third-party software.

Cyber espionage plays an increasingly important role in modern warfare as exemplified in its use by Russia. The Moonlight Maze virus, for example, was deployed by Russia to steal confidential information from the Department of Defense, the Department of Energy, NASA, and military contractors. Were it not for its discovery by the U.S. cyber security experts in late 1999, the malware may have been used by Russia to collect crucial military information to give Moscow an advantage over Washington, and potentially trigger an actual attack. Essentially, it tears down the defenses of a country making it a sitting duck for its adversaries.

Sabotage

Cyber sabotage refers to deliberate and malicious activities that disrupt normal processes and functions, or damages equipment and information. Sabotage in cyberspace can make it difficult for armies to coordinate attacks or defenses in the event of a conflict. Although there have been wartime saboteurs in the past, the shift to digital dependence makes it easier for attackers to lie in wait in their safe cocoons - far away. In addition, cyber sabotage is difficult to defend against for several reasons. First is the huge number of machines and networks that need protection. Secondly, the overlapping links between military organizations, defense firms, and other contractors create many potential loopholes for infiltration. Lastly, the large amount of software code used to underwrite military hardware bears characteristic flaws that defenders may not be aware of until they are compromised.

A recent example to illustrate the difficulty in making computer systems 100 percent safe from cyber saboteurs occurred about 15 years ago. In November 2007, 3200 hard drives linked to Seagate Maxtor Basics Personal Storage were inflicted with a Trojan Horse Attack. Trusted sources revealed that the Trojan was intended to copy information on the computer and transmit it to a Beijing-based website without the users' knowledge.

Denial-of-Service (DoS) Attacks

Widely referred to as DoS attacks, Denial-of-Service (DoS) Attacks prevent legitimate users from accessing a website by sending the website a deluge of fake requests; and forcing it to process these requests. Such an attack overwhelms the website and disrupts critical operations and systems. As a result, it blocks access to sensitive websites by civilians, research bodies, and even military/security personnel. DDoS attacks threaten the security of a country because they disrupt the organization needed to put up a strong defense.

Russia has been using DoS attacks on its neighbors, as a form of warfare and in conjunction with traditional warfare. When Estonia removed a pro-soviet Union statue back in 2007, Russia responded by launching a crippling DDoS attack on Estonia that brought down service on key websites and disrupted communication across the country. Just months later, it also sent torrential DDoS attacks that shut down communication to cut off Georgia from the outside world; then sending its troops in the secluded country. In 2014, Russia employed the same tactic by disabling Ukraine's mobile phone communications before invading it.

Collateral Damage Attack Potential

Below are some of how cyber attacks can jeopardize international security. It is worth noting that these attacks may be facilitated by any or a combination of the types of attacks covered in the previous section.

Electrical Power Grid Attacks

Attacking the computer systems that control power grids enables attackers to bring down critical systems, disrupt infrastructure, and potentially lead to the destruction of property and loss of life. For instance, such an attack can cut off power to a healthcare facility and can lead to many deaths. The recent extensive blackout caused by a severe winter storm in February 2021 provides a view of the aftermath of an attack on the electrical power grid. The power outage was experienced across Texas and left about 11 million people freezing for up to 3 days. Additionally, a disrupted power supply system translates to disrupted communication such as phone calls and text messaging. In the event of an invasion, poor communication could result in poor coordination of defense strategies. Without electrical power modern societies are doomed.

The European Network of Transmission System Operators for Electricity (ENTSO-E), which represents 42 European transmission system operators in 35 countries, was hacked in 2020. Similarly, Saudi Aramco petrochemical plants and the Russian power grid were hacked in 2017 and 2019 respectively.

Propaganda as a Weapon

Cybercriminals hired by rogue regimes may want to control the minds and thoughts of citizens of a given country to fight for depraved causes. Propaganda can be used to reveal hidden truths, spread lies, make people distrust their government, and therefore side with the enemy. Propaganda attacks are similar to traditional propaganda save for the fact that they are transmitted through online channels. Around late August of this year (2023), Facebook's parent company – Meta – discovered that there had been a prolonged anti-American and pro-Chinese messaging campaign that infiltrated the ideals of the authoritarian Chinese regime to thousands of Facebook accounts and pages. Before being taken down, the campaign that went by the name "Spamoflauge" had approximately 7,000 fake accounts linked to it.

Aside from Facebook, this propaganda attack targeted over 50 accounts, which include Instagram, X (formerly Twitter), YouTube, TikTok, Reddit, Pinterest, Medium, Blogspot, LiveJournal, VKontakte, Vimeo, and a handful of other smaller social media platforms. Such attacks pose a threat to world people as they pit countries against each other.

Economic Disruption

Cyber attacks can also destabilize global security by sabotaging economies around the world. These attacks are becoming more troublesome to economies because modern economic systems are interconnected and run on computers. Attackers may target computer networks supporting economic systems including payment systems, the stock market, and banking systems. It is important to always maintain harmony of economic interests among individuals, groups, states, and regions because– according to the writing of economist John Stuart Mill– this state of balance minimizes incidences of conflict. Therefore, attacks on economic systems may upset the socioeconomic balance, which may result in widespread conflict.

Conclusion

As it stands now, there is no recorded case of death directly linked to a cyberwar attack but there is one case where a 2019 ransomware attack on Springhill Medical Center in Alabama caused disruptions that allegedly led to a newborn's death. However, cyber attacks have cost individuals, groups, businesses, and companies billions of dollars in losses. Cybercriminals have used varying techniques to terrorize organizations and briefly render entire governments dysfunctional. Additionally, it has denied citizens basic services like power and communication—if only shortly, so far—as well as extended deprivations of transportation services and access to money. Even worse, cyberwar seems to be evolving in the hands of polarized countries like Iran, North Korea, and Russia as they continue to improve their cyber attack techniques.

Among the primary ways to combat cyberwar is to conduct real-life exercises or simulations—commonly known as a cyber wargame. In sum, a wargame can test if and how governments and other organizations are prepared to respond to a cyberwar scenario; reveal the gaps in defenses, and improve cooperation among relevant bodies.