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

By Abhishek 2 pages

* **Introduction**
  + Recent advances in technology have completely changed how we live on this planet. Everything can be done in an online world now, from shopping to banking to collaborating on projects. As with all technologic advances in history, this cyber world has also been turned into a weapon. It began with individuals pushing the limit of the web or going for personal gain, but now governments have begun to realize that the potential for a cyber attack is very real, and the resulting damage could be catastrophic. Because of this, several countries are researching and preparing cyber defences, independently and collaboratively.

At the same time, being able to organize such an attack would allow a nation to cripple an enemy without any traditional military action. This has prompted governments to also invest in cyber weapons. Because of the Internet's anonymity, it is easy for an attacker to either hide his tracks or leave a false trail. As such, there have been several large cyber attacks already that cannot be definitively traced to a country, organization, or person. Only the motives behind the attack and how the attack was performed can give clues towards the aggressor.

Reference**:** <https://www.cse.wustl.edu/~jain/cse571-11/ftp/cyberwar/index.html#intro>

* + Cyberspace has eliminated traditional geographic boundaries. States, organisations and individuals are today linked by vast, interconnected networks to disseminate information and data at a rapid rate. Everyday activities – from banking and sharing musings through blogs or email, to controlling systems and infrastructure – occur through digital networks in interconnected infrastructure. Alongside the extensive utilisation and uptake of cyber operations, there arises a great risk that these linked systems and networks, and the data contained therein, may become the target of intentional malicious acts by States and non-State actors. It is not surprising that cyberspace has become a new frontier for attack given the ease and global uptake of cyber connectivity. There is global concern that the nature and scope of cyber-attacks could cause far-reaching and devastating consequences. The concern of cyber warfare manifests in the law of armed conflict (LOAC) especially given the potential impact on civilian populations. This paper will canvas five selected issues in LOAC as applying to cyber warfare:

Reference: <https://core.ac.uk/download/pdf/41339676.pdf>

* **Definition**

| **Title** | **Definition** |
| --- | --- |
| **Cyber space** | Interconnected networks, from IT infrastructures, communication networks, computer systems, embedded processors, vital industry controllers, information virtual environment and the interaction between this environment and human beings for the purpose of production, processing, storage, exchange, retrieval and exploitation of information. |
| **Cyber capital** | A vital (or sensitive) infrastructure of a country, a vital cyber system, a key information, or individuals belonging to a country. |
| **Cyber vulnerability** | Vulnerability refers to a weakness within an asset, security procedures or internal controls, or the implementation of that national cyber asset that can be exploited or activated by internal or external threats to conduct cyber warfare. |
| **Cyber threats** | Any event with the ability to strike a blow to missions, tasks, images, national cyber assets or personnel through an information system, through unauthorized access, destruction, disclosure, alteration of information and/or obstruction of (disruptive) service delivery. |
| **Cyber threat level** | Cyber threats are able to affect national cyber assets at the transnational, national, institutional, provincial, critical, and critical levels of infrastructure. |
| **Probability of cyber threats** | Very high (imminent), high (probable), low (unlikely) and very low (very unlikely) |
| **Intensity of cyber threat** | Very high (disaster), high (crisis), moderate (major security incident), low (security incident) and very low (security incident) |
| **Cyber attack** | Any unauthorized cyber act aimed at violating the security policy of a cyber-asset and causing damage, disruption or disruption of the services or access to the information of the said national cyber asset is called cyber-attack. Intentional use of a cyber-weapon against an information system in a manner that causes a cyber-incident is also considered cyber-attack. |
| **Cyber weapon** | A cyber weapon is a system designed and manufactured to damage the structure or operation of other cyber systems. These systems include bot networks, logic bombs, cyber vulnerability exploitation software, malware, and traffic generation systems to prevent service attacks and distributed service. |
| **Cyber warfare** | Cyber warfare is the highest level and most complex type of cyber-attack (cyber operation) that is carried out against the national cyber interests of countries and will have the most severe consequences. |
| **Cyber warfare origin** | The cyber force of the aggressor country or groups organized under the aggressor states, cyber weapons controlled or abandoned by these forces |
| **Cyber defense** | Utilization of all unarmed cyber and non-cyber facilities of a country, to create deterrence, prevention, prevention, timely detection, effective and deterrent response to any cyber attack |
| **Cyber biome** | Cyber biome refers to the formation of a native and dynamic cyber environment that is supportive for a country in various fields. |
| **Virus** | A virus is a self-replicating program that spreads to other documents and other programs by duplicating itself, and may cause programs to malfunction. A computer virus acts like a biological virus that spreads through its reproduction to cells in the host body. Some of the popular viruses are: NIMDA, SLAMMER, and SASSER. |
| **Hacker** | A person who enters a system without permission or who increases his/her access to information to browse, copy, replace, delete or destroy it. |

Diagram, venn diagram

Description automatically generated

Fig. . Distinction between cyber-crime, cyber-warfare, and cyber-attack.

Reference: <https://www.sciencedirect.com/science/article/pii/S2352484721007289>

* **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. The 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. Like other types of cyber-attacks, some malware attacks end up with mainstream news coverage due to their severe impact.

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

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

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It 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.

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

[**SQL Injection Attack**](https://www.rapid7.com/fundamentals/types-of-attacks/#f3)

An SQL injection, sometimes abbreviated to SQLi, is a type of vulnerability in which an attacker uses a piece of SQL (structured query language) code to manipulate a database and gain access to potentially valuable information. It's one of the most prevalent and threatening types of attack because it can potentially be used against any web application or website that uses an SQL-based database (which is most of them).

Reference: <https://www.kaspersky.com/resource-center/definitions/sql-injection>

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. Attackers often initiate an XSS attack by sending a malicious link to a user and enticing the user to click it. 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.

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

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.

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

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. The attack is a type of [eavesdropping](https://www.techtarget.com/searchunifiedcommunications/definition/eavesdropping) in which the attacker intercepts and then controls the entire conversation. 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

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

1. [**Credential Reuse**](https://www.rapid7.com/fundamentals/types-of-attacks/#f7)

Users inundated with requirements to supply complex passwords to different systems often resort to reusing the same password across multiple accounts so that they can easily manage their credentials. This can cause major security issues when those credentials are compromised.  
In a credential reuse attack, the attacker is able to obtain valid credentials for one system and then tries to use the same credentials to compromise other accounts/systems.

Reference: https://doubleoctopus.com/security-wiki/threats-and-tools/credential-stuffing/#:~:text=In%20a%20credential%20reuse%20attack,to%20compromise%20other%20accounts%2Fsystems.

* **Case studies**

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

Relations between India and Pakistan have been complex due to a number of historical and political events. Relations between the two states have been defined by the violent partition of British India in 1947, the Kashmir conflict and the numerous military conflicts fought between the two nations. Consequently, even though the two South Asian nations share linguistic, cultural, geographic, and economic links, their relationship has been plagued by hostility and suspicion. On December 24, 2008, the Whackerz Pakistan Cr3w defaced India’s Eastern Railway website with the following announcement: “Cyber war has been declared on Indian cybers[ace by Whackerz-Pakistan1.”

The Indian group Guards of Hindustan hacked into the Oil and Gas Regularity Authority of Pakistan website and placed their organization’s logo and the Indian national symbol on the site. The Pakistani organization Pakistan Cyber Army soon answered the attack by hacking the websites of the Indian Institute of Remote Sensing, the Centre for Transportation Research and Management, the Kendriya Vidyalaya of Ratlam and the Oil and Natural Gas Corporation of India. Following this a Pakistani group calling itself Zombie\_KSA hacked and defaced the Criminal Investigation Department website, a cyber security unit of the Andhra Pradesh state police, and removed the site’s information about 10 most wanted criminals. Soon after the Eastern railways attack, another Pakastani group, which is yet to be identified, hacked an Indian television station and State Bank of India. The website of Bank of India, one of the largest banks in India, was completely down on Christmas Eve.

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

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

Russia launched its war on Ukraine on 24 February 2022, but Russian cyber-attacks against Ukraine have persisted ever since Russia's illegal annexation of Crimea in 2014, intensifying just before the 2022 invasion. Over this period, Ukraine's public, energy, media, financial, business and non-profit sectors have suffered the most. Since 24 February, limited Russian cyber-attacks have undermined the distribution of medicines, food and relief supplies. Their impact has ranged from preventing access to basic services to data theft and disinformation, including through deep fake technology. Other malicious cyber-activity involves sending of phishing emails, distributed denial-of-service attacks, and use of data-wiper malware, backdoors, surveillance software and information stealers. Organisations and governments around the world have not been indifferent to the hybrid risks thus posed. EU-, US- and NATO-led initiatives have been carried out with the aim of neutralising cyberthreats and protecting essential infrastructure. As part of these initiatives, the EU has activated its Cyber Rapid Response Teams (a project under Permanent Structured Cooperation (PESCO) in the area of security and defence policy), to support Ukraine's cyber-defence. Non-government and private players have supported Ukraine through various cyber-resilience activities. Since the beginning of the invasion, a significant number of counter-attacks have been launched by independent hackers, affecting the Russian state, security, banking and media systems. The European Parliament has called for stepping up cybersecurity assistance to Ukraine and for making full use of the EU's cyber-sanctions regimes against individuals, entities and bodies responsible for or involved in the various cyber-attacks targeting Ukraine.

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