TABLE OF CONTENTS

Letter From Under Secretary General

I am Yiğit Efe Dadaş, a 11th grade student at Tevfik Ileri Anatolian Religious High School, and I am welcoming you to ULTEK'25. I will be serving as the Under Secretary General of the Cybersecurity Council. I hope the 3 days you will experience in this conference will be great. This document will help you to learn fundamentals of cybersecurity, current and past incidents and gain you a better perspective for the council. Make sure you read at least once before the conference, otherwise you may struggle at the council.

Our Council is going to have discussions on carrying cybersecurity one step ahead, possible solutions for the current digital operations, and taking ethics into account while practicing cybersecurity. Cybersecurity is a critical matter, particularly for our day. We have to keep moving forward while protecting cyber environments, technology, and all the rights. I hope our council will help us to have a point of view on this topic.

In conclusion, I hope these 3 days will stay a wonderful memory for all of us. Please do not hesitate to contact me if you have any question marks in your mind about the commission, agenda item or anything else related to our council.

My e-mail: 1525.yigit@gmail.com

Best Regards,

Yiğit Efe Dadaş

Introductory Unit

1.1 Introduction to the Cybersecurity Council

Cybersecurity is the practice of protecting the networks, computer systems, and programs from digital attacks. Throughout computer history, humanity has encountered various threats, whether malicious or just experimental. However, professionals have always overcome the issues with very few exceptions. Thanks to them, computer science and cybersecurity have evolved to where they are today. In the Cybersecurity Council, alongside the agenda item, the representatives are expected to discuss the current obstacles the cyber world is facing and find solutions for them. Furthermore, it is a mission of this commission to take cybersecurity one step ahead while taking the future of cybersecurity into account.

Additionally, one of the other duties of our council is to write an official document consisting of each dilemma and issue that has been discussed in the commission, in the final.

UNIT 2: TECHNICAL UNIT

2.1Fundamentals of Cybersecurity and Brief History

2.1.1 Brief History of Cybersecurity

The Rise of Cybersecurity

In 1946, the first computer, ENIAC, was exposed to the public. Although earlier computing devices, such as Charles Babbage's Analytical Engine, had been conceptualized, this was the first complex machine capable of performing high-level calculations at unprecedented speed. ENIAC's creation was driven primarily by wartime needs, especially to calculate artillery firing tables for the United States of America during World War II. The construction required over 17,000 vacuum tubes, and it occupied approximately 167 square meters. The scale of sources used for this construction demonstrates technological limitations and the ambitious scale of early computing. Its successful operation not only revolutionized data processing but also opened a path for future developments in the digital world, ultimately directing the field of computer science and, decades later, the emergence of cybersecurity as a discipline. In the

years following ENIAC's debut, the computer world evolved so fast. Year by year, moving from massive complex machines towards interconnected systems. While the computers were developing rapidly, these systems concerned only physical security. The 1960s and 1970s witnessed the birth of computer networking, most importantly through the creation of ARPANET in 1969, which changed the security landscape from securing only the machines to protecting the data traveling across vast digital connections.

The roots of cybersecurity can be traced back to the first years of computer networking, decades before the term "cybersecurity" entered our lives. In the 1960s, computers were large, expensive, and mostly isolated systems primarily used by government agencies, research institutions, and large corporations. As previously mentioned, security concerns at this time were only focused on physical access to ensure that unauthorized individuals could not approach or gain access to these machines. Software-based systems were rudimentary at that time, as most systems were not connected to one another. The first real shift in the nature of security concerns occurred in 1969 with the creation of ARPANET, the precursor of the modern internet, funded by the United States Department of Defense's Advanced Research Projects Agency (ARPA). It linked computers across various institutions, enabling remote access and data exchange. This connectivity was revolutionary for its time, but it brought in its wake some new risks, not from physical trespassers but from malicious actors who exploited the network.

In 1971, the first computer virus appeared, "Creeper" written by Bob Thomas. Although it was called the first virus in computer science history, it was just a harmless experiment rather than a malicious cyberattack. The program was designed to move between computers on ARPANET, displaying the message "I am the creeper, catch me if you can." It was then followed by the "Reaper" credited as the first antivirus software, which was specially programmed to remove Creeper from systems. These first programs were non-destructive. However, these events demonstrated the risks of self-replicating code spreading across connected systems. In the same year, Ray Tomlinson introduced the first e-mail program for ARPANET, including the iconic "@" symbol, marking the beginning of networked digital communication.

During the early 1970s, ARPANET usage was expanded, and there were additional protocols developed to facilitate remote operations and file management. In 1973, Telnet was

introduced as a remote terminal product, allowing users to reach and log into distant computers. Telnet transmitted data, including passwords, in plain text, making it highly vulnerable to interception. In parallel, FTP (File Transfer Protocol) was implemented to enable file exchanges over the network. Despite its utility, this protocol lacked encryption, and it made the files open for unauthorized access. These protocols highlighted the growing tension between developing network functionality and the need for security mechanisms.

The mid-1970s witnessed further developments in network infrastructure. X.25 Protocol was standardized in 1974 to establish a framework for packet-switched communication that would later serve as the basis for public data networks. X.25 provided more reliable connections and paved the way for global network expansion, but also introduced additional vectors for potential cyber attacks. Whitfield Diffie and Martin Hellman recognized the increasing complexity of networked communications and then introduced public key cryptography in 1976. Public key cryptography utilized a pair of mathematically linked keys, a public key for encrypting messages and a private key for decryption, unlike traditional symmetric encryption, where the same key is utilized for both encryption and decryption. This breakthrough enabled secure communications over unsecured networks, and it later provided the foundation for modern digital signatures, secure e-mails, and later protocols like SSL/TLS. Public cryptography represents a milestone for cybersecurity, demonstrating that security could be built into the very mechanisms of network communication, not only applied externally.

The late 1970s brought TCP/IP's (Transmission Control Protocol/Internet Protocol) foundation. TCP/IP standardized the way networks routed information, forming the backbone of what would become the modern internet. On the 1st of January, 1983, TCP/IP culminated in widespread adoption by being implemented on all the host computer systems that were connected to the ARPANET. Alongside this development, the Domain Name System (DNS) was implemented in 1983, translating the human-readable domain names into numerical IP addresses. Although these technologies brought more usability and connectivity, they introduced new vulnerabilities. For instance, the spread of BSD UNIX systems with TCP/IP stacks exposed systemic security gaps that would later be exploited by malicious software. These

As personal computing emerged in the early 1980s, cybersecurity obstacles multiplied. In 1982, the “Elk Cloner” virus demonstrated that self-replicating code spread wildly through sloppy disks, even outside of institutional networks. In 1986, the Brain virus targeted MS-DOS systems, marking the first PC malware accident in cybersecurity history. These developments throughout history coincided with legislative action; the U.S. Congress passed the Computer Fraud and Abuse Act (CFAA) in 1986, criminalizing the unauthorized access to computer systems. All together, these events underscored the dual necessity of technical defenses and legal frameworks to protect digital sources.

The year 1988 marked a watershed in cybersecurity history with the Morris Worm. Written by graduate student Robert Tappan Morris, the worm exploited the vulnerabilities in UNIX systems to propagate across the nascent Internet. While Morris claimed the experiment was intended to measure network size, a code flaw caused it to replicate uncontrollably, creating a denial-of-service effect on thousands of systems. The incident emphasized both the fragility of interconnected systems and the urgent need for organized response mechanisms. Consequently, the first Computer Emergency Response Team (CERT) was established, providing a coordinated framework for rapid response to incidents and knowledge sharing.

Concurrently, the late 1980s witnessed the development of both network defenses and deceptive attack methods. Firewalls introduced between 1988 and 1989 represented the first dedicated systems for monitoring and filtering network traffic, preventing unauthorized access to personal and private resources. At the same time, Trojan Horse attacks proliferated, where the software appeared legitimate but concealed harmful functionalities. These Trojans exploited user trust and demonstrated that these security threats could be embedded within ostensibly safe programs. Together, the advent of firewalls and the rise of Trojan Horse attacks reflected a new era of cybersecurity where defense systems were necessary not only against external attacks but also for insidious internal attack programs hidden within legitimate actions.

By the end of the 1980s, cybersecurity had transformed from a niche technological concern into a recognized essential discipline. Technology shifted from safeguarding isolated hardware to defending complex, interconnected network systems against an expanding array of threats. Early incidents, from harmless experiments like Creeper to disruptive attacks like the Morris Worm and Brain virus, illustrated both the potential and peril of networked computing. The foundation laid during these decades, with encryption mechanisms, legal

frameworks, network protocols, and early defensive technologies, set the stage for the explosive growth of cybersecurity challenges in the 1990s and later. These early incidents served as lessons for later practices, improvements on network infrastructures, and developments in cybersecurity frameworks.

Cybersecurity in the 1990s and Beyond

The 1990s marked a significant turning point in cybersecurity history. Personal computing spread widely with explosive speed globally, and network and communication technologies developed rapidly. Alongside these, the scale and sophistication of cyber threats expanded with a snowball effect. Malicious actors and security professionals were entering a new era where the cyber threats no longer targeted isolated network systems but instead targeted complex interconnected network systems.

The Rise of the Internet, Network Exploits and Cryptographic Foundations

The early 1990s witnessed the rapid adoption of the World Wide Web and standardized internet protocols. This period also experienced the first large-scale cyber intrusion that targeted not only technical infrastructure but also public trust. In 1994, one person named Kevin Mitnick, who would later make a name for himself in the cyber world by the crimes he committed, hacked the cellular network, exploited the vulnerabilities of digital switching systems, and then penetrated corporate networks. This incident was one of the most prominent incidents of the early 1990s and was extensively covered by the media, becoming symbolic of the growing challenges law enforcement faced in combating cybercrime.

On the other hand, the foundations of modern secure communication were being established. For instance, the implementation of Secure Sockets Layer (SSL), later Transport Layer Security (TLS), both following Public Key Cryptography (PKC), enabled encrypted data transmission over the internet, leading e-commerce to rise as it allowed the safe transmission of sensitive data, such as payment information, laying the groundwork for the digital economy.

Mid and late 1990s: Malware Evolution and Global Connectivity Risks

By the mid and late 1990s, internet usage was expanding to homes, businesses, and public institutions. However, this expansion brought in its wake an increased attack surface. Malicious malware such as the Melissa Virus (1999) demonstrated the new potential risks of

disruptive e-mail based attacks, hiding the malicious code through Microsoft Word documents and overwhelming the corporate e-mail servers. Nearly at the same time, first large-scale Distributed Denial of Service (DDoS) attacks began to emerge, aiming at corporate, university and institution networks.

This era also witnessed the commercialization of cybersecurity tools. Firewalls often integrated with Intrusion Detection Systems (IDS) became an essential parts of corporate networks. Antivirus Softwares became more efficient against polymorphic threats, marking a shift from reactive to more proactive defense mechanisms.

2000s:Internet Becoming a Critical Infrastructure

The new decade started with some series of new major cyber incidents that highlighted the vulnerability of new emerging technology.For instance, The “ILOVEYOU” worm (2000), one of the most impactful incidents of 2000s, spreading via e-mails with the subject line "I love you” , infected millions of systems across the world causing huge damages and prompting regulations on digital forensics and incident reporting.

Cybercriminal Organizations became more structured, several states took new actions on cybersecurity, developing underground economies for stolen data, malware kits, and exploit tools. Botnets such as “Storm” and “Conficker” infected millions of systems paving the way for large-scale spam campaigns and DDoS attacks. The increasing complexity of cyber threats demonstrated the need for international cooperation, leading international frameworks such as Council of Europe’s Convention on Cybercrime (2001), the first international treaty on cybersecurity addressing internet and computer crime.

2010: Stuxnet and the Era of Cyber Warfare

Perhaps the most significant moment of the early 2010s was the discovery of Stuxnet in 2010. This sophisticated worm specifically targeted Supervisory Control and Data Acquisition (SCADA) systems used in Iran's Natanz Nuclear Facility, later attributed to state-sponsored actors. Stuxnet redefined the boundaries between cyber crime, cyber espionage and cyber warfare, demonstrating that digital attacks could have tangible, real-world consequences.

Mid 2010s:Ransomware Epidemic and Advanced Persistent Threats (APTs)

Following Stuxnet, the mid 2010s witnessed a surge in ransomware attacks where malicious actors took victims' files and demanded ransom for their release after encrypting the files. These type of attacks were targeting individual users at first. However malicious actors took their job one step ahead and started to target hospitals, corporations and municipal systems. In 2017, WannaCry became a global crisis, exploiting a vulnerability in Microsoft Windows (Eternal Blue) to infect more than 200,000 systems in over 150 countries. It disrupted healthcare services in the UK, manufacturing plants, and government agencies, underscoring the global scale and speed of modern cyber threats.

Parallel to ransomware, Advanced Persistent Threats (APTs), often linked to national states because it requires extensive financial, technical and human resources, became the dominant concern. As an addition, these attacks are taking a long time and aiming to steal significant information, secret observation, and give political disruption.

2020s:Supply Chain Vulnerabilities and Geopolitical Cybersecurity

The 2020s began with one of the most significant supply chain compromises in history: SolarWinds (2010) attack. The malware was injected in a legitimate software update, affecting thousands of companies, U.S.A. government agencies, and Fortune 500 companies. The incident demonstrated that even well protected networks could be compromised through trusted third-party vendors. Additionally, COVID-19 pandemic created new opportunities for cybercriminals. Malicious actors took actions to exploit insecure home networks, misconfigured VPNs, and phishing campaigns disguised as health alerts.

Conclusion: From Crawls to Being One of the Most Essential Matters in the World

Starting with the invention of the computer, cybersecurity crossed its long way and evolved what it is today. Malicious actors throughout history, didn't stay still and always always took one step ahead with from just experimental attempts to sophisticated, malicious, and disruptive codes. The period has been marked by a constant escalation of threats, and a parallel growth in defensive measures, international cooperation, and public awareness.
As emerging technologies such as artificial intelligence, quantum computing, and the Internet of Things (IoT) continue to reshape the future of cybersecurity, the lessons of the past three decades will remain essential in preparing for future challenges.

2.1.2 Core Pillars of Cybersecurity

Cybersecurity is not a discipline not limited to just single sets of practices, but rather rests on a group of fundamental principles that ensures the protection of digital systems. These principles commonly known as “Core Pillars of Cybersecurity”, provide a conceptual framework that helps governments, private institutions, and individuals build resilient digital infrastructures. The most common pillars of cybersecurity are Confidentiality, Integrity, Availability. These pillars are known as the CIA Triad, and they keep each other up in a cycle.

First Pillar:Confidentiality

Confidentiality represents one of the most fundamental pillars of cybersecurity, ensuring that information is only accessible to individuals,entities, or systems with the proper authorization. In the digital age, where huge amounts of sensitive data are transmitted across networks, confidentiality serves as a protection mechanism against the unauthorized disclosure of personal data, state secrets and corporate intellectual property. For instance, the leakage of classified military intelligence may compromise national security, while exposure of customer databases in the private sector can lead to identity theft, reputational damage, and financial losses.

To safeguard confidentiality,organizations adopt a wide range of mechanisms. Encryption plays a crucial role by converting data into unreadable formats for unauthorized actors, ensuring that even if data is intercepted, it can not be understood. Access control systems and role-based permissions further restrict data usage to specific individuals, aligning user privileges with operational necessity.Additionally, multi-factor authentication (MFA) strengthens confidentiality by requiring multiple proofs of identity, mostly reducing credential theft.

Second Pillar: Integrity

Unlike confidentiality, which protects against unauthorized access, integrity focuses on protecting data from unauthorized modification, deletion, or corruption. This ensures that information remains consistent, accurate, and trustworthy throughout its lifecycle. The

importance of integrity becomes evident when one considers the consequences of manipulated data. For example, the alteration of financial records in a banking system could cause devastating economic losses, while tampering with medical records might result in incorrect treatments with life-threatening outcomes.

Maintaining integrity requires a blend of technical and procedural solutions. Cryptographic hashing is widely used to generate unique fingerprints for files and messages, ensuring that even the smallest alteration can be detected. Checksums and error-detection codes verify data consistency during transmission, while digital signatures provide cryptographic proof of authenticity. Additionally, version control systems in software development environments preserve the history of changes, allowing verification and rollback in case of corruption or malicious edits.

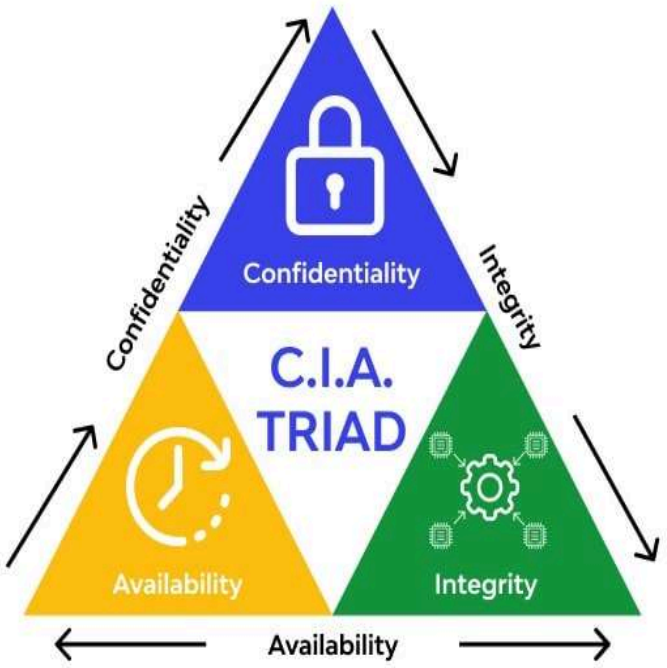
Third Pillar: Availability

Availability is a critical pillar of cybersecurity, ensuring that information systems, networks, and digital resources remain accessible to authorized users whenever required. Unlike confidentiality, which focuses on restricting access, or integrity, which ensures the accuracy of data, availability addresses the operational continuity of services. In contemporary society, where financial institutions, healthcare systems, energy grids, and government services rely heavily on digital infrastructure, a failure in availability can have immediate and far-reaching consequences.

Threats to availability can originate from a variety of sources. Technical failures, such as hardware malfunctions, software bugs, or network congestion, can temporarily disrupt access to essential services. Malicious attacks, particularly Distributed Denial of Service (DDoS) campaigns, deliberately overwhelm systems with excessive traffic, rendering them inoperable. Even natural disasters, such as earthquakes or floods affecting data centers, can compromise availability if redundancy measures are insufficient.

Organizations implement multiple strategies to maintain high availability. Redundant system architectures, including failover servers and mirrored databases, ensure that if one component fails, another can take over without service interruption. Load balancing distributes network or application traffic across multiple resources, preventing bottlenecks. Disaster recovery plans and regular system backups allow rapid restoration of services following an unexpected

outage. Additionally, continuous monitoring and predictive maintenance help identify potential failures before they impact users.



2.2 Cyber Threats and Key Actors

2.2.1 Types of Cyber Attacks

This section will make you understand cyber attacks by examining how they are made and the details on the background. Additionally, the solutions given after will make you gain a better perspective on cybersecurity matters since they are directly related to agenda. We will be examining 4 types of common cyber attacks.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

These two types of attacks aim to overwhelm a system's resources by sending illegitimate requests to the system until it is unable to answer any requests. However, the point where these two types of attacks differ is the funds. While the attacker uses one system that does all the job by sending unrelenting requests to the resources, to launch a Denial of Service attack, it requires initiating the attack by a vast array of malware-infected host machines controlled

by the attacker when it comes to a Distributed Denial of Service attack. These attacks generally end up with the full shutdown of the targets, depending on how big the attack was.

Solutions for the Attacks

Throughout history, malicious actors have launched many DoS and DDoS attacks. However, the cybersecurity experts overcame the issues they encountered with various solutions.

Firewalls and IDS/IPS Systems: Firewalls are one of the oldest and most efficient protection systems against DoS and DDoS attacks. Its job is to examine all the incoming and outgoing packages to detect DoS and DDoS attacks. These systems can detect the attacks through suspicious packages, malformed requests or excessive connections from the same source. However, these defense mechanisms alone can not always detect advanced, large-scale DDoS attacks. At this point, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) come into play. To start with, IDS Systems monitors the networks and searches for abnormal actions such as sudden spikes in traffic, unusual connection attempts, and known attack signatures. However, although these systems are capable of detecting DoS and DDoS attacks, they are not able to prevent them. On the other hand, IPS Systems actively intercept the malicious traffic and drop it before it reach to the target network.

Rate Limiting Systems: Rate Limiting Systems are the types of systems that restrict the number of requests a user or system can send within a specific period of time. These defense mechanisms are especially useful against DoS attacks which overwhelm the services by sending excessive requests. By applying thresholds, Rate Limiting allows each user to have a fair portion of resources. As an example, a web server allows each user to send up to 100 requests per minute, if a user exceeds the limit, the additional requests they send will be either blocked, delayed, or redirected. This prevents malicious bots from monopolizing the bandwidth and CPU power the server has, while legitimate users still maintain service access. In the end, Rate Limiting Systems' simplicity and low overhead are their strong side. However, when it comes to DDoS attacks, the system alone is not enough to prevent thousands of devices sending requests under the threshold.

Cloud DDoS Protection Systems: Cloud-based DDoS Protection Systems are one of the most essential and effective defense mechanisms against large-scale DDoS attacks. These

services are provided by companies like Cloudflare, Akamai, AWS Shield by continuously monitoring the incoming traffic in real time. When abnormal patterns are detected such as sudden spikes in the traffic or traffic originating from thousands of IP's, the system automatically filters and blocks the malicious packages before it even reach to the target. One of the key advantages these systems are known for is its scalability. Unlike traditional solutions like firewalls or load balancers, cloud protection mechanisms can absorb huge amounts of traffic allowing users to get access to services even at peak attack periods.

Phishing Attacks

Phishing is one of the most common and dangerous forms of cyber attacks, exploiting human psychology rather than technical vulnerabilities. In a phishing attack, cybercriminals attempt to deceive individuals into revealing sensitive information such as usernames, passwords, credit card numbers, or other personal data. Unlike network-based attacks like DoS or DDoS, phishing specifically targets the human element, making it a critical concern in cybersecurity awareness and defense strategies.

These attacks usually occur through emails, text messages, social media, or fake websites. Attackers craft messages that appear legitimate, often mimicking trusted institutions like banks, government agencies, or well-known companies. A typical phishing email might request the user to "verify their account" or "reset their password," prompting them to enter confidential information on a fraudulent site. A more advanced form, spear phishing, targets specific individuals or organizations, using detailed personal information to increase credibility and the likelihood of success.

The consequences of phishing attacks can be severe. Victims may suffer identity theft, financial losses, or unauthorized access to corporate systems. Compromised accounts can further facilitate the spread of malware, ransomware attacks, or even DDoS attacks from hijacked devices. Because phishing relies on deception, purely technological defenses are insufficient.

Solutions for the Phishing Attacks

Protecting against phishing attacks requires a combination of technological measures and user education. On the technical side, email filtering systems are crucial. These systems automatically scan incoming emails for suspicious links, known malicious domains, or unusual sending patterns. Advanced filters use machine learning to detect subtle signs of phishing attempts, reducing the chances that a fraudulent email reaches the user's inbox.

Another critical measure is multi-factor authentication (MFA). Even if a user's credentials are stolen through phishing, MFA ensures that the attacker cannot access the account without a second verification method, such as a code sent to a mobile device. Organizations can also deploy anti-phishing toolbars or browser extensions that warn users when visiting suspicious websites, preventing credential theft from fake login pages.

However, technology alone is not enough. User training and awareness programs play a central role in mitigating phishing risks. Employees and users must learn to recognize signs of phishing, such as urgent messages, spelling errors, or unexpected requests for personal information. Simulated phishing exercises can reinforce this training by allowing users to practice identifying phishing attempts in a controlled environment.

Brute-Force Attacks

A brute-force attack is a method used by cybercriminals to gain unauthorized access to accounts, systems, or encrypted data by systematically trying all possible combinations of usernames and passwords until the correct one is found. Unlike phishing, which relies on deception, brute-force attacks depend on computational power and persistence.

The most basic form is the simple brute-force attack, where an attacker tries every possible password combination. For example, if a password is only four digits long, the attacker can attempt all 10,000 possible codes until the correct one is discovered. With stronger hardware and automation tools, attackers can attempt millions of combinations per second.

There are more advanced types of these attacks such as dictionary attacks, credential stuff, and hybrid attacks combining with other things. The cybersecurity risk of brute-force attacks is significant. If successful, attackers can gain full control over user accounts, corporate

networks, or encrypted files. This can lead to data breaches, financial theft, or further attacks launched from compromised accounts.

Because brute-force attacks exploit weak or reused passwords, they highlight the importance of strong authentication policies and system-level protections in cybersecurity defense.

Solutions for Brute-Force Attacks

The most effective defense against brute-force attacks is enforcing strong password policies, requiring long and complex passwords that are difficult to guess. Account lockout or delay mechanisms further protect systems by limiting repeated login attempts. For example, locking an account after five failed attempts or introducing increasing time delays slows attackers significantly.

Another critical layer is multi-factor authentication (MFA). Even if a password is compromised, attackers cannot access accounts without a second factor, such as a one-time code or biometric verification. Finally, monitoring login activity and using intrusion detection systems help identify and block suspicious patterns before damage occurs.

SQL Injection Attacks

SQL Injection is a type of cyber attack that targets databases through vulnerable web applications. In this attack, an attacker inserts or “injects” malicious SQL code into input fields, URLs, or cookies, exploiting insufficient input validation. If successful, the attacker can manipulate the database to read, modify, or delete sensitive data, bypass authentication, or even execute administrative operations on the server.

This attack is particularly dangerous because it directly targets the data layer, often without requiring high-level system access. Common examples include entering SQL statements into login forms, search bars, or feedback fields that trick the application into executing unintended queries.

The consequences of SQL Injection attacks can be severe, including data breaches, financial loss, and exposure of confidential user information. Unlike brute-force or phishing attacks,

SQL Injection exploits coding vulnerabilities, emphasizing the importance of secure software development practices, proper input sanitization, and the use of parameterized queries to prevent exploitation.

Solutions for SQL Injection Attacks

Preventing SQL Injection attacks requires a combination of secure coding practices, technical measures, and continuous monitoring. The first and most critical step is input validation and sanitization. Every piece of user-supplied data—whether from forms, URLs, or cookies—should be carefully checked to ensure it does not contain malicious SQL code. Using parameterized queries or prepared statements is highly effective, as it separates code from data and prevents injected commands from being executed.

In addition, deploying a Web Application Firewall (WAF) adds another layer of protection by detecting and blocking suspicious database requests before they reach the application. Regular vulnerability assessments and penetration testing help identify weaknesses in applications and databases. Educating developers about secure coding standards and monitoring database activity for unusual behavior are also essential measures.

By combining these approaches, organizations can significantly reduce the risk and impact of SQL Injection attacks, protecting sensitive data and maintaining trust in their web applications.

2.2.2 Main Actors in the World

In this section, we will be examining the main actors in the world that hold cyber power in their hands. These actors may be national states, organizations, hacker groups or even individuals. So, we got to divide them into four categories: State-Level Actors, Organizational-Level Actors, Group-Level Actors. In each category, we will see 2 major actors .

State-Level Actors

United States (USA)

The United States is one of the global leaders in cybersecurity, excelling in both defense and offensive capabilities. Through agencies like the NSA (National Security Agency) and US Cyber Command, the US can conduct cyber operations targeting critical infrastructure while protecting national security. It also plays a key role in establishing international cybersecurity standards. Collaborations between government institutions and the private sector create a broad defensive network. Additionally, the US conducts intelligence gathering, cyber espionage, and threat analysis on a global scale, making it a highly influential actor in the international cyber arena.

China

China stands out for its state-sponsored cyber operations and advanced technological infrastructure. Cyber units within the PLA (People's Liberation Army) carry out both economic espionage and strategic cyber attacks. China views cybersecurity as a matter of national sovereignty and enforces comprehensive cyber laws to protect its digital infrastructure. Collaborations with major tech companies enhance its global cyber capabilities. Active in both offense and defense internationally, China is also influential in cyber diplomacy and regulation, making it a prominent actor in shaping global cybersecurity dynamics.

Russia

Russia is recognized as a major cyber power, known for its sophisticated state-sponsored cyber operations. Russian cyber units, such as those linked to the GRU (Main Intelligence Directorate), are capable of conducting espionage, disinformation campaigns, and cyberattacks targeting foreign governments, corporations, and critical infrastructure. Russia emphasizes both offensive and defensive cyber strategies to advance its geopolitical interests. It often employs hybrid tactics, combining cyber operations with political influence and information warfare. Globally, Russia is considered a significant player in shaping cyber norms and challenging international cybersecurity frameworks, making it a key state-level actor.

Organization-Level Actors

NATO (North Atlantic Treaty Organization)

NATO is one of the most significant organizational actors in global cybersecurity. It treats cyber defense as part of its collective defense framework under Article 5, meaning that a cyberattack on one member state could trigger a collective response. NATO has established the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estonia, which focuses on research, training, and strategy development. The organization coordinates cybersecurity efforts among its 30+ member states, enhancing resilience against state-sponsored cyber threats. NATO's ability to unite multiple nations under shared defense policies makes it a powerful organizational cyber actor.

United Nations (UN)

The United Nations plays a unique role in the cybersecurity domain by shaping global norms and fostering international cooperation. While it does not conduct cyber operations itself, it establishes frameworks for responsible state behavior in cyberspace. The UN Group of Governmental Experts (UN GGE) and the Open-ended Working Group (OEWG) focus on issues such as cyber norms, international law in cyberspace, and confidence-building measures. The UN encourages dialogue among states, aiming to reduce the risk of cyber conflicts and promote human rights online. Its diplomatic influence makes it an essential organizational actor.

European Union (EU)

The European Union is a strong organizational cyber actor, primarily through its regulatory power and collaborative defense mechanisms. The EU Agency for Cybersecurity (ENISA) develops strategies, policies, and technical standards to strengthen member states' cyber resilience. The EU also introduced the NIS Directive and the Cybersecurity Act, which set mandatory requirements for critical infrastructure protection and certification of digital products. In addition, the EU coordinates cyber crisis response through initiatives like the Cyber Rapid Response Teams (CRRTs). By integrating legislation, cooperation, and capacity-building, the EU holds a central position in global cybersecurity governance.

Group-Level Actors

Anonymous

Anonymous is one of the most well-known hacktivist groups, operating as a decentralized

collective of hackers around the world. It does not have a central leadership, which makes it unpredictable and difficult to counter. The group is known for targeting governments, corporations, and organizations in protest against censorship, corruption, or human rights violations. Anonymous has carried out high-profile attacks such as website defacements, DDoS operations, and data leaks. While its actions are often politically or socially motivated, they raise ethical debates about cyber vigilantism and accountability. Its global presence makes it a significant group-level cyber actor.

Lazarus Group

The Lazarus Group is a state-sponsored hacking collective believed to be linked to North Korea. It is infamous for sophisticated cyberattacks involving espionage, financial theft, and disruption of critical systems. The group has been linked to the 2014 Sony Pictures hack, the WannaCry ransomware outbreak in 2017, and multiple large-scale cryptocurrency thefts. Lazarus operates with both financial and political motives, often to bypass international sanctions and fund North Korea's regime. Its advanced tools, stealth techniques, and global reach make it one of the most dangerous and influential group-level cyber actors.

APT28 (Fancy Bear)

APT28, also known as Fancy Bear, is a Russian cyber-espionage group associated with the GRU (Russia's military intelligence). The group has been active since at least the mid-2000s and is known for targeting governments, defense organizations, media outlets, and NGOs. APT28 uses phishing campaigns, malware, and disinformation operations to achieve its goals. It has been linked to interference in the 2016 US elections and multiple cyber campaigns against NATO members. With its advanced persistent threat (APT) capabilities, APT28 plays a key role in advancing Russia's geopolitical interests, making it a critical group-level cyber actor.

2.3 Cybersecurity In Emerging Technology

2.3.1 The Impact of Developing Systems on Cybersecurity

The rapid evolution of digital systems constantly reshapes the cybersecurity landscape. As new technologies emerge, they introduce opportunities for innovation but also create vulnerabilities that malicious actors can exploit. For instance, the integration of smart devices, automation tools, and cloud-based services has expanded the digital ecosystem,

increasing the number of potential entry points for cyberattacks. This growing complexity makes it harder for security frameworks to remain comprehensive and up to date. Furthermore, developing systems often prioritize functionality and efficiency during their early stages, sometimes neglecting security considerations until vulnerabilities are exposed. Another challenge is the accelerated pace of adoption; organizations and individuals tend to embrace new technologies before thoroughly assessing the risks. As a result, cybercriminals exploit these transitional phases to launch sophisticated attacks. Therefore, understanding the impact of developing systems is crucial for designing proactive defense mechanisms. It highlights the need for continuous adaptation, stronger regulations, and more collaboration between developers, policymakers, and cybersecurity experts.

2.3.2 The Internet of Ting (IoT) and Smart Devices

The Internet of Things (IoT) has become one of the fastest-growing technological fields, connecting billions of smart devices worldwide. From household appliances and wearable gadgets to industrial sensors and critical infrastructure, IoT enables efficiency and convenience. However, this vast interconnected network also introduces significant cybersecurity risks. Many IoT devices are developed with limited processing power and minimal built-in security, making them vulnerable to exploitation. Hackers can infiltrate poorly secured devices and use them as entry points for larger attacks, such as Distributed Denial of Service (DDoS) campaigns. Additionally, the sheer number of devices increases the difficulty of monitoring and managing potential vulnerabilities. Since IoT devices often collect sensitive personal or operational data, breaches can have severe consequences for privacy and safety. As IoT continues to expand, ensuring secure firmware, regular updates, and strong authentication methods becomes critical. Addressing these challenges requires collaboration between manufacturers, cybersecurity experts, and regulators to create sustainable standards for IoT security.

2.3.3 Quantum Computing and Future Cyber Threats

Quantum computing is one of the most anticipated breakthroughs in modern science and technology, promising unprecedented computational power that far surpasses classical computers. While this advancement could revolutionize industries such as medicine,

logistics, and artificial intelligence, it simultaneously poses serious concerns for cybersecurity. The most pressing issue is the potential of quantum computers to break traditional cryptographic systems. Algorithms like RSA and ECC, which currently secure most online communications, financial transactions, and classified government data, rely on the computational difficulty of factoring large numbers or solving discrete logarithm problems. A sufficiently powerful quantum computer, using Shor's algorithm, could solve these problems exponentially faster, rendering current encryption methods obsolete.

This possibility creates what experts call the "quantum threat." Even though fully operational large-scale quantum computers are not yet available, adversaries could already be harvesting encrypted data today to decrypt it in the future, once quantum technology matures. To mitigate this, researchers and institutions are working on "post-quantum cryptography," developing algorithms resistant to quantum attacks. However, transitioning global systems to new encryption standards is a complex and time-consuming process, especially for critical infrastructures such as banking, healthcare, and defense.

Beyond cryptography, quantum technology may also enhance cyber offense by enabling advanced simulations for malware development or optimization of attack strategies. On the defensive side, it holds potential for creating stronger security models and unbreakable communication through quantum key distribution. Thus, quantum computing represents a double-edged sword—its benefits are vast, but its risks demand urgent preparation and international cooperation.

2.4 Cybersecurity Infrastructure and Defense Mechanisms

2.4.1 National and Organizational Cybersecurity Structures

Robust national and organizational cybersecurity structures are essential for protecting critical infrastructure, managing cyber risks, and facilitating coordinated responses to incidents. These structures encompass governmental agencies, international organizations, and private sector entities, each contributing specialized expertise, operational frameworks, and regulatory guidance. Understanding the functions and interactions of these institutions provides a foundation for designing effective cybersecurity strategies and policies that are technically sound, internationally aligned, and capable of addressing evolving cyber threats.

United States Cybersecurity and Infrastructure Security Agency (CISA)

CISA protects critical infrastructure and provides guidance to both government and private sectors against cyber threats. National security strategies often rely on CISA's risk assessment methodologies and collaboration mechanisms to reduce attacks on critical infrastructure. Its frameworks and operational guidelines offer concrete examples of how security policies can be implemented and coordinated effectively across multiple sectors.

European Union Agency for Cybersecurity (ENISA)

ENISA coordinates cybersecurity efforts across EU member states. Its guidelines and best practices support the protection of critical infrastructure, such as energy networks, and provide standardized approaches for risk management. ENISA also facilitates cross-border collaboration and information sharing, which strengthens overall cybersecurity resilience in multinational contexts.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

CCDCOE enhances NATO members' cyber defense capabilities through research, training, and simulation exercises. Its methodologies support the development of coordinated defense strategies for critical infrastructure, balancing technical measures with strategic operational planning. CCDCOE also serves as a model for international collaboration in cyber defense.

International Telecommunication Union (ITU)

ITU establishes global communication standards and develops international cybersecurity policies. Its guidelines promote cooperation between nations, ensuring consistent approaches to cyber threat intelligence sharing and infrastructure protection. ITU frameworks help integrate national policies into broader international strategies.

National Institute of Standards and Technology (NIST)

NIST develops cybersecurity frameworks and standards widely used in critical infrastructure protection. Its Cybersecurity Framework provides structured approaches for identifying, protecting, detecting, responding to, and recovering from cyber incidents. Application of NIST standards increases the reliability and effectiveness of security measures at both organizational and national levels.

INTERPOL Cybercrime Directorate

INTERPOL coordinates international responses to cybercrime, supporting intelligence sharing and joint operations. Its protocols enable multinational collaboration to prevent

attacks such as ransomware campaigns. INTERPOL frameworks provide operational guidance that complements national security measures and enhances global cybersecurity coordination.

Private Sector Cybersecurity Units (e.g., Microsoft, Palo Alto Networks)

Large technology companies maintain dedicated cybersecurity teams to protect systems and sensitive data. Their threat intelligence and advanced detection tools can be integrated into national cybersecurity strategies. Private sector initiatives demonstrate how commercial technologies and organizational best practices contribute to overall cyber defense.

CERT (Computer Emergency Response Teams) Networks

CERT teams provide rapid response to cyber incidents at both national and international levels. Coordination across local and global CERT networks ensures timely mitigation of attacks against critical infrastructure. CERT structures exemplify operational models for incident response and resilience planning in complex cyber environments.

2.4.2 Incident Response Systems and Networks

Effective incident response systems and frameworks are critical for minimizing the impact of cyberattacks and ensuring rapid recovery of affected infrastructure. Structured guidelines such as the NIST Computer Security Incident Handling Guide (SP 800-61r2) provide detailed procedures for preparation, detection, analysis, containment, eradication, and recovery, ensuring systematic management across sectors. Similarly, international standards like ISO/IEC 27035 offer globally recognized methodologies for planning, response, and post-incident review. Coordination among national and international teams is facilitated through networks such as CERT/CC and the FIRST community, which promote best practices, communication protocols, and information sharing during cyber events. Practical operational guidance is also provided by organizations like the SANS Institute, which emphasizes clearly defined roles, responsibilities, and escalation procedures, while high-security environments benefit from frameworks developed by entities such as the US Department of Defense. Regional collaboration is exemplified by the EU CSIRT Network, which standardizes reporting and mitigation across member states. Additionally, analytical

tools such as the MITRE ATT&CK Framework enhance understanding of attacker tactics, enabling organizations to anticipate threats and integrate them into comprehensive response strategies. Collectively, these systems and frameworks form a structured and collaborative approach that strengthens resilience, reduces risk, and aligns incident response with international best practices.

2.4.3 Partnership and International Cooperation

International collaboration and strategic partnerships play a crucial role in strengthening global cybersecurity resilience. Cross-border coordination enables the sharing of threat intelligence, harmonization of legal frameworks, and joint responses to cyber incidents that transcend national boundaries. By fostering cooperation among governmental agencies, international organizations, and private sector entities, these partnerships enhance the effectiveness of cybersecurity strategies and ensure that protective measures are both comprehensive and aligned with evolving global standards.

INTERPOL Cybercrime Directorate

INTERPOL's Cybercrime Directorate facilitates international collaboration among law enforcement agencies, enabling the exchange of intelligence, coordination of operations, and rapid responses to transnational cyber threats. Its protocols support joint investigations, cross-border monitoring, and preventive strategies against cybercrime, ensuring that nations can collectively mitigate attacks that would be difficult to address individually. INTERPOL also provides operational guidance and standardized procedures for managing incidents that span multiple jurisdictions.

Budapest Convention on Cybercrime

The Budapest Convention establishes international legal standards for investigating and prosecuting cyber offenses. By harmonizing legislation across member countries, it enables law enforcement agencies to cooperate effectively in cross-border investigations. The Convention also provides a framework for sharing digital evidence, securing mutual legal assistance, and fostering international collaboration to deter cybercriminal activity while maintaining legal consistency among participating nations.

European Union Agency for Cybersecurity (ENISA)

ENISA supports EU member states in coordinating cybersecurity policies and responses. Its initiatives include threat intelligence sharing, infrastructure protection guidelines, and cross-border incident coordination. By providing best practices and facilitating regional cooperation, ENISA strengthens the overall security posture of member states, ensuring that national strategies align with broader European standards and promote consistent cybersecurity measures across borders.

EU CSIRT Network

The EU CSIRT Network connects Computer Security Incident Response Teams across member states, standardizing incident reporting, mitigation, and communication protocols. This collaborative network enhances cross-border response capabilities and allows for rapid containment of cyber threats affecting multiple countries. Its structured coordination mechanisms improve situational awareness and foster shared operational practices among participating national teams.

Private Sector Partnerships

Collaboration between governments and private technology companies is critical for effective cybersecurity. Large corporations, cybersecurity vendors, and industry consortiums provide expertise, threat intelligence, and innovative tools that complement governmental capabilities. These partnerships facilitate rapid detection, mitigation, and prevention of cyber incidents, demonstrating how public-private cooperation strengthens both national and international cybersecurity resilience.

Forum of Incident Response and Security Teams (FIRST)

FIRST promotes global cooperation among incident response teams by establishing best practices, communication channels, and coordinated procedures. Membership in FIRST allows organizations to access shared threat intelligence, standardized incident handling frameworks, and collaborative training programs, enabling consistent and effective responses to cyber incidents across diverse jurisdictions.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

CCDCOE provides training, research, and simulation exercises that enhance member states' cyber defense capabilities. Its cooperative initiatives support the development of shared

frameworks and operational strategies, fostering interoperability between national military and civilian cyber units. By offering standardized methodologies and collaborative exercises, CCDCOE strengthens the collective capacity to respond to complex cyber threats.

UNIT 3: ETHICAL UNIT

3.1 Human Rights in Cybersecurity World

As digital communication spread around the world and became the main source of information gathering both between the humankind and from the internet many concerns have been raised regarding cybersecurity, privacy and most importantly relating ethical issues. Core of the discussions are mainly topics regarding the privacy and freedom of the user by protecting the balance between security and individual rights. In the past years many international organisations have taken action in order to protect safety and guidelines by publishing many documents as in :frameworks, declarations and so on.

3.1.1 Free Usage of Internet and Censorship

Free usage of the internet and censorship also is an issue which has been the centre of debates for decades. This problem mainly occurs as a result of nations with aggressive policies towards expression of words. Many points state that many of these policies go against freedom of speech and such restrictions from high authorities mustn't be.Internet censorship may be seen in many ways such as: website blocking, filtering, content remıval, shutdown, etc. Supporting the topic the International Covenant on Civil and Political Rights(ICCPR) article 19 guarantees the freedom of speech and access to information, however the treaty also states that such restrictions shall be allowed if allowed by the law, serve a legitimate aim, and is necessary or proportionate to the aim. Other resolutions released from the UN states that “The same rights that people have offline must also be protected online.” As well as ‘’Blanket censorship and shutdowns are considered human rights violations.’’

Globally censorship comes in many ways. For instance open democracies do allow access to the internet freely however would occasionally remove content which relate to terrosim, speech of hatred, child explosion. On the other hand such powers with authoritarian regimes do broadly use censorship by blocking opposition websites, restricting social media and so on in order to hold political strength.

Contrary to these views many argue that censorship protects national security from possible cyber attacks and spread of misinformation still, without cybersecurity laws or guidelines regarding the agenda it can turn into tools of mass censorship which means that there still will be the possibility of limited usage of free internet.

Other Documents Related to the subject:

-UN Human Rights Council(UNHRC) Resolution 20/08/2012
-Council of Europe, Budapest Convention 2001 article 15
-Special Rapporteur Reports(UN)

3.1.3 Data Protection and Consent

There are many principles which refer to data protection and consent regardless the most important five can be visualised as autonomy, gives the person control of their personal data; transparency, informs the user of the data collected and how it will be used; proportionality, ensures that the data gathered is only limited to necessary information; termination/cancelability, gives the user the right of canceling or customizing the data, securing consent isn't a one time trap, avoiding possible scams that could occur from; and lastly, fairness, making sure that no tricks are to be played in order to get consent, such as manipulation.
In the EU, data protection is principally governed by the EU General Data Protection Regulation (GDPR), which came into force on 25 May 2018 and is applicable in all EU Member States. The GDPR, which repealed the Data Protection Directive 95/46/EC, regulates the collection and processing of personal data across all sectors of the EU economy and introduced new data protection obligations for controllers and processors alongside new rights for EU individuals.

3.1.4 Right of Accession to the Internet

The right of internet access refers to the idea of how internet access must and is a fundamental human right. It is to be considered at the same value of content as access to information, education; expression of personal opinion and participation in democracy. This point of view is strongly supported in many UNHRC resolutions stating ‘’The same rights people have offline must be protected online.’’
Furthermore, denying internet access can be seen as a form of social exclusion and restriction of knowledge.
Furthermore, European Court of Human Rights declare that:
Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
European Convention on Human Rights, Article 10.

3.2 Ethical Concerns of State Behaviour

The effects of cyber attacks in common warfare is undeniable one of the biggest reasons being that the information used in Modern Warfare is mostly if not fully laid behind government data. What's more, in a possible situation where the country's cyber security system collapses and the web is hacked then the nation will most probably be left defenseless against any foreign forces and aggressions. This means that in many cases cyber security is very crucial and important for the nation's protection.
Defensive operations that aim at infrastructure private companies and public areas can cause heavy civilian harm. These operations can disturb hospitals Financial systems putting lives and safety in danger. Expanding on the topic we can see many examples in the past. one of which is an offense by the United States and the Israeli government On the Irani nuclear facilities where they deployed a cyber weapon. It was highly targeted however his friend beyond the intended boundaries affecting possible civilian lives this is where the ethical concerns increase.

One of the main reasons why cyber warfare is a bigger issue compared to traditional warfare is that unlike traditional warfare it is not bounded by sufficient treaties which makes accountability difficult.
In addition to that many states also use online platforms in order to spread often manipulative misinformation through social media using bots and fake accounts which leads to loss of informed choice making ability among citizens. This issue gets worse and worse especially around election eras. Free and fair votes are often under the threat of deceived voter decisions.

In recent years digital inequality and the gap between the 1. world countries and 3. world countries seize to grow as the less developed countries fail to hold on to the technology age and innovations. As a result many countries restrict or simply fail to protect and invest in connectivity within the country. This causes unequal access to digital infrastructure.
Lack of internet access leads to limited reach towards healthcare, work opportunities, and education.
However some governmental authorities might deliberately follow a policy intending to keep the population uneducated with the purpose remaining in political power as some might claim that the uneducated are easier to rule. So anti-education campaigns can be commonly seen in totalitarian regimes as the uneducated are less likely to question authority, more vulnerable to propaganda and overall less aware of their economic political situations.

3.2.1 Ethics of Cyber Countermeasures

In the 21st century many nations are now obligated to expand on cybercountry measures in order to neutralize, defend or punish cyber attacks. Passive actions in response to malicious cyber activity are seen as necessary by many governments. One of many defense types are countermeasures. One of the examples would be hack back which intends to take action inside the attacker system. Others May follow more offensive country measures by punishing attackers by striking back this may be visualized an example with launching cyber attacks to damage attackers infrastructure distracting attackers economic or political systems

In conclusion cyber countermeasures are a series of responses which range from defensive actions to literal offensive Operations. Nevertheless it must be kept in mind that these country measures do come with ethical concerns regarding attribution of civilian harm and the legality.

3.2.2 Attribution and Accountability Dilemmas

Attribution and accountability dilemmas are mostly at the heart of ethical problems regarding cyber security; the reason being is that it is extremely difficult for defensive applications to detect who exactly is behind the attacks. Many attackers can use proxies vpns or simple ways to interrupt these applications to locate the attacker in this issue might result in false flags leading the innocent to be misjudged. These unfair punishments would cause heavy injustice and escalation in the global stage of web security and international peace. Cyberspace constitutes a new frontier, which – although crucial for the functioning of modern societies – remains largely unregulated under international law. Following the emergence of cyberspace, the international community accepted that the traditional norms and principles of international law would continue to apply to this domain. While in general this provided clarity on the application of international law in cyberspace, it did not address the specificities of cyberspace that complicate this. One of these key areas is the norms and standards for the attribution of cyber-attacks. Under international law, attribution is an important prerequisite for establishing state responsibility for an internationally wrongful act. An act or omission can be attributed to a state if it is committed either by a state organ or by persons or entities exercising elements of governmental authority.4 The ability or inability to attribute a cyber-attack therefore has various political and legal implications

3.2.3 Cyber Operations in Conflicts between Countries

Cyber Operations in Conflicts between Countries is one of the most sensitive issues in modern day cybersecurity and it continues to get heated and heated day by day. Many cyber operations are either state-directed or state-sponsored actions in common cyberspace, o8ften during the time of political tensions or armed conflicts. These attacks mainly target intelligence infrastructure.

–Espionage, theft of information
–Sabotage, disruption of infrastructure
–Psychological operations, spread of disinformation propaganda
–Pre-war shaping operations, weakening a country before military conflict and actions

While judged from the ethical perspective one can argue whether cyber operations are equivalent to armed attacks under the UN charter. According to the UN charter article 2(4) states must refrain from using force against territorial integrity or political independence. The argument is if a cyberattack equals ‘’use of force’’? If it causes physical destruction upon power units, hospitals many support the idea that it does. If it is used as espionage or propaganda then it shall not be considered as so as it usually does not reach the baseline.

–*All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.* United Nations Charter, article 2(4).

On the other hand UN charter article 51 also declares that the attacks can be justified under self-defence as a response to armed attacks as the nation would have the inherent right of self-defence.

–*Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.* United Nations Charter, article 51.

Exemples,

–Israel-Iran Cyber conflict:

*The first major state-sponsored cyberweapon was dropped on Iranian centrifuges at Natanz, an Iranian Nuclear facility causing physical destruction without traditional bombing.

*Iranian hackers tried hacking into Israeli alter chemical levels with the intention of poisoning water supplies which clearly violated distinction and proportionality under international humanitarian law, direct targeting of civilian harm.

*Israel allegedly disrupted operations at an Iranian port as retaliation. On top of that there has been several repeated cyberattacks on oil facilities, transport systems and even civilian infrastructure.

3.3 Ethics of Surveillance and Data Collection

There are many matters concerning this topic. Mainly being digital ethics, security, human rights… And why surveillance and data collection matters so much is that governments and companies worldwide collect vast amounts of data. What is more is that it is justified for national security, crime prevention and business purposes. Yet it too raises questions about privacy, autonomy , consent and so on.

Expanding on the ethical view of the topic, we can see that even though surveillance may provide protection against terrorism, cybercrimes consent monitoring threatens privacy in many ways as a fundamental human right which is documented by the Universal Declaration of Human Rights Article 12. This setback raises many questions in reference to how much privacy should individuals sacrifice for collective security. In conclusion the balance between protective security and personal protection of consent must be secured by the authorities.

3.3.1 Corporate Data Harvesting

Corporate data harvesting is when large scale data is collected by private companies via social media, search engines etc. This data gathered by private companies may contain personal data such as browsing habits, purchase history, voice data, location data, and even biometrics according to research. The ethical level of this intelligence browsing is very complicated as some might say that many users agree to data harvesting through long terms

of service that they do not read. Some companies even further violate this by applying forced necessity: ‘’ click accept or don't use’’
Many researches show that a lot of companies world wide including companies with the likes of yahoo, facebook and so on have been charged with and have been dealing with online identity theft. Corporate data harvesting often without meaningful consent or user control transforms personal information into digital products. These actions may enable innovations yet it also risks explosion, manipulation and human rights violence if left unorganised.

3.3.2 Whistleblowing and Ethical Lines

Whistleblowing is when an insider exposes unethical, illegal or harmful activities within a government. Some of the ways cybersecurity might be involved in whistleblowing are unlawful surveillance, data misuse of breaches and human right violations.
These whistleblowing may influence political, economical and social situations within the country. Raising the tension during election times may be beneficial for some parties.
Whilst some might spread as misinformation some may be acquired through insiders or intelligence services.
In 2022, the U.S. saw highly impactful whistleblower and retaliation events primarily resulting from an active U.S. Securities and Exchange Commission. This was an aggressive approach taken by the Occupational Safety and Health Administration and consequential decisions from federal and state courts around the country. This initiative has only grown, and in May 2023, the SEC awarded a tipster on Ericsson the largest-ever whistleblower award of $279 million. This is more than double the previous record amount of $114mn, which was announced in October 2020.

3.3.3 Mass Surveillance and Targeted Monitoring

Mass surveillance is the whole of collective data from entire populations which reach immensely large scales and usually consist of phone records, internet traffic, location data, social media activity etc. Often it is implanted by states justified by national security or crime prevention. On the other hand targeted monitoring is focused on specific individuals, groups

or networks. The government may monitor terrorists, suspects, cybercriminals and targeted individuals. The data provided usually is more detailed and limited on a case by case basis. Mass surveillance may sometimes violate privacy, proportionality and transparency. While targeted monitoring can be seen as ethical if it respects human rights and necessity it must be made sure that the usage is limited to the purpose.
Some nations tend to be abusing mass monitoring both within the state and towards foreigners as well. This issue causes many arguments as many argue that it disturbs international peace.
The Universal Declaration of Human Rights (UDHR) states that *"Everyone has the right to privacy and freedom from attacks on their reputation."*

3.3.4 Case Studies

A case study is an in-depth, detailed examination of a particular case (or cases) within a real-world context. For example, case studies in business might cover a particular firm's strategy or a broader market; similarly, case studies in politics can range from a narrow happening over time like the operations of a specific political campaign, to an enormous undertaking like world war, or more often the policy analysis of real-world problems affecting multiple stakeholders.
Case studies are usually data intelligence that targets individuals but most cases show examples of ethical dilemmas, human rights risks. These detailed examinations are used to understand big concepts, issues or theories. In cybersecurity we may see case studies in specific events, scandals or incidents. A regular case study would cover the topics of background, impact, etc.
In 2021 many case studies were done targeting Pegasus Spyware, an advanced spyware developed by the NSO Group connected to Israel. Pegasus Spyware was one of the highest developed of its type as it had access to iOS and Android devices being able to read encrypted messages from facebook, whatsapp, telegram; record calls; access files, contacts, and active locations. The spyware used zero-click exploits meaning the user wouldn't be informed upon the intelligence obtained.
In 2021 investigation by Forbidden Stories and Amnesty International revealed that pegasus targeted and spied on journalists, human rights defenders, opposition politicians, and activists. Apparently over 50.000 contact numbers were selected as potential targets. Among

these 50.000 people were also: Murdered Saudi journalists, Emmanuel Macron, Imran Khan and Indian politicians, Human rights activists from Mexico, Morocco, India…
Pegasus Spyware violated:
Right to Privacy
Freedom of Expression & Press
Abuse of State Power
Lack of Transparency & Accountability.

3.4 AI and Automation in Cybersecurity

AI significantly enhances cybersecurity through automation by providing enhanced contextual information, enabling better signal-to-noise ratios, and ultimately reducing response times. This powerful combination allows security teams to identify, prioritize, and respond to threats with unprecedented speed and precision, augmenting human capabilities to manage the growing complexity of the threat landscape.
As each day passes Artificial Intelligence & Automation is getting more and more adopted to the battlefield and cyber hardware and software. These systems are used in the topics of:
-Threat detection
-Incident response
-Pattern recognition and defence against cyber operations
-Monitoring information
The reason is simple, AI is much faster than humans in many ways. It can detect anomalies both in physical and cyberspace within seconds which might have been impossible to spot with the human eye.
Nonetheless the ethical level of AI is not to be denied as the decision making system of artificial intelligence may be controversial and often argued if it is humanly or not.

3.4.1 Use of AI in Threat Detection and Attribution

AI systems are now a cornerstone in cybersecurity decision-making. These systems adeptly address a broad spectrum of threats, automating highly accurate incident response strategies. This evolution is pivotal in handling the rapidly evolving nature of cyber threats, coupled with the challenge of managing vast volumes of threat intelligence inputs.

Although as mentioned before, Artificial Intelligence is able to make split second decisions in crisis situations immediately tackling a problem it is a matter of suspicion if AI afterall is reliable or not and should decision making responsibility be left entirely on AI. It is arguable that AI might not be perfect or it may not give the best decision compared to the human mind and point of thinking.
Usage of AI in threat detection enhances security and regional safety but puts privacy under risk. AI in attribution speeds up the process of investigations but creates ethical risks if wrong, Thus human oversight and transparency is seen as necessary in order to prevent misuse.

3.4.2 Autonomous Cyber Defence Systems(ACDS)

Autonomous Cyber Defence Systems are self-driven AI powered security programs which are able to detect, analyze, and respond to other various cyber attacks without direct human support. These systems can actively counter attack, isolate threats, shut down dangerous viruses and more. So ACDS can take action fully independent of any human supervision or support.
From the ethical view many find it hard to completely trust AI. Some question accountability, it may be hard to address the responsibility for the fault of AI thus making the process of international law and determining who is at fault more rough. Furthermore, if AI hits innocent servers or even physical locations as a part of a launched counter attack, it would violate sovereignty and international peace.
Debates regarding to the agenda has raised many questions:

-Should the autonomous systems only have the right of defence or should they be able to counterattack?
-Should human permit be mandatory, Wouldn’t the process of “AI suggestion, Human approval” slow down military operations?
Autonomous security systems may guarantee speed, efficiency but fail on the ethical level as they may endanger civilian lives and might violate international human rights such as right to life, privacy and as such. Many argue they should be appointed only for defence or non-lethal operation and be under the supervision of mankind at all times.

4.Questions to Be Answered

1)How can states and organizations effectively strengthen critical infrastructure against increasingly sophisticated cyberattacks, including ransomware and supply chain threats?

2)What measures can be implemented to improve international cooperation and information sharing in response to cross-border cybercrime and cyber espionage?

3)How should emerging technologies such as artificial intelligence, quantum computing, and IoT be regulated to prevent new cybersecurity vulnerabilities while promoting innovation?

4)What strategies can ensure the protection of personal data and privacy in an era of mass surveillance, targeted monitoring, and increasing cyber-enabled economic activity?

5)How can the international community promote capacity-building and cyber resilience in developing countries while ensuring equitable access to cybersecurity resources and expertise?

6)How can public-private partnerships be optimized to enhance threat detection, incident response, and proactive cyber defense on both national and global levels?

7)How can global standards and frameworks be developed or improved to ensure consistent cybersecurity practices across different sectors and regions?

8)What strategies can be adopted to prevent and mitigate the growing threat of cyberattacks targeting critical public services, such as healthcare, energy, and transportation systems?

5.Glossary

1)Legitimate Service: A legitimate service is an authentic and authorized online platform or resource intended for genuine user activities, as opposed to malicious or fraudulent services created for exploitation.

3)Static File: A static file is a fixed digital resource, such as an image, CSS stylesheet, JavaScript file, or document, that is delivered to users exactly as stored on the server, without being dynamically generated or altered by backend code.

4)Web Application Firewalls (WAF): A Web Application Firewall (WAF) is a security system that monitors, filters, and blocks malicious HTTP/HTTPS traffic to and from a web application, protecting it against common attacks such as SQL injection, cross-site scripting (XSS), and request forgery.

5)Anycast Routing: Anycast routing is a network addressing and routing method in which multiple servers share the same IP address, and user requests are automatically directed to the geographically closest or most efficient server, improving speed, reliability, and resilience against attacks such as DDoS.

6)Ransomware Attacks: These attacks are the types of attacks that malicious actors ask for ransom after they steal personal data from individuals, intellectual property from corporates etc. and encrypt the files they reach in order to disable users to have it.

7)Band Width: Bandwidth is the maximum rate at which data can be transmitted over a network connection, usually measured in bits per second (bps), determining how much information can flow between devices in a given time.

Bibliography

- https://www.allot.com/100-plus-cybersecurity-terms-definitions/
- https://www.dcaf.ch/sites/default/files/publications/documents/accountability-cybersecurity.pdf

- https://www.amnesty.org/en/what-we-do/universal-declaration-of-human-rights/?utm_source
- https://www.un.org/en/about-us/un-charter/full-text
- https://www.echr.coe.int/documents/d/echr/FS_Access_Internet_ENG
- https://www.geeksforgeeks.org/ethical-hacking/what-is-cyber-security/
- https://www.un.org/counterterrorism/cybersecurity
- https://www.itu.int/en/action/cybersecurity/pages/un-resolutions.aspx
- https://news.un.org/en/tags/cybersecurity
- https://www.cisa.gov/news-events/news/what-cybersecurity
- https://en.wikipedia.org/wiki/Computer_security
- https://en.wikipedia.org/wiki/Cybercrime
- https://en.wikipedia.org/wiki/Malware
- https://www.microsoft.com/en-us/security/business/security-101/what-is-ai-for-cybersecurity
- https://www.cisa.gov/ai
- https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762292/EPRS_ATA(2024)762292_EN.pdf

- https://www.ibm.com/think/topics/critical-infrastructure
- https://www.ibm.com/think/topics/nist
- https://www.ibm.com/think/topics/cybersecurity#:~:text=Cybersecurity%20is%20the%20practice%20of,and%20specifically%2C%20cyber%20risk%20management.
- https://online.adelaide.edu.au/blog/cyber-security-fundamentals
- https://www.dataguard.com/cyber-security/tools/
- https://www.fortinet.com/resources/cyberglossary/smb-cybersecurity-tools