SC

The Global Threat of Cyberterrorism

www.yeniyolmun.org/committees

Dear Delegates,

It is with great excitement that we welcome you to Yeni Yol Model United Nations 2023! Our names are Rana Beril Gülcü and Yağmur Onarlı, and we are humbled by the opportunity to serve as your Secretaries-General for the 2nd Session of YYMUN.

The Secretariat team has been working diligently to ensure that all delegates will be given the opportunity to develop broader perspectives, voice their opinions on current global issues, and cooperate with others to produce effective resolutions. We expect that the topics covered in the committees will appeal to all the delegates' levels or more challenging in Intermediate and Advanced committees so that they may provide challenge, helpful guidance to your needs and assistance to improve your visions. After an eventful weekend full of diplomacy, debate, and delight, we wish you to leave our conference with the potential to become future leaders of our society.

This document will provide you with the Study Guide for your committee, which will enable you to comprehend the issue to be debated more easily. The entire Secretariat and Staff have committed countless hours to ensure that the substance and presentation of this document are of the highest quality, and that you are be supported with the most useful tools to succeed at the conference. Each Chair has worked over the past few months to provide you with the foundation necessary to continue your own exploration of the topic areas. We look forward to working with you to continue YYMUN's substantive excellence.

Apart from this document, you will also be able to access a number of additional documents that will aid in your preparations for the conference. We will provide you with the **Code of Conduct** that reviews some rules, principles and expectations, as well as our updated **Rules of Procedure**, which you can find on our website.

If you have any questions about this document, the other Guides, or your committee in general, please do not hesitate to contact us or your Under-Secretaries-General. We are truly excited to meet you all and are eager to address any concerns you may have before, during, or after the conference. I hope you enjoy reading the following Study Guide, and I cannot wait to see your solutions in YYMUN'23!

Yours in diplomacy,

Secretaries of General
Rana Beril Gülcü I Yağmur Onarlı

YYMUN’23 Study Guide of UNSC Committee

by Tuna Sinan Karasu and Yağmur Onarlı

The Idea of the Global Threat of Cyberterrorism

Cyberterrorism is a type of terrorism that uses the internet and computer networks to cause harm or disruption. Techniques used include hacking, phishing, and DDoS attacks, and goals range from causing panic to stealing information or causing physical harm.
Cyberterrorism can target various entities such as companies and governments. Measures to prevent and respond to cyberterrorism include cybersecurity laws, agencies, and international collaborations which, through means of collaboration, aim to tackle these attacks. Strong cybersecurity measures and awareness are essential for individuals and organizations to protect against cyber-attacks. Cyberterrorism requires ongoing attention and action from governments, organizations, and individuals worldwide.

More About the Committee

The United Nations Security Council (UNSC) is one of the six principal organs of the United Nations and is charged with the maintenance of international peace and security. Its establishment and nature are enshrined in Chapter V of the United Nations Charter. Its powers include the establishment of peacekeeping operations, the establishment of international sanctions, and the authorization of military action through Security Council resolutions; it is the only UN body with the authority to issue binding resolutions to member states.

The Security Council held its first session on 17 January 1946. It consists of fifteen members. The great powers that were the victors of World War II - Russia, the United Kingdom, and the United States - along with France and China, serve as the body's five permanent members. These permanent members can veto any substantive Security Council resolution, including those on the admission of new member states or candidates for Secretary-General. The Security Council also has 10 non-permanent members, elected on a 5 regional basis to serve two-year terms. The body's presidency rotates monthly between its members.

The UNSC was designed to address some of the flaws of the UN's spiritual predecessor, the League of Nations, which was often paralyzed as complete unanimity among its members was required to be able to act. The Security Council was designed to act as a quasi-executive for the UN and to be able to respond rapidly to international crises as and when they arose. This was not too dissimilar from the former League of Nations, which like the modern United Nations, had as its principal organs; a General Assembly of all members, an International (permanent) Court of Justice, and an Executive Council. However, unlike the League's Council, the United Nations Security Council has a far larger set of powers and enjoys a more comprehensive membership than the League's Executive Council. With the addition of the United States and the former Soviet Union as permanent members, the UNSC not only had unprecedented legal powers but also effectively controlled the balance of power in the world, with the ‘hard power’ and political will to act. The United Nations Security Council is, in many ways, a unique institution. It exercises legislative, judicial, and executive powers; operates with few legally binding checks and balances, and has even been described as 'unbound by law'.

The Council has broad powers to maintain international peace and security, most notably under Chapter VII of the UN Charter, and its decisions are binding on UN members. There are two systems of voting in the Security Council. On procedural matters the affirmative vote of any nine members is necessary, but on substantive matters, the nine affirmative votes required must include those of the five permanent members. This requirement of Big Five unanimity embodies the so-called veto. In practice, the council has, on most substantive matters, not treated an abstention by a permanent member as a veto. In two situations, however, those of recommending applicants for UN membership and of approving proposed amendments to the charter, the actual concurrence of all permanent members has been required. The veto has prevented much substantive action by the UN, but it embodies the reality that resolution of major crises requires the agreement of the major powers. Under the charter, the council may take measures on any danger to world peace. It may act upon the complaint of a member or of a non-member, on notification by the Secretary-General or by the General Assembly, or of its own volition. In general, the Council considers matters of two sorts. The first is "disputes" (or situations that may give rise to them) that might endanger peace. Here the council is limited to making recommendations to the parties after it has exhausted other methods of reaching a solution. In the case of more serious matters, such as "threats to the peace," "breaches of the peace," and "acts of aggression," the council may take enforcement measures.

These may range from full or partial rupture of economic or diplomatic relations to military operations of any scope deemed necessary. By the terms of the charter, the UN was forbidden to intervene in matters "which are essentially … domestic," but this limitation was not intended to hinder Security Council measures to prevent threats to peace. The charter was intentionally ambiguous regarding domestic issues that could also be construed as threats to peace and left a potential opening for intervention in domestic issues that threaten to have dangerous international repercussions.

Key Terms

Data Breach: A data breach is an issue regarding security in which sensitive or confidential information is apprehended, disclosed, or stolen by an unauthorized party.

Malware: software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Exploit kits: An exploit kit is a toolkit that attackers use to attack specific vulnerabilities in a system or code

Advanced persistent threats: An advanced persistent threat (APT) is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network to steal sensitive data over a prolonged period of time

Malicious code: Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches, or damage to a system.

Malicious cyber intrusion: For a malicious cyber intrusion to occur, a third party must gain access to unauthorized areas that house confidential information, core code, and application infrastructures**.**

Web application firewalls: A web application firewall (WAF) protects web applications from a variety of application layer attacks such as cross-site scripting (XSS), SQL injection, and cookie poisoning, among others.

Runtime application self-protection: Runtime Application Self Protection (RASP) is a security solution designed to provide personalized protection to applications. It takes advantage of insight into an application's internal data and state to enable it to identify threats at runtime that may have otherwise been overlooked by other security solutions.

Problems that can be triggered by Cyberterrorism:

1. **Disruption of essential services:** Cyber terrorists may target critical infrastructure, such as power grids, water systems, transportation systems, and emergency services, causing widespread disruption and chaos, therefore, leading to the failure of an essential part of society.
2. **Financial losses:** Cyberterrorism can lead to financial losses for individuals, businesses, and governments. Cybercriminals can steal sensitive financial information, such as credit card numbers and bank account details, and use it for fraudulent purposes. Furthermore, they can steal prominent information from the government, creating a national social breach.
3. **Physical harm:** Cyberterrorism can lead to physical harm in some cases, for example, cyberterrorists can gain access to critical infrastructure and disrupt essential services like hospitals or emergency response systems resulting in a great level of confusion and chaos.
4. **Political instability:** Cyberterrorism can cause political instability, especially when governments and government bodies are targeted. This can lead to military coups, unrest, protests, and other forms of social disruption.

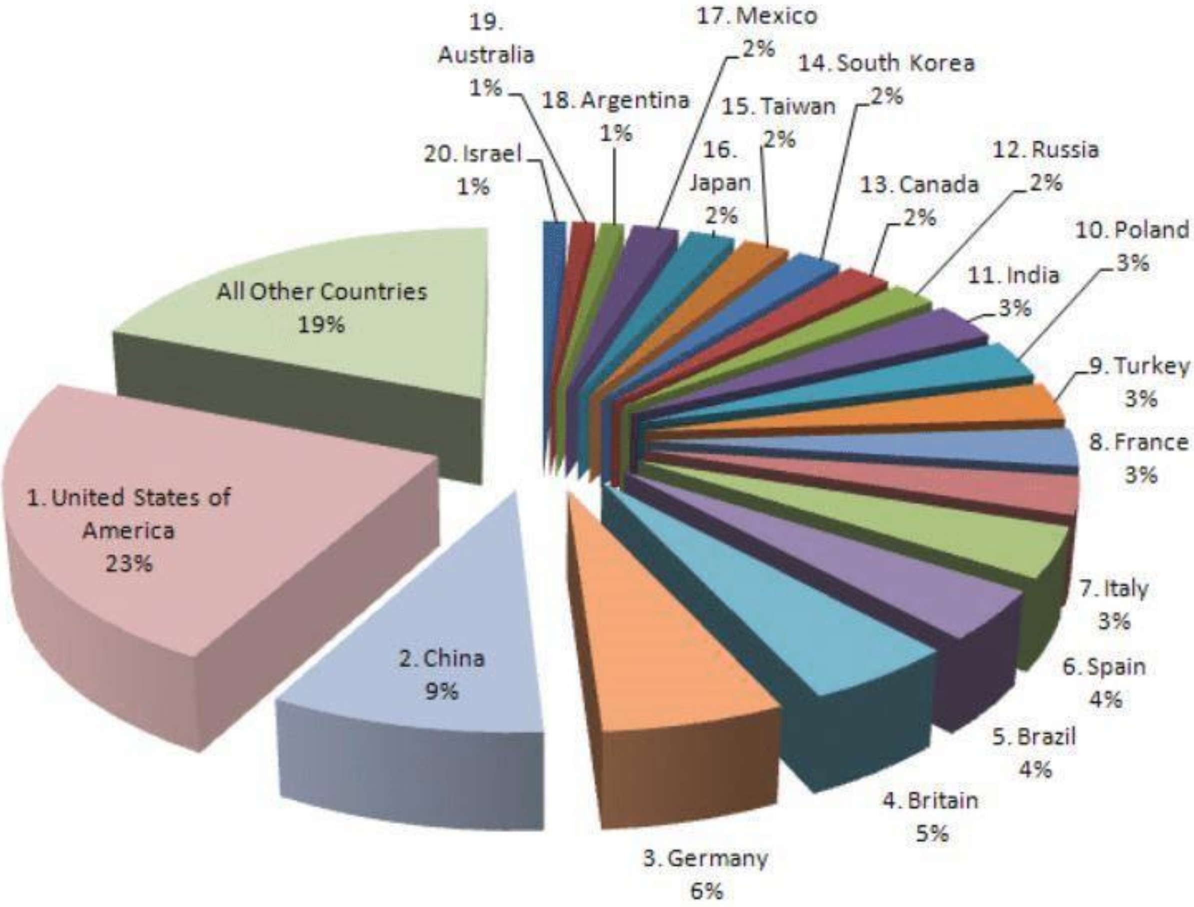
The History of Cyberterrorism

Cyberterrorism is a relatively new phenomenon, and its history is still unfolding. The term "cyberterrorism" first emerged in the 1990s when the internet became more widely accessible. Since then, there have been several notable instances of cyberterrorism that have had a significant impact on individuals, organizations, and governments. One of the earliest known instances of cyberterrorism occurred in 1996 when a group of hackers launched a series of attacks on the Pentagon and other government agencies in the United States. The attacks caused significant disruption, but no serious damage was done. Today, the threat of cyberterrorism remains a significant concern for governments, businesses, and individuals around the world. As technology continues to evolve, we will likely see new and more sophisticated forms of cyberterrorism emerge, making it more important than ever to remain vigilant and take steps to protect ourselves and our information online.

Prominent Cyber Terrorist Attacks from History:

- **The Biggest Password Leak yet: RockYou2021**
  - In June 2021, about 8.4 billion passwords leaked in the RockYou2021 attack. It was the largest breach since the Rock You site in 2009 which affected 32 million accounts.
- **Ukraine's power grid attack**
  - Ukraine’s power grid attack in 2015 was the first cyberattack on a power grid. As a result of the attack, around half of the homes in the Ivano-Frankivsk region of Ukraine were without power for a few hours.
- **2017 WannaCry ransomware attack**
  - One of the biggest ransomware attacks of all time took place in 2017, it affected around 200,000 computers in over 150 countries. To sum up, ransomware had a huge impact on several industries with a global cost of around 6 billion Pounds to fix.
- **Adobe Cyber Attack**
  - The Adobe cyber-attack was first thought to have breached the data of 2.9 million users (about the population of Connecticut). Moreover, it compromised the personal data of up to 38 million users (about twice the population of New York). Adobe claims that only the passwords and credit card information of the first 2.9 million users (about the population of Connecticut) were compromised, however, the remaining 35.1 million suffered the loss of their passwords and user IDs making it one of the greatest leaks of the century.

In conclusion, many problems can derive because of cyberterrorism such as disruption to essential services, grave financial losses, physical harm, and political instability in the case that the cyber-attack targets governments. Cyberterrorism is a concept that has developed in size during the expansion and familiarization of the internet. There have been many major and minor attacks in the past few decades which include the RockYou2021 attack, Ukraine's power grid attack, the 2017 Wanna Cry ransomware attack, and the Adobe cyber-attack.



Top 20 countries with the highest level of cyber terrorism in their respective percentages.

Case Study

The 2007 Estonia Cyber Attack

In response to Estonia's dispute with Russia over the relocation of the Bronze Soldier of Tallinn, an elaborate Soviet-era grave marker, as well as war graves in Tallinn, a series of cyberattacks began on 27 April 2007 and targeted websites of Estonian organizations, including the Estonian parliament, banks, ministries, newspapers, and broadcasters. Most attacks that impacted the public were distributed denial of service techniques, which could be carried out by a single person using a variety of strategies such as ping floods or by paying outrageous rentals for botnets that are commonly used to distribute spam. Larger news portals' webpages were also defaced, including the website of the Estonian Reform Party, and spammed with commentary. A "commissar" of the Kremlin-backed young people's group Nashi, Konstantin Goloskokov, claimed responsibility for what happened on March 10th, 2009. These various claims of responsibility have attracted criticism from specialists. The NATO Cooperative Cyber Defense Centre of Competence emerged as a direct result of recent cyberattacks.

Estonia's Response:

The Kremlin was swiftly suspected of being personally involved in the attacks by the Estonian state. Later, when Estonia's defense minister, Jaak Aaviksoo, noted that he had no proof connecting the cyberattacks to the Kremlin, it became obvious that the accusations were not entirely correct. In an interview with Estonia's Kanal 2 TV channel, he stated, "Of course, at the moment, I cannot state with certainty that the cyber-attacks have been planned by the Kremlin or other Russian government agencies." "Once more, it is not possible to say with certainty that orders came from the Kremlin or that a wish for something like that was expressed there as well," Russia termed the allegations "unfounded." Neither NATO nor European Commission experts were able to confirm the charges to find any proof of official Russian government participation. Since the attack, Estonia has advocated for increased cybersecurity protection and response protocol.

NATO'S Response:

NATO evaluated its internal internet safety and infrastructural measures in response to such threats. A report from the evaluation was delivered to the defense ministers of the Allies in October 2007. The NATO Cooperative Computer Defense Center of Excellence (CCDCOE) was established in May 2008 because of subsequent advances, including the development of a cyber defense doctrine.

The Tallinn Manual on the International Law Applicable to Cyber Warfare was also created due to the attacks. This research outlined the worldwide regulations that are thought to apply to the online world. Ninety-five "black-letter rules" addressing cyber conflicts are included in the guidebook. By incorporating current international legislation into cyber warfare, the Tallinn Manual has tried to establish an international standard in cyberspace.

Lessons Learned:

One of the biggest lessons emerging from this event is that in a modern conflict, cyber-attacks are becoming increasingly more common and dangerous. Any country with sufficiently well-developed network infrastructure is vulnerable to these attacks. Primitive cyber-attacks take very little time and effort to organize and defending against them is becoming more and more difficult. Under cover of the primitive and

noisy attacks, more professional intrusions can be performed to gain a foothold for further attacks.
There are several problems with using the Internet as a field of battle by lone hackers, terrorist groups, and states. First, the Internet spans the globe, thus a large-scale attack is likely to influence innocent bystanders in other countries as well as the target country. Therefore, some of these attacks could be classified as terrorist activity, since they target civilian systems in the hopes of getting more attention from the press. Second, the relative anonymity of the Internet allows for near-perfect deniability, as was the case in Estonia. All one must do is either originate the attack from or route the traffic through a country that is not willing to cooperate. This makes it almost impossible to bring the attackers to justice, especially when considering the lack of common international legal grounds for these new types of attacks and conflicts.

Third, a new phenomenon is currently emerging that could change the concept of information assurance radically. This phenomenon is the militarization of cyberspace. Most systems today are built with lone hackers and script kiddies in mind. But militaries are moving into cyberspace. What if all the nationally critical systems fall under a simultaneously concentrated cyber-attack from thousands of professional, well-trained, and equipped cyber attackers? In a war scenario, these attacks would most likely be complemented by physical destruction at some key sites, as well as special operations troops capturing others. The author believes that this could be devastating to any country with a developed network infrastructure. Organized military resistance could be knocked out overnight, in theory.

Types of Cyber Attacks

Cyber-attacks vary drastically throughout the following categories:

DoS and DDoS Attacks:

A denial-of-service (DoS) attack floods a server with traffic, making a website or resource unavailable. A distributed denial-of-service (DDoS) attack is a DoS attack that uses multiple computers or machines to flood a targeted resource. Both types of attacks overload a server or web application to interrupt services.

As the server is flooded with more Transmission Control Protocol/User Datagram Protocol (TCP/UDP) packets than it can process, it may crash, the data may become

corrupted, and resources may be misdirected or even exhausted to the point of paralyzing the system.
The principal difference between a DoS attack and a DDoS attack is that the former is a system-on-system attack, while the latter involves several systems attacking a single system. There are other differences, however, involving either their nature or detection, including:

Ease of detection/mitigation: Since a DoS comes from a single location, it is easier to detect its origin and sever the connection. A profitable business can do this. On the other hand, a DDoS attack comes from multiple remote locations, disguising its origin.

Speed of attack: Because a DDoS attack comes from multiple locations, it can be deployed much faster than a DoS attack originating from a single location. The increased speed of attack makes detecting it more difficult, meaning increased damage or even a catastrophic outcome.

Traffic volume: A DDoS attack employs multiple remote machines (zombies or bots), which means that it can send much larger amounts of traffic from various locations simultaneously, overloading a server rapidly in a manner that eludes detection.

Manner of execution: A DDoS attack coordinates multiple hosts infected with malware (bots), creating a botnet managed by a command-and-control (C&C) server. In contrast, a DoS attack typically uses a script or a tool to attack a single machine.
Tracing of source(s): The use of a botnet in a DDoS attack means that tracing the actual origin is much more complicated than tracing the origin of a DoS attack.

MITM Attacks:

MITM stands for "Man-in-the-Middle" attack, which is a type of cyber-attack in which an attacker intercepts communication between two parties, such as a client and a server, without their knowledge or consent.

In a typical MITM attack, the attacker positions themselves between the client and the server and intercepts and alters the communication between them. The attacker can then steal sensitive information, such as login credentials, personal information, or financial data, or can even inject malicious code into the communication to gain control of the client or server.

MITM attacks can be carried out through various methods, including packet sniffing, ARP spoofing, DNS spoofing, and session hijacking. These attacks can be particularly dangerous in public Wi-Fi networks or unsecured websites, where attackers can easily intercept unencrypted data.

To prevent MITM attacks, it is important to use secure communication protocols, such as HTTPS, and to be cautious when using public Wi-Fi networks or visiting unfamiliar websites. It is also recommended to use two-factor authentication and to keep software and security patches up to date to minimize the risk of vulnerabilities

Phishing Attacks:

Phishing refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information, or other, important data to utilize or sell the stolen information. By masquerading as a reputable source with an enticing request, an attacker lures in the victim to trick them, similarly to how a fisherman uses bait to catch a fish.

How is phishing carried out?

The most common examples of phishing are used to support other malicious actions, such as on-path attacks-site scripting attacks. These attacks typically occur via email or instant message and can be broken down into a few general categories. It’s useful to become familiar with a few of these different vectors of phishing attacks to spot them in the wild.

Advanced-fee scam:

This common email phishing attack is popularized by the “Nigerian prince” email, where an alleged Nigerian prince in a desperate situation offers to give the victim a large sum of money for a small fee upfront. Unsurprisingly, when the fee is paid, no large sum of money ever arrives. The interesting history is that this type of scam has been occurring for over a hundred years in different forms; it was originally known in the late 1800s as the Spanish Prisoner scam, in which a con artist contacted a victim to prey on their greed and sympathy. The con artist is allegedly trying to smuggle out a wealthy Spanish prisoner, who will reward the victim handsomely in exchange for the money to bribe some prison guards.

This attack (in all its forms) is mitigated by not responding to requests from unknown parties in which money has to be given to receive something in return. If it sounds too good to be true, it probably is. A simple Google search on the theme of the request or some of the text itself will often bring up the details of the scam.

Account deactivation scam:

By playing off the urgency created in a victim who believes an important account is going to be deactivated, attackers can trick people into handing over important information such as login credentials. Here’s an example: the attacker sends an email that appears to come from an important institution like a bank, and they claim the victim’s bank account will be deactivated if they do not act quickly. The attacker will then request the login and password to the victim’s bank account to prevent deactivation. In a clever version of the attack, once the information is entered, the victim will be directed to the legitimate bank website so that nothing looks out of place.

This type of attack can be countered by going directly to the website of the service in question and seeing if the legitimate provider notifies the user of the same urgent account status. It’s also good to check the URL bar and make sure that the website is secure. Any website requesting a login and password that is not secure should be seriously questioned, and nearly without exception should not be used.

Website forgery scam:

This type of scam is commonly paired with other scams such as the account deactivation scam. In this attack, the attacker creates a website that is virtually identical to the legitimate website of a business the victim uses, such as a bank. When the user visits the page through whatever means, be it an email phishing attempt, a hyperlink inside a forum, or via a search engine, the victim reaches a website that is believed to be a legitimate site instead of a fraudulent copy. All information entered by the victim is collected for sale or other malicious use.

In the early days of the Internet, these types of duplicate pages were easy to spot due to their shoddy craftsmanship. Today the fraudulent sites may look like a picture-perfect representation of the original. By checking the URL in the web browser, it is usually easy to spot fraud. If the URL looks different than the typical one, this should be considered highly suspect. If the pages are listed as insecure and HTTPS is not on, this is a red flag and virtually guarantees the site is either broken or a phishing attack.

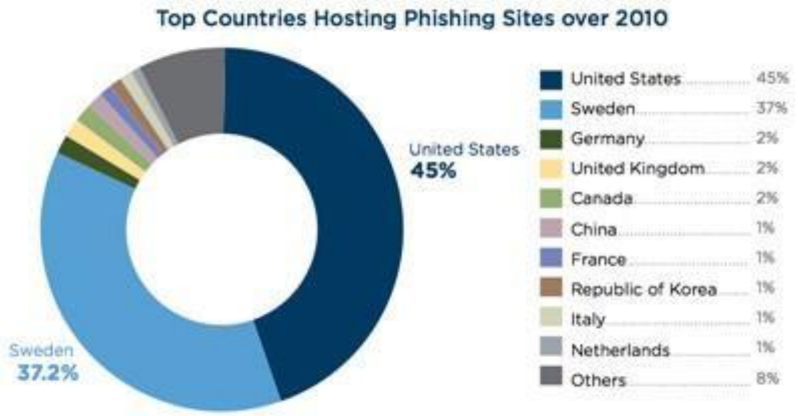
Spear phishing attack:

This type of phishing is directed at specific individuals or companies, hence the term spear phishing. By gathering details or buying information about a particular target, an attacker can mount a personalized scam. This is currently the most effective type of phishing, and accounts for over 90% of the attacks.

Whaling-phishing attacks:

For attacks that are directed specifically at senior executives or other privileged users within businesses, the term whaling is commonly used. These types of attacks are typically targeted with content likely to require the attention of the victim such as legal subpoenas or other executive issues.

Another common vector of this style of attack is whaling scam emails that appear to come from an executive. A common example would be an email request coming from a CEO to someone in the finance department requesting immediate help in transferring money. Lower-level employees are sometimes fooled into thinking the importance of the request and the person it’s coming from supersedes any need to double-check the request’s authenticity, resulting in the employee transferring large sums of money to an attacker.



Ransomware:

Ransomware is a type of malware attack in which the attacker locks and encrypts the victim’s data, and important files and then demands payment to unlock and decrypt the data.

This type of attack takes advantage of human, system, network, and software vulnerabilities to infect the victim’s device—which can be a computer, printer, smartphone, wearable, point-of-sale (POS) terminal, or other endpoints.

WannaCry:

WannaCry is encrypting ransomware that exploits a vulnerability in the Windows

SMB protocol and has a self-propagation mechanism that lets it infect other machines. Wanna Cry is packaged as a dropper, a self-contained program that extracts the encryption/decryption application, files containing encryption keys, and the Tor communication program. It is not obfuscated and is relatively easy to detect and remove. In 2017 WannaCry spread rapidly across 150 countries, affecting 230,000 computers and causing an estimated $4 billion (about $12 per person in the US) in damages.

Cerber:

Cerber is ransomware-as-a-service (RaaS) and is available for use by cybercriminals, who carry out attacks and spread their loot with the malware developer. Cerber runs silently while it is encrypting files and may try to prevent antivirus and Windows security features from running, to prevent users from restoring the system. When it successfully encrypts files on the machine, it displays a ransom note on the desktop wallpaper.

Locky:

Locky can encrypt 160 file types, primarily files used by designers, engineers, and testers. It was first released in 2016. It is primarily distributed by exploit kits or phishing—attackers send emails that encourage the user to open a Microsoft Office Word or Excel file with malicious macros, or a ZIP file that installs the malware upon extraction.

Cryptolocker:

Crypto locker was released in 2021 and affected over 500,000 computers. It typically infects computers through email, file-sharing sites, and unprotected downloads. It not only encrypts files on the local machine, but can also scan mapped network drives, and encrypt files it has permission to write to. New variants of Crypto locker can elude legacy antivirus software and firewalls.

Not Petya and Petya:

Petya is ransomware that infects a machine and encrypts an entire hard drive, by accessing the Master File Table (MFT). This makes the entire disk inaccessible, although the actual files are not encrypted. Petya was first seen in 2016 and was spread mainly through a fake job application message linking to an infected file stored in Dropbox. It only affected Windows computers.

Petya requires the user to agree to permit it to make admin-level changes. After the user agrees, it reboots the computer, and shows a fake system crash screen, while it starts encrypting the disk behind the scenes. It then shows the ransom notice. The original Petya virus was not highly successful, but a new variant, named NotPetya by Kaspersky Labs, proved to be more dangerous. Not Petya is equipped with a propagation mechanism and can spread without human intervention.

Not Petya originally spread using a backdoor in the accounting software used widely in Ukraine and later used Eternal Blue and Eternal Romance, vulnerabilities in the Windows SMB protocol. Not Petya encrypts not only the MFT but also other files on the hard drive. While encrypting the data, it damages it in such a way that it cannot be recovered. Users who pay the ransom cannot get their data back.

Ryuk:

Ryuk infects machines via phishing emails or drive-by downloads. It uses a dropper, which extracts a trojan on the victim’s machine and establishes a persistent network connection. Attackers can then use Ryuk as a basis for an advanced persistent threat (APT), installing additional tools like keyloggers, and performing privilege escalation and lateral movement. Ryuk is installed on each additional system the attackers gain access to.

Once the attackers have installed the trojan on as many machines as possible, they activate the locker ransomware and encrypt the files. In a Ryuk-based attack campaign, the ransomware aspect is only the last stage of the attack, after the attackers have already done damage and stolen the files they need.

SQL Injection Attack:

An SQL injection attack consists of an insertion or injection of a SQL query via the input data from the client to the application. SQL commands are injected into data-plane input that affects the execution of predefined SQL commands. A successful SQL injection exploit can read sensitive data from the database, modify database data (viz., insert, update, or delete), execute administrative operations on the database, recover the content of a file present in the database management system, and even issue commands to the operating system in some instances.

If a web application or website uses SQL databases like Oracle, SQL Server, or MySQL, it is vulnerable to an SQL injection attack. Hackers use SQL injection attacks to access sensitive business or personally identifiable information (PII), which ultimately increases sensitive data exposure

SQL injection attacks are one of the most prevalent among OWASP’s top 10 vulnerabilities and one of the oldest application vulnerabilities. One recent report lists it as the third most common serious vulnerability.

Why Do Attackers Perform an SQL Injection Attack?

To perform an SQL injection attack, an attacker must locate a vulnerable input in a web application or webpage. When an application or webpage contains a SQL injection vulnerability, it uses user input in the form of an SQL query directly. The hacker can execute a specifically crafted SQL command as a malicious cyber intrusion. Then, leveraging malicious code, a hacker can acquire a response that provides a clear idea about the database construction and thereby access all the information in the database.

SQL serves as a way of communication with the database. SQL statements are used to retrieve and update data in the database. Attackers use malicious SQL statements in the input box, and in response, the database presents sensitive information. This exploit of security aims at gaining access to the unauthorized data of a website or application. Several websites and web applications store data in SQL databases. For any of these applications, it becomes essential to perform vulnerability testing to ensure there are no loopholes for executing SQL injection.

What Are the Risks Associated with SQL Injection?

In an SQL injection attack, an application interprets data submitted by a cybercriminal as a command and responds with sensitive details. An SQL injection can result in several risks that may pose severe threats to the organization. Following are some of the scenarios:

a) When a hacker performs an SQL injection to delete data or tables from the database. In this case, even if there are database backups, deleting the data can affect the application’s availability until the database can be restored. Further, backups may not include recent data.

b) Attackers use SQL injection to alter or update data in the database and add additional data. For instance, in the case of a financial application, an attacker can use SQL injection to change account balances. Even worse, attackers can gain administrative rights to an application database.

c) The most common risk of an SQL injection attack is the theft of user data. Email addresses, login credentials, and personally identifiable information (PII) can be stolen and sold on the dark web. Therefore, a successful SQL injection poses a threat not only to the organization but also to its users.

Even after 20 years of SQL injection discovery, it remains one of the primary concerns when it comes to data breaches and the security of data. Recent attack trending analysis shows SQL injection attacks up to 47%

How an SQL Injection Attack Is Performed

SQL injection is performed by using a structured query that instigates the desired response. The response is essential for the attacker to understand the database architecture and to access the secure information of the application. An attacker may perform SQL injection with the following approaches:

In-band SQL injection:
In-band SQL injection is the most frequent and commonly used SQL injection attack. The transfer of data used in in-band attacks can either be done through error messages on the web or by using the UNION operator in SQL statements. There are two types of in-band SQL injection: union-based and error-based SQL injection.

Union-based SQL injection:
When an application is vulnerable to SQL injection and the application's responses return the results for a query, attackers use the UNION keyword to retrieve data from other tables of the application database.

Error-based SQL injection:
The error-based SQL injection technique relies on error messages thrown by the application database servers. Here, attackers use the error message information to determine the entities of the database.

Inferential SQL injection:
Inferential SQL injection is also known as a blind SQL injection attack. In a blind SQL injection attack, after sending a data payload, the attacker observes the behavior and responses to determine the data structure of the database.
There are two types of blind or inferential SQL injection attacks: Boolean and time-based.

Treaties That Have Been Signed in The Past Regarding Cyber Terrorism Attacks:

United Nations Cybercrime Treaty The United Nations is currently negotiating a major Cybercrime Convention that has the potential to substantively reshape international criminal law and bolster cross-border police surveillance powers to access and share users' data, implicating the human rights of billions of people worldwide.
To coordinate the new Convention, the UN General Assembly passed Resolution

74/247 in December 2019 and established the Ad Hoc intergovernmental committee to
“Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purpose.” The Ad Hoc Committee held its first negotiating session on February 28th, 2022, aiming to finalize the text by early 2024 amidst contentious negotiations among Members States’ disagreement about the broad scope of the Treaty. The proposed Convention will likely deal with several topics such as substantive cybercrime provisions, international cooperation, access to potential digital evidence by law enforcement authorities, including across borders, as well as human rights and procedural safeguards. The United Nations Office on Drugs and Crime (UNODC), through the Organized Crime and Illicit Trafficking Branch, Division for Treaty Affairs, serves as Secretariat for the Ad Hoc Committee.

The stakes are high, so the treaty's scope must be narrow, and human rights safeguards must be a priority. EFF is a registered NGO actively fighting to protect human rights online, attending and speaking in meetings via submissions, oral statements, and joint coalition letters.

The permanent member's laws on cyber terrorism:

Cyber Security Laws of China:

China enacted the CSL on November 7, 2016. The CSL came into force on June 1, 2017, intending to establish a uniform regulatory regime for cybersecurity and data protection in China.

Multiple government agencies are involved in implementing the CSL, including:

- Cyberspace Administration of China (CAC) and its local offices
- Ministry of Public Security (MPS) and local Public Security Bureaus
- Ministry of Industry and Information Technologies (MIIT) and local Telecommunication Bureaus
- Other sectoral regulators, such as:
    - Ministry of Science and Technology (MOST)
    - National Energy Administration (NEA)
    - China Banking and Insurance Regulatory Commission (CBIRC)

While some provisions have yet to be implemented, the CSL is currently being enforced in the following ways:

- It imposes baseline data protection and cybersecurity obligations on network operators, including compliance obligations with Multi-Level Protection Scheme (MLPS) rules
- It provides a regulatory framework for critical information infrastructure (CII) operators
- It establishes a cybersecurity review mechanism for network products and services that may put China’s national security at risk
- It establishes presale certification requirements for critical network equipment and network security products
- It imposes requirements to protect data collected in the operations of networks
- It stipulates a wide array of sanctions and penalties for non-compliant companies

Cyber Security Laws of France:

The French Data Protection Act (Loi Informatique et Libertés): This act was first passed in 1978, and it regulates the collection, processing, and storage of personal data by organizations. The law was updated in 2018 to align it with the EU's General Data Protection Regulation (GDPR).

The Military Programming Law (Loi de Programmation Militaire): This law sets out the framework for cybersecurity in France's military and intelligence agencies. It requires these agencies to take measures to protect their IT systems from cyber-attacks and report any incidents to the authorities.

The Network and Information Security (NIS) Directive: This directive is a European Union regulation that aims to improve the cybersecurity of critical infrastructure across the EU. France has implemented the directive through its national legislation.

The Cybersecurity Information Sharing Act (Loi de Programmation Militaire): This act encourages the sharing of cybersecurity threat intelligence between public and private organizations. It also establishes a national platform for sharing such information.

The French Penal Code: This code contains provisions that criminalize cybercrime, including unauthorized access to computer systems, hacking, and the distribution of malware.

The Digital Republic Act (Loi pour une République Numérique): This act was passed in 2016 and contains provisions related to cybersecurity, including the obligation for companies to notify customers in the event of a data breach.

Cyber Security Laws of the Russian Federation:

1. Unauthorized access to law-protected computer information in the electronic computers, their systems or networks, or on the machine carriers resulted in erasing, blocking, or copying computer information, disturbing the work of electronic computers, their systems or networks is punished with a fine from two hundred to five hundred minimum wages, condemned person’s wages or another income within the term from two to five months, refinery works within the term from six months to one year, or imprisonment within up to two years.

2. The same action carried out by a group of persons in the prior agreement or an organized group or a person abusing his official position and having equal access to electronic computers, their systems, or networks is punished with a fine from five hundred to eight hundred minimum wages, condemned person’s wages or another income within the term from five to eight months, refinery works within the term from one to two years, arrest within the term from three to six months or imprisonment within up to five years.

Article 273. Production, use, and spread of detrimental electronic computer programs

1. Production of electronic computer programs or introduction of changes into current programs resulted in erasing, blocking, modifying or copying information, disturbing the work of electronic computers, their systems or networks, and use or spread of these programs are punished with imprisonment within up to three years with fine from two hundred to five hundred minimum wages or condemned person’s wages or another income within the term from two to five months.
2. The same actions entailed serious consequences through imprudence are punished with imprisonment within the term of three to seven years.

Article 274. Violation of electronic computer, system or network operating rules 1. Violation of electronic computer, system, or network operating rules on the part of a person having access to electronic computers, their systems, or networks resulting in erasing, blocking, or modifying law-protested information and causing considerable damage is punished with denial of particular position or activity privileges within up to five years, obligatory works within the term from one hundred and eighty to two hundred hours or freedom limitation within up to two years.

2. The same action entailed serious consequences through imprudence and is punished with imprisonment within up to four years.

Cyber security laws of the United Kingdom:

The Data Protection Act 2018: This act replaced the Data Protection Act 1998 and incorporated the EU's General Data Protection Regulation (GDPR) into UK law. It sets out rules on how personal data should be collected, processed, and stored. The Computer Misuse Act 1990: This act makes it illegal to access computer systems without authorization or to create and distribute malware.

The Network and Information Systems Regulations 2018: These regulations implement the EU's Network and Information Systems Directive (NISD) into UK law. They require certain organizations to implement security measures to protect against cyber-attacks and report any incidents.

The Investigatory Powers Act 2016: This act grants authorities the power to access and monitor electronic communications data to prevent and investigate crime and terrorism.

The Cyber Security Information Sharing Partnership (CiSP): This is a government-run platform that enables businesses and organizations to share cyber threat information and best practices.

The National Cyber Security Centre (NCSC): The NCSC is a government agency responsible for providing cybersecurity guidance, support, and advice to businesses and organizations across the UK.

Cyber security laws of the United States of America:

Computer Fraud and Abuse Act (CFAA): This law makes it illegal to access a computer without authorization or to use a computer to commit fraud or cause damage to another computer system.

Electronic Communications Privacy Act (ECPA): This law regulates the interception and monitoring of electronic communications and provides guidelines for the government's use of electronic surveillance.

Cybersecurity Information Sharing Act (CISA): This law encourages information sharing about cyber threats between private companies and the government. Gramm-Leach-Bliley Act (GLBA): This law requires financial institutions to protect consumers’ personal information.

Health Insurance Portability and Accountability Act (HIPAA): This law mandates that healthcare providers protect patients' personal and medical information.

General Data Protection Regulation (GDPR): Although not a U.S. law, GDPR is a regulation that applies to all organizations that handle the personal data of EU citizens.

Questions a Resolution Paper Should Cover:

Enhance Cybersecurity Measures: One of the most effective ways to combat cyberterrorism is to improve cybersecurity measures. This includes regular software updates, strong password policies, encryption of sensitive data, and implementation of firewalls and intrusion detection systems.

Increase Public Awareness: Raising public awareness about the dangers of cyberterrorism can help people take appropriate measures to protect themselves and their organizations. Governments and security agencies can run awareness campaigns to educate the public on best practices to avoid cyber-attacks.

Collaboration and Information Sharing: Collaboration between different stakeholders including governments, international organizations, the private sector, and individuals is crucial to combat cyber terrorism. This includes sharing information on cyber threats, vulnerabilities, and countermeasures this can be achieved through the common body of the United Nations.

Cyber Defense and Offensive Strategies: Governments can develop cyber defense and offensive strategies to detect and neutralize cyber terrorist threats. This includes investing in technology to identify and track potential cyber terrorists and their activities.

Establish International Agreements: International agreements can be established to coordinate efforts among countries to combat cyber terrorism. This includes cooperation between law enforcement agencies and international organizations to develop effective strategies and share information.

Delegates must not forget to keep in mind the past of the cyberattack relations between each other.

Bibliography

International Centre for Defence Studies (ICDS) (2007) ”Moskva käsi Tallinna rahutustes. Rahvusvahelise kaitseuuringute keskuse kiirülevaade 7. mail”, Sõdur, No

2, pp 4-8. (Moscow’s Hand in the Tallinn Riots. A Quick Overview by the International Centre for Defence Studies on 7th of May)

- https://www.cloudflare.com/learning/access-management/phishing-attack/
- https://www.imperva.com/learn/application-security/ransomware/
- https://www.contrastsecurity.com/glossary/sql-injection
- https://www.cybercrimelaw.net/Cybercrimelaw.html
- https://www.eff.org/issues/un-cybercrime-treaty