**Cyber Attacks: The Art of Silent Warfare**

By: - Abhishek Sheoran

Ishpreet Singh

Kohinoor Sharma

Tapish Tanwar

**Abstract**

Cyber Attacks target digital infrastructures to gain sensitive information which may later be used to exploit an individual or an organization. The name itself may not carry much weight but, in recent years, this form of insidious assault has proved more lethal than entire artilleries.

The boon of technological advancements soon lost its credibility as humans realized their alternate capabilities. What may have started as a simple hack, soon became a viable alternative to armies. It enabled us to cause more concentrated damage with limited casualties of our own. This paper intends to cover the amalgamation of cyber-attacks into a means of warfare.

The readers will also be provided an objective rationalization of the motives behind the attacks. The writers of this paper don’t condone terrorism or vandalism but do consider the possibility of cyber-attacks being a viable platform for stating one’s views without being castigated.

The future of the digital world is intricate and capricious, but so are the minds controlling it.

**Introduction**

Cyber Networks act as the nucleus for all minor to major operations ranging from an individual’s personal information to the very nuclear codes. It is independent of geographic boundaries and is much faster, and often requires less manpower. The world is on the path of digitalization and hence it is no surprise cyber operations are also experiencing an uprise.Some important terminology is mentioned below:

**Types:**

1. [**Malware**](https://www.rapid7.com/fundamentals/types-of-attacks/#f1)

A malware attack is a common cyberattack where malware (normally malicious software) executes unauthorized actions on the victim’s system. Malicious software (a.k.a. virus) encompasses many specific types of attacks such as ransomware, spyware, command, and control, and more. Criminal organizations, state actors, and even well-known businesses have been accused of (and, in some cases, caught) deploying malware.

1. [**Phishing**](https://www.rapid7.com/fundamentals/types-of-attacks/#f2)

This occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack, or the revealing of sensitive information.

1. [**Cross-Site Scripting (XSS)**](https://www.rapid7.com/fundamentals/types-of-attacks/#f4)

Cross-site scripting (XSS) is an attack in which an attacker injects malicious executable scripts into the code of a trusted application or website. If the app or website lacks proper data sanitization, the malicious link executes the attacker’s chosen code on the user’s system. As a result, the attacker can steal the user’s active session cookie.

1. [**Denial of Service (DoS)**](https://www.rapid7.com/fundamentals/types-of-attacks/#f5)

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e., employees, members, or account holders) of the service or resource they expected.

1. [**Session Hijacking and Man-in-the-Middle Attacks**](https://www.rapid7.com/fundamentals/types-of-attacks/#f6)

A man-in-the-middle (MiTM) attack is a type of cyber-attack in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other. MiTM cyber-attacks pose a serious threat to online security because they give the attacker the ability to capture and manipulate sensitive personal information -- such as login credentials, account details, or credit card numbers -- in real time

**Case studies:**

1. **The Eastern Railway Website Defacement:**

Indo-Pak relations have been tense since '47. This contentious environment was only made worse on December 24, 2008, when the official eastern railway site was corrupted by numerous messages like, "Cyber war has been declared on Indian cyberspace by Whackerz-Pakistan" followed by "Indians hit hard by Zaid Hamid", etc.

The notorious group responsible called itself "Mianwalian of Whackerz", and the reason provided was a violation of Pakistan air space. In retaliation, the Indian Group Guards hacked into the oil and gas regularity authority of Pakistan’s website. A series of churlish attacks followed back on forth with multiple unidentified hacking groups being involved, ending with the Bank of India, one of the largest Indian banks, being completely down on Christmas eve.

1. **Russia's war on Ukraine: Case Study 2**

Since the illegal annexation of Crimea in 2014, a series of Russian cyber attacks have been directed toward Ukraine The most recent occurring in February of 2022. The purpose of these attacks ranged from the restriction of basic needs and services to Ukrainian citizens to data theft and manipulation.

Various initiatives by NATO, the US, and the EU to put an end to these cyber-attacks were carried out. One of them is the cyber rapid response team to strengthen cyberspace Now, various counterattacks have also been initiated by Ukraine, mostly by independent hackers.

Cyber warfare has caused more concentrated damage to both countries.

**Literary Review:**

The first case study was an example of cyber-attacks, and the second explained how these attacks morphed into cyber warfare. One of the reasons the Russians were so successful was because of their concentrated attacks. Cyber Warfare made it comparatively easier to gather intel about Ukraine’s escape measures and stratagems. They bordered Kyiv to limit escape and cause maximum damage. A century ago, this assault would have been less efficient cause an actual agent would have had to be deployed to gather intel, with the added chance of the agent being compromised or being unfaithful to its country and providing false intel.

.

**Links to Terrorism**

Cyber-attacks can cause electrical blackouts, failure of emergency equipment, and breaches of national secrets. They can result in the theft of sensitive data. They can disrupt phone and computer networks or paralyze systems, making data inaccessible. We earlier discussed various types of cyber-attacks, the following are more sophisticated forms of the commonly used techniques:

**Ransomware:**

An attack involves encrypting data on the target system and demanding a ransom in exchange for letting the user have access to the data again. These attacks range from low-level nuisances to serious incidents like the locking down of the entire city of Atlanta’s municipal government data in 2018.

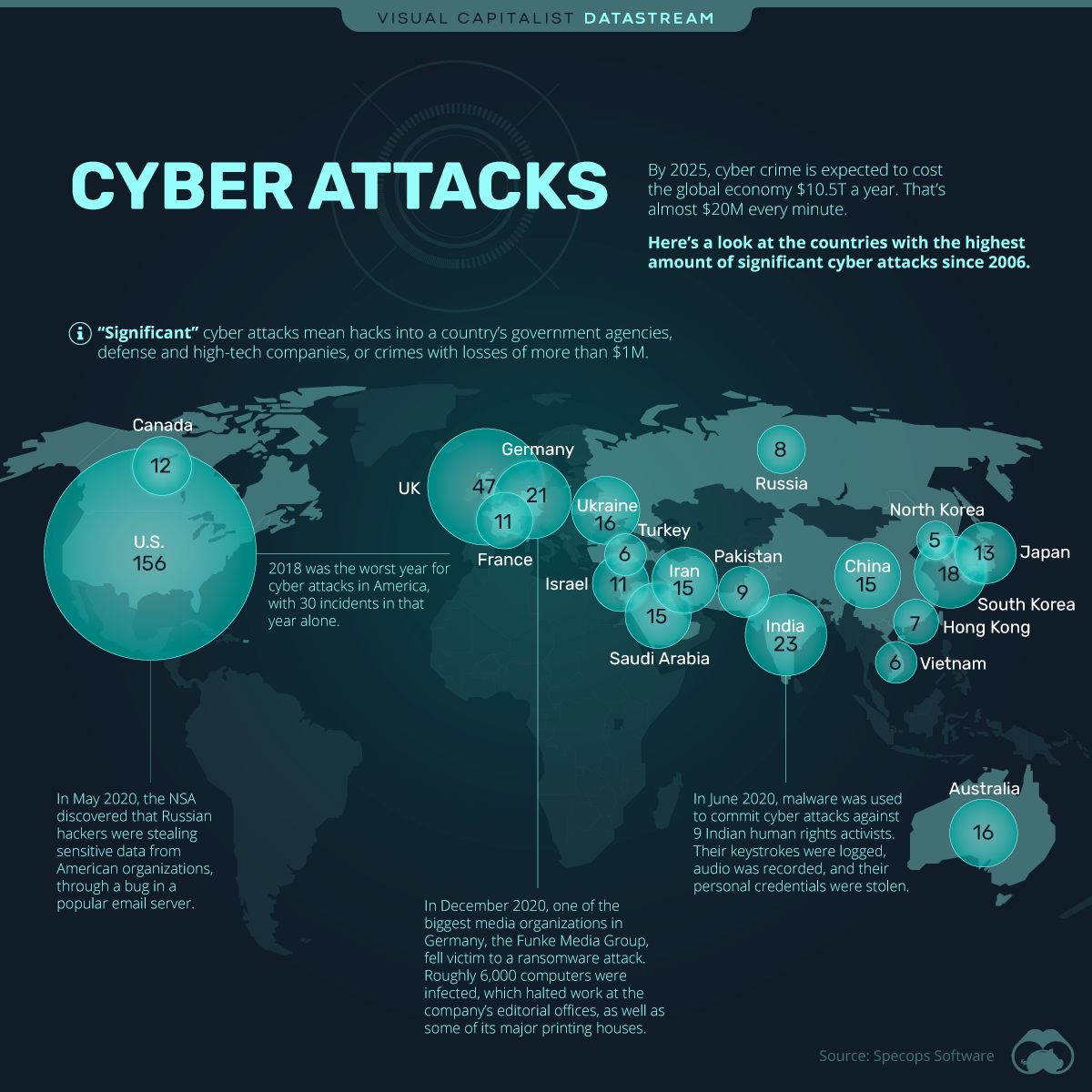
**Malware on Mobile Apps:**

Attackers may embed malware in apps, mobile websites, or phishing emails and text messages. Once compromised, a mobile device can give the malicious actor access to personal information, location data, financial accounts, and more. The risk of this very form of attack was one of the reasons why India banned apps developed in China.

**Trojans**

Named after the Trojan Horse of ancient Greek history, the Trojan is a type of malware that enters a target system looking like one thing, e.g. a standard piece of software, but then lets out the malicious code once inside the host system.

Cyber-attacks aren’t limited to these techniques, but these were the most recently used forms that we need to be aware of. Following is a pictorial representation of how minor attacks have conduced terrorism.



Following are examples of 2021 attacks that CSIS identified:

* **January.** Hackers with ties to the Chinese government deployed ransomware attacks against five major gaming companies. They demanded over $100 million in ransom.
* **February.** Hackers tried to [contaminate the water supply](https://www.techtarget.com/searchsecurity/feature/After-Oldsmar-How-vulnerable-is-US-critical-infrastructure) of Oldsmar, Fla., by exploiting a remote access system to increase the amount of sodium hydroxide present.
* **March.** The Polish government said it suspected Russian hackers had taken control of Poland's National Atomic Energy Agency and Health Ministry websites for a short time. They tried to spread alarms about a radioactive threat that didn't exist.
* **May.** North Korea carried out a cyber-attack against South Korea's state-run Korea Atomic Energy Research Institute by taking advantage of a virtual private network vulnerability.
* **July.** [Iran used Facebook](https://www.techtarget.com/searchsecurity/news/252509744/CISA-Microsoft-warn-of-rise-in-cyber-attacks-from-Iran) to target U.S. military personnel, posing as recruiters, journalists, and nongovernmental organization personnel. The hackers sent files with malware and used phishing sites to trick victims into providing sensitive credentials.
* **September.** Hackers stole 15 terabytes of data from 8,000 organizations working with Voicenter, an Israeli company. The hackers offered the data online for $1.5 million.
* **October.** Brazilian hackers attacked a website belonging to Indonesia's State Cyber and Password Agency.
* **December.** A Russian group claimed responsibility for a ransomware attack on CS Energy, an Australian utility company.

**A Necessary Evil?**

Till now we have discussed the harmful impacts that cyber warfare has had on the world, the authors believe it to be fair to objectively consider the causes of these digital insurrections.

It cannot be ignored the initial purpose of cyber-attacks was extortion and the gain of other selfish benefits. But, then why did it go to a larger scale? Greed couldn’t be enough of a reason for taking such a huge risk. The primary objective of this method going global and large scale could have been to be heard.

Founding principles, such as freedom of speech and complete transparency, have had their authority diminished over the past few years. Petitions and rallies have proved to be futile. Major corporations (and/or governments) are successfully polluting our world and hiding incriminating evidence without none the wiser. In this case, it seems almost essential to reveal the misdeeds and provide people with the opportunity to judge for themselves, whether they want things to continue the way they are or do they need a change. Sometimes, a small wake-up call is all takes to start a revolution.

Granted, we can’t ignore the fact that more often than not, these “revolutionaries” go overboard, by vandalizing the people in question. Emotions take control, things go out of hand. A sane man would argue that the evidence of misconduct be provided to proper authorities. Presenting the citizens with the evidence is the epitome of transparency but proper justice can’t come out of emotional masses. But then can it also come out of corrupt judiciaries?

Let’s consider an example from 2012 when the notorious group of hackers called “Anonymous” hacked into the Ugandan prime minister’s website to raise their voice against the government repressing the stance of gay and transgender communities on their websites. Now, if the very authority of justice is suppressing your voice what choice is left but to ask your fellow compatriots for support.

This paper has given multiple accounts of when cyber-attacks caused irreparable damage to innocents. The purpose of this section was to show both sides of the coin, not to justify terrorist actions.

**Prognosis**

**References**

<https://www.rapid7.com/fundamentals/malware-attacks/>

<https://www.imperva.com/learn/application-security/phishing-attack-scam/#:~:text=Phishing%20is%20a%20type%20of,instant%20message%2C%20or%20text%20message>

<https://www.synopsys.com/glossary/what-is-cross-site-scripting.html#:~:text=Cross%20site%20scripting%20(XSS)%20is,the%20user%20to%20click%20it>.

<https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos#:~:text=A%20Denial%2Dof%2DService%20(,information%20that%20triggers%20a%20crash>.

https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM#:~:text=Session%20hijacking.,access%20to%20users'%20saved%20resources

<https://web.mit.edu/smadnick/www/wp/2017-10.pdf>

<https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf>

https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/