GA1: Disarmament and International Security Committee

Student Officer: Zeynep Poyanlı

Issue: Curbing terrorist use of the Internet

TIMUN '21

Turkish International Model United Nations

THIMUN Affiliated Conference

Committee: Disarmament and International Security Committee (GA1)

Issue: Curbing terrorist use of the Internet

Student Officer: Zeynep Poyanlı – President Chair

I. Introduction

Ever since its introduction to the public in 1993, the Internet has become an essential part of the human experience, opening an intriguing yet enigmatic portal of accessible information. However, the Internet's wide availability also gave rise to certain concerns— particularly about how the Internet could be abused by opportunistic terrorist groups to facilitate their activities, further magnifying the threat terrorism presents for international security. Terrorists usually utilize the internet in ways such as but not limited to finding recruits, funding their activities using discreet websites or forums, and planning for their attacks, which was exemplified during the 9/11 attacks.

The "uncertainty" in this case, as stated by the theme of TIMUN '21, is the fact that "cyberterrorism" has not yet been officially defined and no "cyberterrorist attacks" have officially occurred, resulting in one of the main issues governments face in tackling this issue internationally— having different understandings of the extent to which cyberterrorism has led to allegations of cyberwar and further political polarization between the Member States instead of fostering international collaboration. Additionally, although governments are becoming more aware of the risks presented by cyberattacks, their established security measures often fall short in preventing data infringements or the dysfunction of military equipment. "Resilience" can only manifest if governments build an international framework amidst the "uncertainty" around a phenomenon which has yet to be comprehensively defined, which is an issue to be addressed.

II. Involved Countries and Organizations

Also called the "world wide web," the Internet knows no territorial boundaries; therefore, every Member State will be under the risk of terrorist use of the internet if adequate security measures are not put into place. Therefore, delegates should keep in mind that there are more countries involved in the agenda item than the ones listed below— those countries who have either experienced major attacks that use the Internet or house most of the infrastructure that is vulnerable to a possible attack.

United States

The United States houses the most developed IT infrastructure out of all countries after Singapore, which means that it also is under the second greatest risk of being exposed to acts of cyberterrorism. After the use of the Internet was proven to be a prominent part of both the planning and execution of the 9/11 attacks, the United States has increased its efforts to prevent future terrorist use of the internet and to make the Internet a more secure platform. As a result of these efforts, simulations of cyberattacks called "Cyber Storm" started taking place biannually and a department solely focusing on cybersecurity matters named "Cyberstructure and Infrastructure Security Agency" (CISA), which functions as a subdivision of the Department of Homeland Security, was formed. CISA aims to collaborate with private and public sectors, the federal government, and infrastructure operators to help them utilize cybersecurity tools such that the appropriate defense is built against possible attacks. CISA also shares its findings regarding new technologies and risk management systems with its collaborators. It is also important to note that the US has been also accused of weaponizing cyber tools in multiple instances, specifically by Iran. For more information on this cyberwarfare, delegates are advised to see the "STUXNET" sub-clause of the Focused Overview section of this report.

Mexico

With a 13.1% annual increase in the number of its internet users since 2006 compared to 3.3% in the United States, Mexico is a newly-emergent target for cyberattacks with its location and economy— while it shows prominent GDP growth, its cybersecurity systems are relatively underdeveloped compared to Iran or the United States. Despite being the second most afflicted country in Latin America by cyberattacks and experiencing a 40% growth in the number of cyberattacks within a year, Mexico has not prioritized the issue of cyber security in its national agenda. In her article, Luisa Parraguez-Kobek reports, "Cybersecurity, sustainability, and resilience are not only necessary for Mexico's safekeeping but they are also important factors in its social and economic development. Mexico needs to engage with its national, regional and international partners to combine resources, multi-stakeholder initiatives and facilitate information sharing to ensure its security in cyberspace" ("The State").

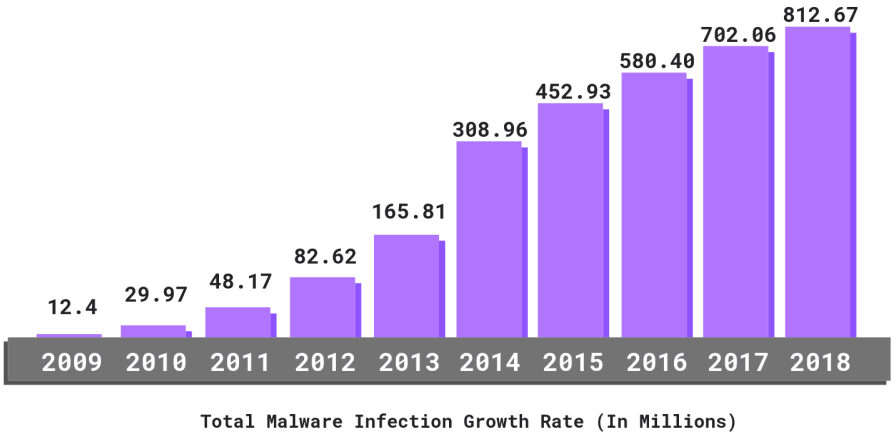
United Nations Office of Drugs and Crime (UNODC)

Although UNODC primarily focuses on combating drug trafficking and organized crime, UNODC's expertise on international justice systems and on issues transcending borders allows them to provide the Member States with cybersecurity assistance. UNODC urges international collaboration, data collection, research and analysis to minimize the consequences of cyberattacks. To that end, the UNODC has published a document entitled "The Use of the Internet for Terrorist Purposes," which essentially builds the

framework for Internet-facilitated cyberattack prevention, investigations of cyberattacks, and the procedure of prosecution for perpetrators. The link for “The Use of the Internet for Terrorist Purposes”can be found in the “Useful Links”section of this report.

III. Focused Overview of the Issue

Considering that the malware infection growth rate has grown exponentially over the last few years, as seen from Figure 1, the urgency of tackling the terrorist use of the Internet has become more of a discussion topic in the governmental agenda. Acknowledging the extent of cyberterrorism is essential to understand from where governments’ concerns stem.. With the progression of the Information Age and the COVID-19 pandemic’s quarantine protocols, governments have become increasingly dependent on transferring information on technological devices rather than storing them on paper, making more information available in cyberspace for terrorist access and creating unforeseen vulnerabilities.



“Figure 1: Total Malware Infection Growth Rate (In Millions) (Kajal)”

1. The Shift Towards Cyberterrorism

Digitization’s impact on accelerating the terrorist use of the Internet goes beyond increasing the amount of data that can be illegally accessed— online platforms also assist terrorists to find and recruit like-minded individuals more easily, which is one of the primary reasons why a shift to cyberterrorism has occurred over the years. Using the Internet to facilitate terrorist activity is cheaper and more convenient than a physical attack because having a computer connected to the web is sufficient to create and disseminate malware, while terrorists are more able to to keep their identity hidden using untraceable nicknames, utilizing the Dark Web to avoid punishments, being physically remote, and hiding their messages within graphic files that can only be accessed with a password during this process. Additionally, terrorist organizations might use the Internet to find funding for their activities, whether by committing online payment fraud (i.e. identity or credit card theft), connecting with potential donors, or using charities as front organizations for their illicit money transfers. The Internet is also a convenient platform to plan and map attacks for terrorist groups, hack military systems, and overall, make systems connected to the Internet dysfunctional.

The fear created by cyberterrorism in the Information Age can be separated into psychological, political, and economic perspectives. The possibility of being exposed to cyberterrorism triggers the humane instinct of fearing the unknown, which occurs as Internet users become random targets of a violent attack, allowing cyberterrorists to spread propaganda or misinformation, thereby causing mass psychological distress and hysteria. Upon experiencing a cyberattack, the targets are expected to resort to and get manipulated by the negative false and/or derogatory information published online, which might result in greater political or economic consequences. For example, if the terrorists accuse a certain government agency or organization of being incompetent in ensuring the safety of their citizens, the citizens might be manipulated into uprising against those organizations or agencies, creating larger-scale political turmoil. Considering that the damage of cyberattacks on the global economy was estimated to be 2.1 trillion dollars in 2019, curbing terrorist use of the internet is essential to achieve economic stability. Unlike physical attacks where there is a lengthy preparation process and higher risks of mortality, cyberterrorist attacks can be performed using more diverse methods, such as DDoS attacks, theft of data, or infection of technological devices with malware, and can even cause physical damage. For more detailed information on the ways of performing cyberattacks, delegates are advised to refer to the "Key Vocabulary" section of this report.

2. Internet Before, During, and After an Attack

A cyberattack doesn't strictly have to be the work of a terrorist group— an attack that is sponsored by a state might also result in casualties, political, economic, or psychological turmoil, which are characteristics that are usually associated with cyberterrorism. In the sections below, two specific examples of cyberattacks will be elaborated on, one of which was perpetrated by a terrorist organization and the other, allegedly, with the assistance of state funding.

a. 9/11

To perform the attack on the World Trade Center on September 11th, 2001, members of the terrorist group Al-Qaeda used the Internet to build and conceal their plans. Relying on the Internet's ability to preserve their anonymity, the terrorists obtained drivers' licenses, fake identification, social security numbers on the Internet, which they then used to purchase plane tickets. Mohammed Atta, who was the leader of the attacks, researched flight schools online from Hamburg. Additionally, two of the hijackers demanded 24/7 internet access from their hotels, showing that Al-Qaeda used the Internet as their main way of communicating. This finding was confirmed after analysts determined that 9/11 attackers used code words, such as the "faculty of urban planning" (i.e. the World Trade Center) and the "faculty of fine arts"(i.e. the Pentagon), to be able to openly communicate online without getting tracked. Atta's final message to the attackers read: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering," which

informs us of the number of terrorists participating and the targeted buildings when deciphered ("Terror on the Internet").

b. STUXNET and the "Cyber Pearl Harbor"

In June 2010, STUXNET, a malicious computer worm as small as 500 kilobytes in size, infected the software of approximately 14 industrial sites in Iran, including a uranium-enrichment plant, altering their usual workings. Since STUXNET is a worm and not a virus, it was able to spread on its own using the computer networks, but the Internet was not its only mode of transmission— if the worm was carried from one device to another using a USB stick, an Internet connection was not necessary. STUXNET specifically targeted and destroyed machines using a Microsoft Windows operating system (OS), a thousand of which were an integral part of Iran's nuclear program, allegedly setting Tehran's nuclear program back by at least 2 years. Iran blamed this attack on the United States and Israeli forces; however, neither of these governments have officially claimed responsibility.

In 2012, two years after the discovery of STUXNET in Iran, a United States corporation confirmed that STUXNET had spread across its machines, leading to the usage of the term "Cyber Pearl Harbor" for the first time by the Defense Secretary of the US at the time. Using an analogy that builds a connection between a devastating event with the consequences of a possible future attack, the Defense Secretary highlighted the importance of cyber preparedness and warned the government on how a cyberattack could suddenly shut down the workings of the military and put the country in a vulnerable position, just like happened in Pearl Harbor.

When the STUXNET infection was first determined, the perpetrators of the attack had not yet been determined. However, upon investigation and 'reverse engineering' of STUXNET data to find the exact types of infrastructure software that were targeted, security analysts understood that the code was complicated to such an extent that the attackers had to be sponsored by a government to write it, which led to STUXNET's classification as a politically motivated attack. A few months after STUXNET's discovery in the US, the employees of an antivirus company were asked by a United Nations agency to investigate malware that had allegedly infected the computers of an Iranian oil company and destroyed their files. A worm that was initially assumed to have a different structure than STUXNET called "Flame" was soon understood to be responsible for this infection. Since experts were already alerted to the possible development of new malware with STUXNET-like consequences, it didn't take them too long to conclude that "Flame" was also a state-funded enterprise. Unlike STUXNET, Flame also could spread through Bluetooth and could better avoid detection by security network systems, making it more advanced, easier to spread, and harder to exterminate. According to David Kushner, the existence of such worms point to other issues aside from state-funded

political attacks— they show the extent of investments made on cybertools, whether they are used as weapons or protection mechanisms, and the necessity of stricter cybersecurity guidelines, considering that this trend is expected to increase in the future ("The Real").

3. Security Measures against Cyberterrorist Threats in the Information Age in the Americas

Starting from February 2006, the United States Department of Homeland Security (DHS) began practicing a simulation called the "Cyber Storm Exercise''once every two years in order to test the security of US defense mechanisms and the government's preparedness against a "digital espionage" attack. The exercise simulates what is expected to occur during a large-scale attack on areas ranging from utilities to infrastructure, with participants from communications, transportation, and energy production sectors. Over the last few years, some of the scenarios that were simulated as part of the Cyber Storm Exercise include the sudden interruption of signals being received by airport control towers, metro trains shutting down, and water supplies getting cut off. Analyzing the data from the first Cyber Storm simulation (Cyber Storm I) in 2006, the DHS found out that the nation's cyber defenses were insufficient as institutions interpreted these hindrances to be unrelated events rather than building a connection of national security between them. In the 15 years Cyber Storm trials were practiced, the contents of the simulation evolved according to the developments of technology and preferences of terrorists. For example, unlike the 2018 Cyber Storm, DDoS attacks and "catastrophic '' false propaganda were also simulated in the latest Cyber Storm in 2020.

While using the Internet helps terrorists to enlarge their web of recruits and supporters, it also puts them at greater risk of being caught by national security organizations such as the Federal Bureau of Investigations (FBI) of the United States. For example, the same data targeted to be obtained during a cyberattack can be used to track down the terrorists if that data is analyzed in statistically-significant quantities. To deal with cyberterrorists, infrastructures can essentially utilize two types of defense, called passive and active defense. Passive defense uses network security devices, such as firewalls and anti-virus software, to protect a device against threats without direct human interaction— it's the "first line of defense" terrorists have to pass through in order to penetrate into the target's device. After the passive defenses have been deactivated, active defenses need to be used in order to halt more advanced and sophisticated attacks. A team of security analysts and expert IT personnel analyze intelligence to prevent similar attacks from occurring in the future based on real-time information and past experience. Governments and organizations need to simultaneously use active and passive defense to properly establish the security of infrastructures and to minimize the impact of the attack.

IV. Key Vocabulary

Terrorism: Terrorism is all kinds of organized crime that result in mass civilian casualties or hinder the working mechanisms of governmental agencies. Terrorists, who are the individuals engaging in terrorist acts, can either work alone, represent the beliefs and motivations of a larger organization, or be supported by a national government to enact their attacks.

- Cyberterrorism is commonly known as an attack done on devices with the intent to create political, economic, or social damage. Unlike the common misconception, cyberterrorism is not limited to online platforms—physical changes that are facilitated through the Internet, such as making a device overheat, also count as cyberterrorism.
- Delegates should keep in mind that although there is a general understanding of what (cyber)terrorism means, an official definition has yet to be established.

Cyberspace: The abstract environment where computer networks are utilized to facilitate communication is called the "cyberspace". While the internet forms the largest part of cyberspace, phone systems, wireless networks, and satellites are also considered as elements of cyberspace considering their vast use of computer systems.

Cyberattack: A sub-category of cyberterrorism, cyberattacks target a computer network and "disrupt the integrity or authenticity of data, leading to errors" in the workings of a system by online means.

Data: Often targeted during cyberattacks, data is any kind of information that can be stored electronically and can be processed by a computer, such as credit card and social security numbers. Stolen data can result in identity theft and fraud.

Espionage: Obtaining sensitive information that is classified as "top-secret" by using human agents (spies) or technology, and using such information for political, economic, or personal benefit is called "espionage".

Malware: Shorthand for the term "malicious software", malware is a program that is specifically designed to "disrupt, damage or gain unauthorized access to a computer network" ("Malware"). Viruses, worms, and spyware are all types of malware.

Spear-phishing: According to Kaspersky, "spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business." The sent email often contains a link for a website that is contaminated with malware, and the target gets "spear-phished" as they click on that link. Attackers often use spear-phishing to steal data or install malware on the target's device ("What").

Distributed Denial of Service (DDoS): DDoS is a method of cyberattacking where a targeted network receives malicious traffic to the extent that it cannot be accessed or operated properly.

V. Important Events & Chronology

Date (Day/Month/Year)	Event
11 September 2001	The 9/11 Attack took place.
23 November 2001	The Convention on Cybercrime was signed.
1 July 2004	All signatories of The Convention on Cybercrime were asked to implement the principles of this treaty within their respective states, putting it into effect.
2006	The first Cyber Storm simulation was enacted by the United States.
2010	The STUXNET malware was first discovered in Iranian computer systems.
October 2012	The Use of the Internet for Terrorist Purposes was published by the UNODC.

VI. Past Resolutions and Treaties

The Convention on Cybercrime, 2001

- The first international treaty addressing cybercrimes, The Convention on Cybercrime, defined punishable Internet offences and aimed to ensure cooperation between signatories in case of a cyberattack. For more information on The Convention on Cybercrime, referral to the “Failed Solution Attempts” section of this report is advised.

The United Nations Global Counter-Terrorism Strategy **(A/RES/60/288)**, September 8, 2006

- Focusing on combating terrorism, The United Nations Global Counter-Terrorism Strategy asked all involved Member States to become parties to existing protocols and conventions against terrorism, ensure the lawful prosecution of terrorists, and utilize the Internet in developing international cooperation and curbing terrorism. In the recent reviews of this document, particularly in the sixth review **(A/RES/72/284)**, the increase in the terrorist use of the Internet was highlighted.

Technical assistance for implementing the international conventions and protocols related to counter-terrorism **(A/RES/66/178)**, December 11, 2011

- With this resolution, the United Nations Office on Drugs and Crime was urged to enhance its technical and legislative assistance to Member States in combating terrorism underlined in The United Nations Global Counter-Terrorism Strategy. Such legislative assistance includes helping nations develop the proper framework to handle the terrorist use of the Internet. To that end, the UNODC has published a document titled **"The Use of the Internet for Terrorist Purposes"** in October 2012, which includes case studies and specific security measures the UNODC advises Member States to adopt for eradication of cybercrimes, as elaborated on previously in this report.

VII. Failed Solution Attempts

Since terrorist use of the internet is a relatively new issue in the governmental agenda, not many solution attempts have been put in place to specifically address cyberterrorism. However, some diplomatic examples of treaties aiming to address general cybercrime do exist, such as the Convention on Cybercrime.

In 2001, The Convention on Cybercrime, the first international treaty aiming to address the criminal use of technology and the internet was signed in Budapest. This convention primarily aimed to build a common framework for punishing cybercriminals, specifically the ones responsible for Internet fraud and network security violations, by suggesting the implementation of new legislation and fostering international cooperation. Security measures that should be taken in response to cyberterrorist threats, such as legally and selectively tracking the Internet activity of suspects were also mentioned in The Convention on Cybercrime. Besides including terms on the proper utilization of technology for investigations, the Convention deemed "illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery and computer-related fraud" illegal and demanded each signatory state to set up an international network that would be accessible 24/7 to encourage cooperation in response to cyberattacks. The Convention on Cybercrime has been ratified by the United States, Canada, Argentina, Peru, Colombia, Chile, Costa Rica, Paraguay, and the Dominican Republic in the Americas at different points in time since 2001. Brazil and Guatemala also became observer states, with Brazil showing its lack of participation in the composition process of the treaty as the reason for not ratifying the convention. In

Considering that cases of cybercrime have grown exponentially since the publication of this treaty, it can be concluded that this convention fell short in preventing the terrorist use of the Internet. First of all, as understood from its title, The Convention on Cybercrime covers a much larger scope of Internet crimes than cyberterrorism within its terms, making it harder to establish a detailed framework with a specific focus on cyberterrorism. Additionally, as mentioned multiple times in this report, the fact that terrorism does not have

an official international definition is one of the primary reasons why more specific and international legislation on the terrorist use of the Internet has not been debated upon yet. Another factor that has made The Convention on Cybercrime fail might be its allowance of exploiting the networks of a Member States by others— instead of fostering international cooperation, some Member States might fear that these networks could be used for the initiation of cyberwarfare or infringement of territorial integrity by their opponents. Lastly, it's important to consider that this convention has been conducted 20 years ago, earlier than when most of the malware systems that threat governments were invented; therefore, The Convention on Cybercrime does not provide Member States with a sufficient framework to combat more recent methods of cybercrime such as DDoS attacks, making it relatively outdated. In an attempt to make this convention on par with the recent cybersecurity threats, Russia has drafted another treaty on cybersecurity called "United Nations Convention on Countering the use of Information and Communications Technologies for Criminal Purposes" in August 2021.

VIII. Possible Solutions

The first, and perhaps, most essential step of combating the terrorist use of the Internet is defining terrorism. Although it would be considerably difficult to bring all Member States on the same page about what actions consist of terrorism as Member States have different criminal policies, states should be urged to come together to concur on a definition of terrorism that would combine their varying definitions and not go against their existing national policies. After the majority of Member States implement this new definition into their legislation, a more *terrorism*-specific version of the Convention on Cybercrime can be drafted, or the Convention on Cybercrime can be amended such that a new section solely focusing on punishments for cyberterrorist crimes is added to the treaty. To achieve international Internet security, Member States should collaborate with related organizations and UN agencies to get assistance on implementing active and passive defence mechanisms. However, delegates should keep in mind the sovereignty of Member States must be respected in every instance of international cooperation.

As stated in the "Involved Countries" section of this report, the United States is the hub of infrastructure in the Americas, which creates a misconception where other Member States with developing infrastructure and economies, such as Mexico and Brazil, are seen to be less prone to cyberattacks. While all of the documented cyberattacks have targeted the US in the past, hence making this report partially US-centric, the US actually is currently more prepared towards cyberattacks due to their experiences, making attackers shift their target on other parts of the Americas with underdeveloped cybersecurity systems. Therefore, all Member States should acknowledge that they might be threatened with cyberattacks and take precautions accordingly. Such precautions might include establishing different versions of the

Cyber Storm simulation, whose recurrence and scope might differ according to the economic or technological status of the Member States. Lastly, after becoming aware of the danger of cyberattacks themselves, governments must work to raise awareness within their citizens and companies, especially the ones who operate and build the infrastructure, since those systems are often controlled over the Internet and have a default password, making them accessible if these passwords are not changed, which is the case more often than it is not.

IX. Useful Links

A 2006 publication summarizing the principles and practices of the Cyber Storm exercise by the United States Department of Homeland Security:

- https://cryptome.org/cyberstorm.pdf

Complete text of the UNODC's "The Use of the Internet for Terrorist Purposes" document:

- https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity

An article summarizing the guideline the International Criminal Police Organization (INTERPOL) follows to prevent terrorist use of the Internet as well as giving information on INTERPOL's collaboration with the United Nations Counter-Terrorism Centre (UNCCT):

- https://www.interpol.int/Crimes/Terrorism/Analysing-social-media

A chronologic list of significant cyber incidents from November 2020 to October 2021:

- https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

X. Works Cited

"About CISA." Cybersecurity and Infrastructure Security Agency CISA,

https://www.cisa.gov/about-cisa.

“Analysing Social Media.” INTERPOL,

https://www.interpol.int/Crimes/Terrorism/Analysing-social-media.

“Balancing Passive and Active Cybersecurity Measures.” LookingGlass Cyber Solutions Inc.,

https://lookingglasscyber.com/blog/threat-intelligence-insights/balancing-passive-active-cybersecurity-measures/.

Brenner, Susan W. “Cybercrime, Cyberterrorism and Cyberwarfare .” cairn.info,

https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.html.

Center for Strategic and International Studies. “Cybercrime Cyberterrorism Cyberwarfare: Averting an Electronic Waterloo.” Cybercrime Cyberterrorism Cyberwarfare: Averting an Electronic Waterloo | Office of Justice Programs, https://www.ojp.gov/ncjrs/virtual-library/abstracts/cybercrime-cyberterrorism-cyberwarfare-averting-electronic-waterloo.

“Covid-19 Cyberthreats.” International Criminal Police Organization (INTERPOL),

https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats.

“Cyber Criminals are Targeting Latin America.” Cyber Security Intelligence,

https://www.cybersecurityintelligence.com/blog/cyber-criminals-are-targeting-latin-america-4412.html.

“Cybersecurity | Office of Counter-Terrorism.” United Nations, United Nations,

https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity.

“Cyberterrorism.” Cyber Terrorism - an Overview | ScienceDirect Topics,

https://www.sciencedirect.com/topics/computer-science/cyber-terrorism.

Department of Homeland Security: Cyber Storm Fact Sheet.

https://www.hsdl.org/?view&did=476170.

"Details of Convention on Cybercrime (Treaty No. 185)." Treaty Office, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

Goldman, Emily O., and Michael Warner. "Why a Digital Pearl Harbor Makes Sense and Is Possible Understanding Cyber Conflict: 14 Analogies." Carnegie Endowment for International Peace, 16 Oct. 2017, https://carnegieendowment.org/2017/10/16/why-digital-pearl-harbor-makes-sense-.-.-.-and-is-possible-pub-73405.

Kajal, Abhishek. "Total Malware Infection Growth Rate in Millions." Research Gate, https://purplesec.us/resources/cyber-security-statistics/.

Kaspersky. "What Is Spear Phishing?" www.kaspersky.com, 13 Jan. 2021, https://www.kaspersky.com/resource-center/definitions/spear-phishing.

Kushner, David. "The Real Story of STUXNET." IEEE Spectrum, IEEE Spectrum, 29 July 2021, https://spectrum.ieee.org/the-real-story-of-stuxnet.

"Malware." Oxford Advanced Learner's Dictionary, https://www.oxfordlearnersdictionaries.com/definition/english/malware#:~:text=malware-,noun,system%20without%20the%20user%20knowing.

Matusitz, Jonathan. "[PDF] Cyberterrorism:: How Can American Foreign Policy Be Strengthened in the Information Age?: Semantic Scholar." Taylor and Francis, 1 Jan. 1970, https://www.semanticscholar.org/paper/Cyberterrorism%3A%3A-How-Can-American-Foreign-Policy-Be-Matusitz/04ac8acb62a406a32c3ba3a498513a78f9cc5afc.

"National Cyber Exercise: Cyber Storm." United States Department of Homeland Security,

https://cryptome.org/cyberstorm.pdf.

Parraguez-Kobek, Luisa. “The State of Cybersecurity in Mexico: An Overview.” Wilson Center, https://www.wilsoncenter.org/publication/the-state-cybersecurity-mexico-overview.

“Parties/Observers to the Budapest Convention and Observer Organisations.” Cybercrime, https://www.coe.int/en/web/cybercrime/parties-observers.

“Technical Assistance for Implementing the International Conventions and Protocols Related to Counter-Terrorism (A/RES/66/178).” A/RES/66/178, https://undocs.org/en/A/RES/66/178.

“Terror on the Internet: Questions and Answers.” *United States Institute of Peace*, 17 Oct. 2016, https://www.usip.org/publications/terror-internet-questions-and-answers.

“The United Nations Global Counter-Terrorism Strategy (A/RES/60/288).” United Nations, https://undocs.org/A/RES/60/288.

“The Use of the Internet for Terrorist Purposes.” United Nations Office on Drugs and Crime, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

“Use of the Internet.” United Nations : Office on Drugs and Crime, https://www.unodc.org/unodc/en/terrorism/news-and-events/use-of-the-internet.html.

Weimann, Gabriel. “Cyberterrorism: How Real Is the Threat.” United States Institute of Peace, https://www.usip.org/sites/default/files/sr119.pdf.