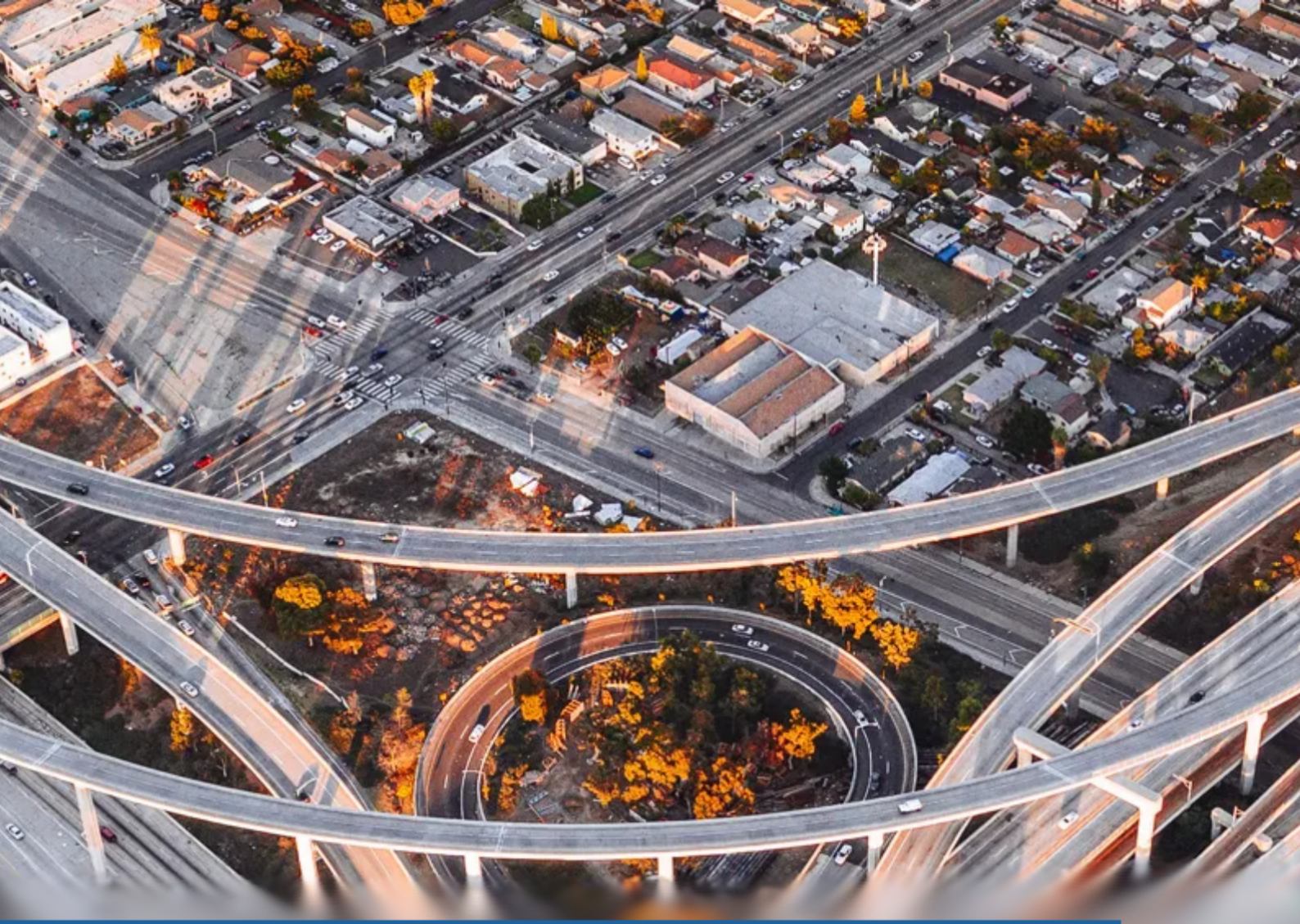

Preventing terrorist cyber attacks against critical infrastructure

UNODC

Betty Leskova
Main Chair

Forum: United Nations Office on Drugs and Crime (UNODC)

Issue: Preventing terrorist cyber-attacks against critical infrastructure

Name: Betty Leskova

Position: Main Chair

Introduction

In the past 50 years technology has been developing at a rapid rate. We have managed to go from only the highest-ranked laboratories having computers, to now, many individuals requiring computers for their day-to-day jobs. Despite technological advancements in the past half century, crime has also adapted to the growing demand for technology, and everyday crime has gone from robbing banks to cyber-attacks and hacking banking accounts. With such crime causing much larger impacts, it is important that we are able to take steps as a society to adapt to technological crime, to prevent large infrastructure from being affected. Specifically with the increase in global conflict, and terrorist attacks it is especially important that we are able to protect our infrastructures from those wishing to destroy them.

A cyber-attack is defined as “an intentional effort to steal, expose, alter, disable, or destroy data, applications or other assets through unauthorized access to a network, computer system or digital device” ("What Is a cyber-attack?"). The first famous instance of cybercrime occurred in 1976 when Kevin Mitnick hacked into The Ark and made copies of confidential documents (Chadd). He was later arrested, however this instance of cybercrime called for increased computer security. The first computer was made in 1943, however computer security was only first thought about in the 1970s (Chadd). After several instances of hacking and the first accounts of cybercrime in the 1970s, engineers and experts in computer science focused on improving the security of computers, and for over 20 years they were successful (Chadd). Expert scientists however could not have protected the world from the 1990s, when the majority of the world went online. This meant that the majority of large and successful companies began to use computer software to speed up their processes and to allow tedious and repetitive tasks to be digitized. This however brought along with it, a large increase in cybercrime. With the majority of the world being digital, cybercriminals had opportunities to break into the majority of companies through their software (Chadd). Cybercrime has continued to this day, with a large uprising from 2020 onwards when the majority of jobs and companies had to go digital due to the Covid-19 pandemic (Chadd). Now there are more cyber-attacks

than ever before, so protecting companies and infrastructure is crucial to preserve society as we know it. This Research Report will focus on the issue of cyber-attacks specifically, those caused by terrorists on critical infrastructure. This Report will also offer some solutions on this topic and background information on the issue of preventing these terrorist cyber-attacks.

Definition of Key Terms

Antivirus

A type of program that is designed to find and remove viruses that have infected a piece of technology (Dube)

Computer Network

Two or more computers that are connected with one another to communicate data with each other ("Computer Network")

Computer Virus

A type of software that aims to spread between computers and technology to cause damage to data and software ("What Are Computers")

Crime

An activity that one commits which does not abide by the laws of the region/country they committed the action in ("Crime")

cyber-attack

An intentional effort to steal, expose, alter, disable, or destroy data, applications or other assets through unauthorized access to a network, computer system or digital device ("What Is a cyber-attack?")

Digitalization the process of converting a region, city, or country into using technology for the majority of processes ("Digitalization")

Infrastructure

A basic physical structure in either a business or a region which is often associated with the production of goods and services (Boyle)

IT (Information Technology)

The use of computers, and other electronic devices to send and store information (also often associated with a specific group of people who have knowledge/actively do this) ("Information Technology")

OT (Operational Technology)

The hard/software that directly monitors and controls digital devices and infrastructure within a designated region ("How Do OT and IT Differ?")

Security

The protection of infrastructure or an organization (in this case) against threats such as criminal attacks or attacks by terrorists ("Security")

Software

A set of instructions, or programs that a computer abides by allowing it to fulfill its functions and execute specific tasks (Rosencrance)

Terrorism

The calculated use of violence creating a general fear in a population to achieve a particular political objective ("Terrorism")

General Overview

On a global scale, cyber-attacks affect millions of people, for various reasons, and it is therefore critical that member nations understand how and why they are so impactful. Not only do cyber-attacks affect citizens, but also critical infrastructures, whose damage often costs a lot of money to restore. These critical infrastructures are named ‘critical’ as they have a large impact on nations. Their damage impacts many citizens of a nation. Therefore, nations have worked tirelessly in the past to prevent cyber-attacks on critical infrastructure and while some have been successful, others have not. Through the digitalization of the world, terrorists have resorted to technology to attack nations. For this reason, it is critical that we act now, in order to establish cyber security that can protect member nations for years to come, and create programs that can prevent terrorist cyber-attacks. There are however some obstacles to this, which is why some nations have not been successful in attaining this goal. These include; reasons for terrorist cyberattack occurrence, method of this occurrence, and consequences of these attacks. In order to understand the topic at hand it is primarily crucial to understand the reason why terrorist cyber-attacks occur;

Reasons for terrorist cyber-attack occurrence

In the day-to-day, cyber-attackers attack citizens to gain something, such as blackmail, finances, or leverage on specific people. However, terrorist cyber-attacks are different in this regard, as they are not caused by someone's want for financial gain, but rather a desire for chaos and fear amongst the citizens of a nation. One can not see terrorist cyber-attacks coming, as just like physical terrorist attacks, they are unpredictable, which is part of the reason why they are so difficult to prevent. With cyber-attacks, terrorists can cause much more destruction than physical attacks, which is why they nowadays, often resort to technology to evoke fear (Bergen). The reason behind them wanting to evoke this fear is due to their dislike or disagreement with policies, religions, actions of a nation, or actions of a specific politician (Bergen). They believe that therefore, attacking this nation's critical infrastructure is a means of "getting back" at the nation for whatever their wrong actions were (Bergen). It is important to note that motivations for terrorist attacks vary based on the person committing them, but they can be grouped into the sections mentioned previously. Oftentimes, those who commit acts of terrorism, whether they be with technology or physically, are in a state of their life where they believe they are powerless but want to act on problems they see in the world (Bergen). They resort to violence to do this, meaning that while they may create fear, the attacks they commit never really change the policies or other things they originally wanted to change. Furthermore, some terrorists have mental health issues, which causes them to want to commit acts of violence (Bergen). Lastly, in terms of terrorism, it is important to understand that terrorist attacks are methodologically planned out, to create the maximum amount of fear possible.

Cyber-attacks are different from physical terrorist attacks, in that they are much more powerful. A single cyber-terrorist attack can destroy a whole infrastructure, which is not like physical terrorist attacks. One should also however consider that terrorist cyber-attacks are much harder to carry out. A terrorist cyber-attack has the same purposes as a physical terrorist attack does, however it uses computers, networks, and technology to commit the attack. There are many motivations for terrorist cyber-attacks, however most motivations are either political, religious, or caused by differing beliefs. The main objective of terrorist cyber-attacks is to harm critical infrastructure to a point where the technology in them completely breaks down and causes chaos and long-term harm. It should be noted that cyber-attacks not only harm technology, they also cause injuries or casualties to those working in or simply in the critical infrastructures. For example, if a hospital's technology were to be attacked, many would perish as a result of the necessity for technology in hospitals. Cyberterrorists often attack infrastructures such as hospitals or other crucial infrastructures like banks, and governmental buildings. It is important to realize that while terrorist cyber-attacks may be carried out by an individual, they may also be carried out by governments. In the case of governments carrying out these attacks, the motivations are often political, in order to harm the other

nation. Governmental cyber-attacks however occur much less often, but are also much more extreme and have much larger consequences.

Method of terrorist cyber-attack occurrence

While there are many ways of carrying out a cyber-attack, only the main 4 methods will be discussed below. These 4 methods include; Advanced persistent threat (ATP) attacks, Malware, Denial of Service (DoS) attacks, and Hacking to find important/classified information (*Gülen*). All 4 of these methods may be used to attack critical infrastructures, however, Malware and DoS attacks are used most frequently (*Gülen*). Malware works based on computer worms and viruses, which once they enter a network of computers, they specifically target IT control systems (*Gülen*). Once the virus/computer worm attacks the IT control systems, then the whole network breaks down, and no longer functions for a certain amount of time depending on how well the virus/computer worm was able to get through the network's cyber security systems (*Gülen*). Malware attacks are most often employed when attacking either transportation networks, power systems, or critical infrastructure (*Gülen*). The 2nd most common type of terrorist cyberattack are DoS attacks. These attacks mainly target governments and vital infrastructure (*Gülen*). They work based on preventing authorized users from accessing specific technology such as computer networks, devices, or critical systems (*Gülen*). In this sense, the attacker can do whatever they want with the network in the place being attacked. This type of attack has the potential to harm most people, as critical processes in infrastructures can be stopped, meaning that whole systems break down and therefore the whole infrastructure can begin to malfunction (*Gülen*). Therefore, these attacks can be considered the most dangerous of all 4 that are being mentioned (*Gülen*). Advanced persistent threat attacks are also very dangerous, as they are persistent attacks on a network of technology (*Gülen*). APT attacks use specific techniques to enter networks (*Gülen*). Once inside, attackers steal data from the network about specific people, or systems, without being discovered (*Gülen*). The main problem with APT attacks is that it is very difficult to find the person/people who carried them out (*Gülen*). For this reason, the attacker can persist in stealing more information without any change to the network, so they are practically undetectable (*Gülen*). APT attacks mainly target governments and military systems due to their anonymous attacking nature. Lastly, hacking, the most known type of terrorist cyber-attack (*Gülen*). While it is widely known, this type of attack is not as effective in gaining information and causing harm as the others previously mentioned. The main objective of hacking is to gain important governmental, or organizational information (*Gülen*). However, due to its 'popularity', there are many systems in place to prevent hacking from occurring (*Gülen*). For this reason, hacking is not as likely to occur, and is also as dangerous as the other types of attacks.

Consequences of terrorist cyber-attack occurrence

As was discussed previously, terrorist cyber-attacks are often chosen for their ability to create a large sense of fear in a certain population. It can therefore be inferred that terrorist cyber-attacks have many consequences, ultimately causing fear in citizens and governments. The specific consequences of terrorist cyber-attacks on critical infrastructures are as follows; physical/digital, economic, psychological, reputational, and social ("Researchers identify"). Each of these categories encompasses the consequences of a terrorist cyber-attack on critical infrastructure. Beginning with physical/digital consequences, when a network is attacked the likelihood of it returning to its original state, especially with large security breaches ("Researchers identify"). The damage to the infrastructure is irreversible and oftentimes causes deaths as well as injuries ("Researchers identify"). Economic consequences include reduced profits for governments in an area that the critical infrastructure aided in, a fall in stock price, and large amounts of money used by the government to restore the infrastructures ("Researchers identify"). These economic consequences cause further social impacts such as; disruption of citizens' daily lives, and negative perceptions of technology within the population ("Researchers identify"). Reputational impacts also have large effects, especially when information is released on politicians or leaders of a nation ("Researchers identify"). This can cause a long-term change in government, a damaged trust of the people in the government, or a decreased trust in other nations of the government/nation which was attacked ("Researchers identify"). Lastly, the psychological impacts also impact people, just like the social impacts. Psychological consequences of terrorist cyber-attacks include individuals feeling powerless or depressed, and an increase in fear of the people which can in some cases cause mass hysteria ("Researchers identify"). All of these consequences have large impacts on nations experiencing them, and can even have long-term effects on nations' relations. Especially due to the increasing number of terrorist cyber-attacks, it is critical that we are able to work towards preventing them and creating a more secure cyber world for all nations (Gülen).

Timeline of Key Events

The timeline below shows the most relevant events and their dates in relation to the issue at hand. It covers the whole timeline of cyber-attacks.

Date	Event
1943	The first all-digital computer is created for MIT
1946	The first computer network is created by Bell Laboratories
1970s	Expert scientists start thinking of creating computer "security"
1971	Bob Thomas creates the "Creeper", the first virus software

1976	The first famous cyber-attack where Kevin Mitnick hacks the “Ark”
1982	CIA attacks the Siberian Pipeline, the first worldwide cyber-attack
1987	The first computer antivirus is created by three Czechoslovaks
1990s	The world for the first time goes digital due to increased access to personal computers
1996	Organized crime units start to resort to technology for stealing governmental and personal information
2003	Crime organizations start largely funding professional cyber-attacks
2020	The global pandemic and digitalization causes a rise in cyber-attacks that have continued to the present
2021	Due to increase in cyber-attacks, cybersecurity start to massively grow
2021	The Colonial Pipeline, critical US infrastructure is hacked by terrorists
November 2023	Chinese hackers attack Japan’s space operations (most recent terrorist cyber-attack as of December 2023)

Major Parties Involved

Denmark

In terms of security and preventing terrorist cyber-attacks, Denmark is the leading nation in the world. This achievement can be acclaimed for its high level of digital development, and its relatively low number of cyber-attacks on governmental infrastructure (Maddison). After a large cyber-attack in 2016 which caused much of the Danish government to resign due to blackmail caused by the group behind the attack (Venkina). They gained a lot of information on the Danish military (Venkina). Since then Denmark has worked towards becoming more secure in its information and networks, and over time has led it to be the most cyber-secure country in the world (Venkina). The methods they use are quite different from those of the US and other cyber-secure nations. Denmark harnessed education to spread knowledge about cyber security to all of its citizens (Venkina). Furthermore, it defined its critical infrastructures allowing workers there to be fully prepared for emergency situations (Venkina). Such methods, if used worldwide, could allow all nations to improve their cyber security, and work towards minimizing the number of terrorist cyber-attacks on governmental institutions. For this reason, Denmark should be taken as a model for cyber security, and should be consulted with to create resolutions on the topic at hand.

People's Republic of China (China)

As the second most powerful nation in the world in technology, after the USA, China is the most powerful in cyber surveillance as well as cyber power specifically in commerce. China is not any less experienced in relation to technology than the USA, however, due to the low number of cyber-attacks on them, they are not as knowledgeable on cyber security. China has largely grown its "cyber expertise through research and development, and public-private partnerships" ("Top 10 Most"). Due to the majority of cyber security companies, or technological companies being privately owned, establishing governmental and private company partnerships is one of the reasons China is able to be so successful in the area of technology as well as cyber. Another reason for its success is the funding it puts into research and development of cyber programs and networks ("Top 10 Most"). For these reasons, China can be thought of as one of the leading powers of cyber. Despite them not having much knowledge about cyber security, they are very knowledgeable about cyber in general and technology.

Russian Federation (Russia)

Along with China and the USA, Russia was, for a long time, perceived to be one of the leaders in technology. While the Russian Federation has a large amount of varying technology and information when it comes to cyber-attacks and security, there have been allegations in the past criticizing the nation's use of the information it has, following the beginning of the Russo-Ukrainian war on the 24th of February 2022. In the past, the Russian Federation had been accused of misusing information regarding technology, however, the nation still has a large amount of knowledge about technology, cyber, and cybersecurity. The Russian Federation is currently one of the most cyber secure countries in Asia. The Russian Federation mainly uses its cybersecurity strategies by itself, however if they were to cooperate with other nations, their cybersecurity measures and tactics would be highly helpful to other nations. Therefore, Russia should be considered as an example of how cybersecurity can be used to effectively protect a nation.

United States of America (USA)

As the country with the most overall number of cyber-attacks, the USA has dealt with many issues in relation to aiming to prevent these cyber-attacks. Over the past 16 years, the USA has had a total of 156 (known) cyber-attacks on critical infrastructure (Ang). There are multiple accounts of cyber-attacks in the USA some of which included terrorists hacking into The Pentagon (where the majority of USA classified governmental information is stored). Over the past 50 years, US networks have been a target for attacks by hackers and terrorists (Chadd). This however also means that the USA has a lot of experience with cyberattacks and is doing all that it can to prevent future ones. The US has done quite a lot in order to ensure that their citizens are aware of the risks of cyber-attacks on them as individuals as well as businesses, which means that they as a nation are aware of the great dangers that these attacks pose (from

experience). Most recently, the US government has employed a new cyber security strategy, which aims to protect critical infrastructures, and collaborate with other nations and businesses to counter threats to their digital systems, in March 2023 and have thus far prevented any dangerous cyber-attacks on critical infrastructure (Joshi and Dobrygowski). In this regard, the USA should be taken as an example of what can be accomplished with the right steps. However, despite these security strategies, the US has also in the past hacked into other nations critical infrastructures in order to gain information, such as in 1982 where the CIA caused a massive explosion in the Siberian pipeline due to deliberately tampering with its software (Keefe). This should be taken into account when looking at the US for aid. While the nation does know a lot about cyber-attacks, they have, in some instances, misused this information. Overall, the USA has a large amount of knowledge about terrorist cyber-attacks, and should most definitely be consulted in any strategies and policies created for preventing these attacks in the future.

United Nations Office on Counter-Terrorism (UNOCT)

Similarly to the UNODC, the UNOCT aims to prevent any terrorist attacks, including any terrorist attacks, including those digitally. While they do not focus on terrorist cyber-attacks, they have the same aim as nations in the UNODC and should therefore be considered when creating a resolution on the issue at hand. The UNOCT is part of the General Assembly and its main aim is to “enhance coherence” across the world in security against terrorism ("Cybersecurity and New Technologies"). The UNOCT has many strategies such as annual reports, enhancing the capacities of nations to prevent cyber-attacks, and strengthening the capacities of law enforcement in the area of digital crime ("Cybersecurity and New Technologies"). Their strategies have been thus far effective in preventing many attackers from entering and destroying critical infrastructures, and should therefore be included in potential solutions in the Office’s resolutions.

Possible Solutions

The largest problem with the current approach to cybersecurity and therefore also preventing cyber-attacks, is that the current coordinated efforts and softwares that prevent/minimize cyber-attacks are privately owned, meaning that they may stop businesses from being affected, but countries and critical infrastructure is not protected (Rosencrance). For this reason, it is crucial that nation leaders of address the gaps in cybersecurity in their infrastructures and take steps like creating policies or protocols to modernize their IT and OT systems (Rosencrance). For example, the European Union published cybersecurity guidelines in 2020, which focused on critical infrastructure and industries had a strict set of regulations they must follow in regards to protection of them (Rosencrance). Similar guidelines can be implemented worldwide,

with more elaboration to help prevent terrorist cyber-attacks. This is however easier said than done, as some nations have larger priorities than cybersecurity. Precisely for this reason should delegates aim to aid those countries who are not as mindful of their cybersecurity, to achieve worldwide cybersecurity in all nations of the Office.

Another method of preventing terrorist cyber-attacks against critical infrastructure is ensuring that these critical infrastructures are as protected as possible (Rosencrance). This can either be done through implementing regular cybersecurity checks and ensuring that all critical infrastructures are up to date on the most recent cybersecurity possible. Oftentimes not all infrastructures' security is updated, resulting in a weakened line of defense that terrorists and hackers can more easily get into. For this reason, your solution should include checking up on the cybersecurity of all critical infrastructures. Especially if these regular checkups would mean that more modern cybersecurity is achieved. Many governments have scientists and technology specialists who are working towards safer computer networks for their governments. If these efforts were to be worldwide they would be much faster and much more effective. Expanding efforts for security in critical infrastructure on a worldwide scale would be beneficial to all nations, and would therefore pose a good solution to the topic at hand.

It is also crucial that workers in critical infrastructures are trained in case a cyber-attack occurs. Regular training would provide knowledge for emergency situations, so that if infrastructures were attacked, then there is a larger chance that they are not as damaged, if workers know what to do in the event of a cyber-attack. Having an organization in these infrastructures is further beneficial, as then, technology workers in these infrastructures would know where attacks have occurred and therefore how to prevent them from breaking too much into the infrastructure (MacLeod). Organization would also allow for the simplification of the computer networks in critical infrastructures, meaning that specialists could better understand and also protect these networks from being attacked.

Lastly, it is important that governments recognize the importance of cybersecurity in their countries, as without this, any efforts for cybersecurity would be pointless. Politicians need to be made aware of the threats that terrorist cyber-attacks pose, to best protect their infrastructures from them. This could be achieved through regular governmental meetings on the issue of cybersecurity, or even regular meetings within the United Nations on the issue in the Office of Counter-Terrorism for example ("Cybersecurity and New Technologies"). That way, all nations would be involved, as in reality, no nation wants to be affected by terrorist cyber-attacks, and working together for cybersecurity would be the best way for nations to share their resources and security tactics (even though some may be against this, which delegates should consider).

Bibliography

Please see the bold sources below for useful information on the issue at hand, that can help you with any further research.

Ang, Carmen. "The Most Significant cyber-attacks from 2006-2020, by Country." *Visual Capitalist*, 10 May 2021, www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/. Accessed 20 Dec. 2023.

Bergen, Peter. "Why Do Terrorists Commit Terrorism?" *The New York Times*, The New York Times Company, 14 June 2016, www.nytimes.com/2016/06/15/opinion/why-do-terrorists-commit-terrorism.html. Accessed 21 Dec. 2023.

Boyle, Michael J. "Infrastructure." *Investopedia*, Dotdash Meredith, 27 Sept. 2023, www.investopedia.com/terms/i/infrastructure.asp. Accessed 20 Dec. 2023.

Chadd, Katie. "The history of cybersecurity." *Avast*, Avast Software, 24 Nov. 2020, blog.avast.com/history-of-cybersecurity-avast#the-1940s. Accessed 18 Dec. 2023.

"Computer Network." *Encyclopaedia Britannica*, Britannica, www.britannica.com/technology/computernetwork. Accessed 20 Dec. 2023.

"Crime." *Cambridge Dictionary*, Cambridge University Press, dictionary.cambridge.org/dictionary/english/crime. Accessed 20 Dec. 2023.

"Cybersecurity and New Technologies." *United Nations Office on Counter-Terrorism*, United Nations, www.un.org/counterterrorism/cybersecurity. Accessed 20 Dec. 2023.

Davies, Vikki. "The History of Cybersecurity." *Cyber.*, 4 Oct. 2021, cybermagazine.com/cybersecurity/history-cybersecurity. Accessed 20 Dec. 2023.

"Digitalization." *Merriam-Webster Dictionary*, Merriam-Webster, www.merriamwebster.com/dictionary/digitalization. Accessed 20 Dec. 2023.

Dube, Ryan. "What Is Antivirus?" *Lifewire*, Dotdash Meredith, 5 Nov. 2019, www.lifewire.com/what-isantivirus-software-152947. Accessed 20 Dec. 2023.

Greig, Jonathan. "Ukraine, Israel, South Korea top list of most-targeted countries for cyberattacks." *The Record*, The Record from Recorded Future News, 6 Oct. 2023, therecord.media/microsoft-2023report-countries-most-targeted-cyberattacks. Accessed 20 Dec. 2023.

Gülen, Kerem. "The war never ends on the cyber front." *Data Economy*, 11 Oct. 2022, dataconomy.com/2022/10/11/cyber-terrorism-definition-attacks/. Accessed 21 Dec. 2023.

"How Do OT and IT Differ?" *Cisco*, Cisco Systems, www.cisco.com/c/en/us/solutions/internet-ofthings/what-is-ot-vs-it.html. Accessed 20 Dec. 2023.

"Information Technology." *Cambridge Dictionary*, Cambridge University Press, dictionary.cambridge.org/dictionary/english/information-technology. Accessed 20 Dec. 2023.

Joshi, Akshay, and Daniel Dobrygowski. "The US has announced its National Cybersecurity Strategy: Here's what you need to know." *World Economic Forum*, 9 Mar. 2023, www.weforum.org/agenda/2023/03/us-national-cybersecurity-strategy/. Accessed 20 Dec. 2023. Keefe, Mari. "Timeline: Critical infrastructure attacks increase steadily in past decade." *Computer World*, IDG Communications, 5 Nov. 2012, www.computerworld.com/article/2717553/timeline--criticalinfrastructure-attacks-increase-steadily-in-past-decade.html. Accessed 20 Dec. 2023.

MacLeod, Calum. "How to Combat Cyber-Terrorism." *The Guardian*, Guardian News and Media, 29 Nov. 2010, www.theguardian.com/technology/blog/2010/nov/29/combat-cyber-terrorism. Accessed 20 Dec. 2023.

Maddison, Lewis. "These are the countries most at risk from cyberattacks." *Techradarpro*, Future US, 4 Dec. 2023, www.techradar.com/pro/security/these-are-the-countries-most-at-risk-from-cyberattacks. Accessed 20 Dec. 2023.

Mutune, George. "8 cyber-attacks on Critical Infrastructure." *Cyber Experts*, CyberExperts.com, cyberexperts.com/cyber-attacks-on-critical-infrastructure/. Accessed 20 Dec. 2023.

"Researchers identify negative impacts of cyber-attacks." *University of Oxford*, 29 Oct. 2018, www.ox.ac.uk/news/2018-10-29-researchers-identify-negative-impacts-cyber-attacks. Accessed 21 Dec. 2023.

Rosencrance, Linda. "What Is Software?" *Tech Target*, TechTarget, www.techtarget.com/searchapparchitecture/definition/software. Accessed 20 Dec. 2023.

"Security." *Cambridge Dictionary*, Cambridge University Press, dictionary.cambridge.org/dictionary/english/security. Accessed 18 Dec. 2023.

"Significant Cyber Incidents." *CSIS*, Center for Strategic and International Studies, 2023, www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Accessed 20 Dec. 2023.

"Terrorism." *Encyclopaedia Britannica*, Britannica, www.britannica.com/topic/terrorism. Accessed 18 Dec. 2023.

"Top 10 Most Powerful Countries in Cyberspace." *Secure World*, Seguro Group, 15 Sept. 2022, www.secureworld.io/industry-news/top-10-most-powerful-countries-in-cyberspace. Accessed 20 Dec. 2023.

Venkina, Ekaterina. "How Denmark became the most cyber-secure country." *IPS*, Friedrich Ebert Stiftung, 20 July 2021, www.ips-journal.eu/work-and-digitalisation/how-denmark-became-the-most-cybersecure-country-5290/. Accessed 20 Dec. 2023.

"What Are Computer Viruses?" *Fortinet*, www.fortinet.com/resources/cyberglossary/computer-virus.

Accessed 20 Dec. 2023.

"What Is a Cyberattack?" *IBM Security*, IBM, www.ibm.com/topics/cyber-attack. Accessed 18 Dec. 2023.