# SECURITY COUNCIL

## Topic B: Threats to International security caused by criminal capacity on cyber-terrorism

INTRODUCTION

Security Council is one of the six main organs of the United Nations. Security Council was created on October 24th, 1945, with the main purpose of maintaining international peace and security and to avoid the threatening against such. Besides its main purpose, it has three others, which are: to develop friendly relations among nations, to cooperate solving international problems and promote respect, and to be the center for harmonizing the actions of nations. This UN organ has in total 15 members, from which 10 are non-permanent and the other 5 are permanent members with veto power: United States, France, Russia, China, and the United Kingdom. The veto power means that any of the 5 permanent members can reject, absent or change any solution given by the committee. (UN, n.d.)

As the world is progressively moving forward into a society even more reliant on technology, the risk of becoming victims of multiple cyber attacks through internet increases, users, companies, and government systems are the most common targets. These attacks are known as cyber-terrorism. Cyber-terrorism is defined as an illegal online invasion against internet information, computer programs, and even governmental platforms. As a consequence, millions of non-combatant targets (individuals who are not taking part in hostilities) are harmed. The main agents are groups such as hackers, rebels groups, and organizations of other nation states. Cyber-terrorism's main objective is the obtention of sensitive information, y mainly accessing to the digital information base data of the organizations. This type of groups recruits members by messaging since they have a huge presence in the Web through diverse media. (FBI, n.d).

Cyber-terrorism is an international problem which involves sensitive sectors, such as the economic, public, medical, military and private ones. According to a 2018 global report form the Center for Strategic

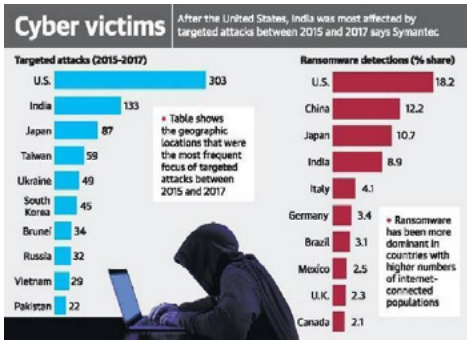


Figura 1

and International Studies (CSIS) every year, cybercrime represents a financial cost of nearly one percent of the global GDP; which means $600 million dollars are lost every year. In 2014, losses were assessed at about $445 billion dollars. The CSIS confirms that this dramatic increase it attributed to the development of illegal digital currencies and online black markets.

The term “cyber-terrorism” was first used by Barry C. Collin, member of the Institute of Security and Intelligence in the 1980’s. The term began to get popular in the 2000s when it started to become a real threat to the population after the events of September 1st, 2001, when the term of cyber terror was spread by different media as a threat to the economy, infrastructure and security of the nation (Curran.P, 4 May 2016). According to the “Internet Security Threat Report”, the United States of America is one of the most vulnerable countries to cyber-terrorism with 26.61%, and it is followed by China with 10.95%. ( Bhargava. Y, April 4 2016).

Figure 1 * The graph represents the countries that are considered targets of cyber attacks between the years of 2015 and 2017. Bhargava. Y. (4 April 2018). India third most vulnerable country to cyber threats. The Hindu. Retrieved on 2 of april, 2019 from: https://www.thehindu.com/news/national/india-third-most-vulnerable-country-to-cyber-threats/article23437238.ece

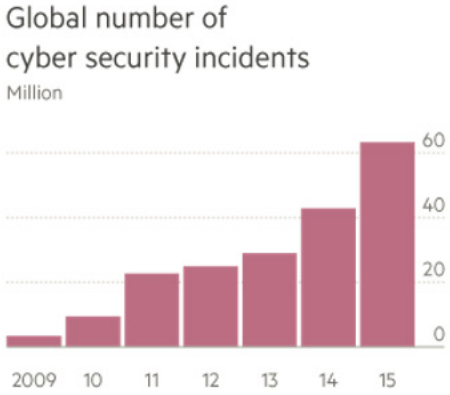


Figure 2

The attacks of cybersecurity have grown within the past years. According to Financial Times, in 2010, there were 10 million of cyber attacks, in 2012, 25 million cases, and in 2015 65 million cyber-attacks were made. (Breene.K, 4 May 2016).

Figure 2* This image expresses the number of cybersecurity incidents globally from 2009 to 2015. K. Breene (May 4th, 2019) Who are the cyber war super power? World Economic Forum. Retrieved on April 4th, 2019, from: https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/

Cyber-security is the term that refers to the action of invasion to all personal data from an unauthorized account. The risk of giving access to an unwanted user to a person’s online information depends on the actions they take, the security measures, risk management, and

practices made to avoid it. (Walker.D, 2019).

The countries that are working to avoid cyber-terrorism are:

* United States: The most prone country to cyber attacks in the world. The country was forced to strengthen and has 58% of the cybersecurity in the world. The participation of organizations such as the FBI and the creation of official documents such as the Presidential Policy Directive 21 have helped fight this issue. (Porter. C, 2018)

* Russia: Often accused from espionage and cyber-attacks. Russia is also fighting cyber terrorism with the automated systems in government organizations. (Aire, 2018).

* Israel: Is the second country with the largest number of cyber security deals in the world, this is because they spend monetary resources on organizations that fight cyber attacks. (Leitersdorf.Y and Schreiber.O, n.d).

* United Kingdom: It is also spending a big amount of economic resources to cyber security and is working to fight cyber terrorism by the creation of organizations such as GCHQ and the National Cyber Security Center. (Dearden.L, 2017)

* China: Adopted a new Security Law, with the purpose of cyber security and the security of the country.

* France: Created a Cyber Security strategy by making partnerships with United Kingdom, China, Russia and the United States.

* Sweden: Country with the lowest malfunctions in their government software in the world. Sweden is preparing to fight cyber terrorism by training “cyber soldiers” trained to detect cyber-attacks and fight them. (The Local, 2019).

(Cyber DB, n.d)

These attacks are made to those countries due to their importance in the economy and social issues in the world, as well as the importance of the data the nations hold in their power and the social conflicts these nations have with others.

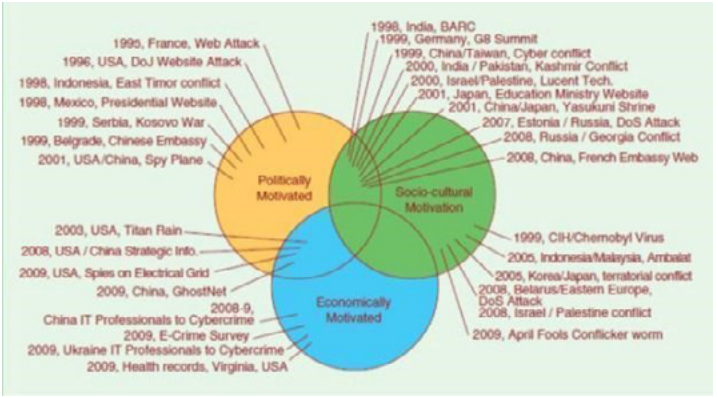


Figure 3

HISTORICAL BACKGROUND

Hacktivism represents for all nations states a matter of concern when it comes to cybersecurity. Thus, cyber-attacks are more common in the XX century; nevertheless, it is important to highlight that the act of terrorism has a historical background of over 2000 years, the main difference between those terms is that cyber-terrorism has the objective of not only damaging the physical world, but also the cyber one; causing losses in multiple sectors such as the governmental, medical, and even financial,  mainly through the implementation of viruses and infected codes via public and social media.

Figure 3. * Graph that represents the different cyber-attacks in different countries depended according to social, economic and political motivations of the attack. Littlefield.R (7 June 2017). Cyber Terrorism: understanding and preventing acts of terror within our cyberspace. Medium. Retrieved on April 2019 from: https://littlefield.co/cyber-terrorism-understanding-and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53cfbb

* March 1791: Claude Chappe d'Auteroche presented the first network of communication, the semaphore visual telegraph.

1834: By using the semaphore telegraph, the Blanc brothers who were financiers, paid an employee to produce an error in one of the stations in order to get the codes from the stock market, which were being transmitted through it. This event is recognized as the first cyber-attack in history.

1903: Guglielmo Marconi "The father of modern Radio" presented the wireless telegraph to the public. While his demonstration was hacked by Nevil Maskelyne, a British spy who sent messages in morse code; consequently, revealing failures in the network security.

June 16th, 1911: The Computing- Tabulating- Recording Company, later renamed International Business Machine (IBM), was founded. It was a company of record-keeping by the use of punched cards.

1924: The Tabulating-Recording Machine was renamed International Business Machine (IBM).

1939: Alan Turing created the Bombe, an electro-mechanical machine that helped Nazis to crack the enigma code during WWII.

1940: The first proto-computer hacking, was accomplished by René Carmille. He censored information in France from the punched cards; consequently, saving the life of thousands of Jews.

February 7th, 1958: Was founded in the United States the Defense Advanced Research Projects Agency (DARPA).

June 1982: The Soviet Union planned to steal a software which was meant to control a Trans-Siberian pipeline. To prevent this to happen, the CIA sabotaged the SCADA system provoking the explosion of the pipe.

November 2nd, 1988: The first computer worm (Morris worm) was spread within the internet around the United States. This was not a destructive virus, yet, it did cause the shutdown of about 10% of the internet servers.

1989: The World Wide Web (WWW) was created and launched as a tool for information-sharing between universities and scientists all around the globe.

April 30th, 1993: Was put into the public domain the World Wide Web (WWW), which allowed the web to bloom.

September 11th, 2001: Al Qaeda used internet for cyber mining within the flight schedule of Pennsylvania, New York. Consequently, causing simultaneous hijacked of four passenger airplanes.

2002:  The non-centralized cyber group “Anonymous” entered to the virtual field, being freedom on the internet their main objective.

2006: Investment in Cyber Warfare started with a group called the Russian Business Network (RBN). They used a “Storm worm” to shoplift identities and send millions of infected emails.

October 16th, 2006: International Business Machine (IBM) acquired Internet Security Systems, the developer of antivirus software for the protection of confidential data which is currently operating in 170 countries.


Figure 4

April 27th - May 2007: Estonian government, banks, and even outlets platforms were hit and taken down by major cyber-attacks, leaving the country with almost no communication.

August 27th, 2008: A worm was found on laptops from the International Space Station; confirmed the NASA.

December 25th, 2008: Pakistan Hackers attacked The State Bank of Indian forcing the bank to shut down their platform.

2010: The virus Stuxnet was first used by the United States and Israeli intelligence in order to stop Iran's nuclear programs.

CURRENT RELEVANCE

This topic is one that affects everyone due to the fact that cyber-terrorism is present in the internet. In the world that we live today people rely a lot in technology as well as countries, especially governments. Cyber attacks have increased drastically and also the amount of people that have access to the web. If cyber-attacks increase even more, they can seriously threat international peace.

October, 2012: Kaspersky, a Russian firm, discovered a cyber-attack named the "Red October", which was active worldwide and had been functioning since 2007.

Figure 4.* This graph represents the percentages of the motivation behind cyber-attacks in 2012. Meharchand.D (18 May 2015). 2012 Cyber Attacks Statistics. Hackmageddon. Retrieved on 5 of April 2019 from: https://www.hackmageddon.com/2012-cyber-attacks-statistics-master-index/

March 2013: In South Korea, their financial and broadcast networks were infected, it is thought that it was caused by the North Korean government.

June 2013: First NATO meeting discussed the topic of cyber-terrorism. An alliance on cyber defense was made, which would protect the networks and be owned by the members of the alliance. (NATO, n.d)

July 2014: The energy sectors of the U.S, Spain, France, Poland, Italy, Turkey and Germany were hacked by Eastern Europe hackers in a cyber espionage campaign.

September 2014: Cyber criminals gained access to 300 governmental websites of Germany, Switzerland and Poland through the falsification of certificates.

October 2014: The Department of State of the United States of America reported a violation to an unclassified email system. Later, the White House reported cyber activity on its computer network.

February 2015: A US health company named Anthem was hacked, with the consequences of the exposure of 80 million customer's personal information.

April 2015: Hackers related to ISIS hacked the public television network from France. They took 11 channels and changed their social media publicity to ISIS related publicity.

September 2015: Cyber Security discovers a Russian group called "The Dukes", which are suspects of attacking other governments and think tanks in Asia, Europe, and United States.

March 2016: North Korea hacked the mobiles of South Korean police, gaining access to conversations, messages and other classified information.

May 2016: Saudi Arabian communication networks and organizations of defense were hacked possibly by Iran.

May 2016: Russian Hackers tried to enter to the Prime Minister office of Turkey and to the German Christian Democratic Party. The attack was made by email.

August 2016: A group called the "Shadow Brokers" claimed they had hacked NSA, as well as published a set of NSA tools in Pastebin.

October 2016: The Director of the national Intelligence and Department of Homeland Security of the USA, identified Russian hackers as the responsible of hacking the Democratic National Committee through WikiLeaks.

February 2017: Hackers entered to the military web of Singapore, stealing personal data of 850 people.

April 2017: Cyber security researchers revealed the discovery of a cyber espionage campaign in China, which had as a target the engineering, aerospace and telecom companies, as well as other governments such

as the one of US, Japan and other countries in Europe.

April 2017: The “Shadow Brokers” launched other supposed NSA hacking tools, one of them being the access to SWIT messages.

June 2017: It was discovered that a hacker group related with Russia launched a campaign against Montenegro after the nation became a member of NATO.

August 2017: The Cyber Warfare Research Center of South Korea reported that the North Korean government has been targeting against the bitcoin exchanges in South Korea.

October 2017: It was discovered that North Korean hackers targeted US electric companies, this with the purpose of probing utilities defenses.

January 2018: The Unique Identification Authority of India is hacked by unknown users, causing that the information of 1 billion people to be revealed and available to buy it.

April 2018: The North Korean hacking group which made the SWIT attacks has discovered targeting Central American online casinos.

June 2018: The US Treasury Department announced that they were going to punish five Russian hacking groups for using technology and military units to make cyberattacks in the US.

September 2018: It is discovered that 36 countries had sent a Pegasus spyware against 45 countries, including US, UK, Canada and France, between others.

November 2018: It was found that North Korean hackers had been using a malware to steal monetary resources from ATMs in Asia and Africa.

December 2018: It was discovered that Russian hacker groups had been attacking government agencies in Ukraine, as well as other countries members of NATO.

January 2019: Russian intelligence service hackers are targeted the Center for Strategic and International Studies.

(CSIS, n.d)

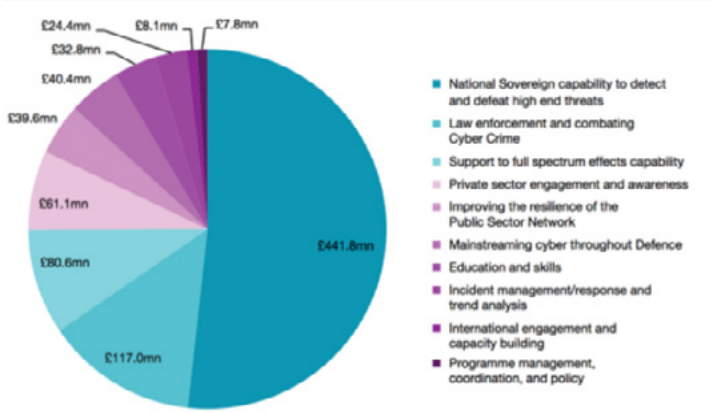


Figure 5

May 15th, 2019: The social platform WhatsApp discovered a spy software within its systems, which main purpose was the espionage of personal data from journalist, activists, lawyers and some other organizations. Authorities and the company reported that such software was developed by the Irani company NSO group technology.

INTERNATIONAL ACTIONS

Rebel groups have used digital platforms to disseminate information, train members, and even to send them instructions for physical and digital attacks, as well as to increase their defensive capacities. These actions have represented a threat to all nations worldwide, since the main movil for this groups is the Darknet. Now more than ever, organized crime is becoming more sophisticated and dangerous. The governmental, private and public networks are asking for new alternatives to ensure the privacy and the security of their platforms, and the only efficient way forward to achieve it is by the creation of exclusive organizations within those areas.

Figure 5. * This graph represents the achievement of the government in the National Cyber Security Strategy. Littlefield.R (7 June 2017). Cyber Terrorism: understanding and preventing acts of terror within our cyberspace. Medium. Retrieved on April 5 2019 from: https://littlefield.co/cyber-terrorism-understanding-and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53cfbb

* The Federal Bureau of Investigation is considered to be the leading agency for the investigations of criminal cyber-attacks. The FBI's International Program seeks to enforce international training in counterterrorism and cyberterrorism; as part of the FBI's initiatives works the International 24/7 network of cyber investigators, which was adopted among the G8 ( USA, France, Russia, United Kingdom, Canada, Japan, Italy and Germany) in 1997. Currently, this net counts with over 50 members, sharing the objective of fast-moving actions in case of a global attack or complot, reducing the time of investigation and losses. (The FBI Federal Bureau of Investigation, 2009)


Figure 6

Figure 6. * Collaborative participation and response though the 24/7 network The FBI Federal Bureau (2009) Combating Cybercrime, Global Network Operates 24/7. FBI, Retrieved on April 4 2019, from: https://archives.fbi.gov/archives/news/stories/2009/january/fordham_011409

In collaboration with the Carnegie Mellon University, The Internet Security Alliance, was founded in 2001, a multi-sector international collaborative agency for the professional collaboration of cyber security, through the creation of guides for fast reactions along with the United States and the European Union.

The ISA has chaired the Cross Sector Cyber Security Working Group, an organization looking forward to identify current threats internationally, for the development of a three-year agenda and its implementation in collaborative member states. The ongoing goals of Cross Sector Cyber Security Working Group are: healthcare cyber risk management and governance, intellectual property data protection, among others. (Critical Infrastructure Security and Resilience Partnership, 2018)

The Asia Pacific Economic Cooperation founded in 1989, headquarter in Singapore, looks forward for the coordination of its 21 member economies, in order to tackle the threats cybercrime represents in each country.  The 21 members are: Singapore, Indonesia, The United States of America, Vietnam, China, Australia, Japan, Russia, Malaysia, Philippines, Thailand, Canada, Hong Kong, Chile, Mexico, New Zealand, South Korea, Peru and Brunei. After the 9/11 outrage in the United States, the APEC leaders considered necessary to reinforce the security, as well as to condemn all cyber-attacks to any member. With this initiative, the creation of the APEC's Endeavour for Cyber Crime Prevention was achieved. It's a branch divided in six organisms:

* The comprising legal development
* Information sharing cooperation
* Security and technical guidelines
* Public awareness
* Training and education
* Wireless security

All these six main targets were established under international legal instruments and the UN General Assembly Resolution 55/63 and Convention on

Cybercrime, which since 2002 have been adopted by countries and security corporations all around the world. (Interpol.int, n.d)

All around the world exist small, yet, effective organizations capable of sharing and train professional within the field of digital security, such as:

* The Information System Security Association is a non-governmental organization for the management of technological risk and protection of essential information. ISSA is present in over 70 countries across the world, with 13,000 cyber security professionals.

* Computer Emergency Response Team Coordination Center founded in 1988 as a center for reactions to face cyber threats. CERT/CC is available all around the world, and multiple times it is been recognize as the main authority for the protection and systems and international networks.

UN ACTIONS

The UN has made a specific agency called International Telecommunications Union (ITU) that specializes in cyber terrorism. This agency is responsible for any issues that concern the information and communication technologies and it coordinates the shared global of radio, spectrum, satellite, orbits, telecommunication infrastructure and worldwide technical standards. The agency is active in areas like internet, wireless technologies, maritime and aeronautical navigation, radio astronomy, satellite meteorology, convergence in cell phones and TV broadcast. (Security Council, 2018)

This agency was formed in 1865 in Paris, France and its current bases are in Geneva, Switzerland. It is member of the United Nations Development Group, has 12 regional offices worldwide. Includes 193 Member States and 800 public and private sector companies, academic institutions and international telecommunication entities (Sector Members and Associates). The agency hosts worldwide exhibitions and forums in order to bring over governments and technological industries. (Security Council, 2018)

The resolution 60/288 by the General Assembly “Counter-Terrorism Implementation Task Force, the Working Group of Countering the Use of the Internet for Terrorist”. Since 2010 the Task Force, approved

by the General Assembly, has initiated a number of conferences with representatives of governments, international organizations, scholars and the private sectors. This conferences are made in order to evaluate the use of internet for terrorist purposes and find means to counter the access to them.  (Security Council, 2018)

On February 17th 2017, the Security Council adopted the Resolution 2341 on the Protection on Critical Infrastructures and Enhancement of States. The resolution's purpose is to have preventing measures by developing strategies and policies. Security Council Resolution 1373 made in 2001 was a call to all states to prevent rebel group's attacks and the early warning to other states by the exchange of information. The Resolution adopted in 2004 (1566) was to prevent any criminal acts against civilians with the purpose of provoking a state terror in the public. (UN, 2019)

Security Council Resolution 2341 in 2017 is directed to the Counter-Terrorism Committee (CTC) and the Counter-Terrorism Committee Executive Directorate (CTED) to protect critical infrastructure from rebel group's attacks; it is an implementations of Resolution 1373. This resolution mandates the Counter-Terrorism Implementation Task Force to work in the technical assistance and capacity building and the awareness in critical infrastructure attacks in particular means. (UN, 2019)

KEY POINTS

* What are some possible solutions?
* How can these threats be prevented?
* Have past efforts to solve this situation functioned?
* What is the role of these threats in current armed conflicts?
* Do these attacks affect the economy of the country attacked? What about other countries economically allied with that country?
* What is the social impact of these attacks?
* Can nations go one step further and with help of brilliant minds that know about technology build systems that are almost impossible to hack? Would most nations agree? Would it work? How long would it take to do this? Would it be viable?
* What is the political impact of these attacks

# REFERENCES


Official sources:

Breene K. (4 May 2016). Who are the cyberwar superpowers? World Economic Forum. Retrieved on 2 of April of 2019 from: https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/

CSIS (n.d) Significant Cyber Incidents. CSIS. Retrieved on April 4 2019 from: https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

Cyber Terrorism. (2018). United Nations Security Council. Retrieved on April 5, 2019 in http://www.cwmun.org/wp-content/uploads/2018/07/BGG-SC-High-School.pdf?x13564

FBI (n.d). Terrorism. Retrieve on March 12, 2019, from: https://www.fbi.gov/investigate/terrorism

Gross (4 August 2016). The psychological effects of cyber terrorism. Retrieved on March 12, 2019, in: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5370589/

Hardy. K (20 February of 2017). Is cyberterrorism is a threat? Australian Institute for International Affairs. Retrieved on 2 of April of 2019 from: https://www.internationalaffairs.org.au/australianoutlook/is-cyberterrorism-a-threat/

Internet Security Alliance (2018) Historic Highlights through the Years. ISA. Retrieved on April 4th, 2019 from: https://isalliance.org/about-isa/history/

Interpol (n.d) Cybercrime. Interpol. Retrieved on April 4, 2019 from: https://www.interpol.int/Crimes/Cybercrime

ISSA (n.d) Developing and connecting Cyber Security Leaders Globally. ISSA. Retrieved on April 2, 2019 from: https://issa-india.org/about/

JM. Dilhac (n.d) The Telegraph of Claude Chappe -An optical Telecommunication Network for The XVIIIth Century. Institut National des Sciences Appliquées de Toulouse. Retrieved on May 27, 2019 from: https://ethw.org/w/images/1/17/Dilhac.pdf

NATO (n.d.) The history of cyber-attacks - a timeline. Retrieved on March 13, 2019, from: https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm

United Nations (2018) The protection of critical infrastructure against terrorist attacks: Compendium of good practices. United Nations Office of Counter Terrorism. Retrieved on April 5, 2019 from: https://www.un.org/sc/ctc/wp-content/uploads/2019/01/Compendium_of_Good_Practices_Compressed.pdf

United Nations (n.d.) What is the Security Council? United Nations Security Council. Retrieved on March 28, 2019 from: https://www.un.org/securitycouncil/content/what-security-council

Links:

A look back at the Israeli cyber security industry in 2018. (n.d). TC. Retrieved on April 20 2019 from: https://techcrunch.com/2019/01/06/a-look-back-at-the-israeli-cyber-security-industry-in/

Bhargava. Y.( 4 April 2018). India third most vulnerable country to cyber threats. The Hindu. Retrieved on 2 of april, 2019 from: https://www.thehindu.com/news/national/india-third-most-vulnerable-country-to-cyber-threats/article23437238.ece

Curran.P (4 May 2016). Cyber Terrorism. How real is the threat?.Checkmarx. Retrieved on 2 of April 2019 from: https://www.checkmarx.com/2016/05/04/cyber-terrorism-real-threat-2/

Cyber DB. (n.d) Top 10 Countries Best Prepared Against Cyber Attacks. Cyber DB. Retrieved on 2 of April of 2019 from: https://www.cyberdb.co/top-10-countries-best-prepared-cyber-attacks/

Dearden.L ( 9 October 2017). Protecting British citizens from cyber attacks must be given same priority as fighting terrorism, GCHQ head warns. Interdependent. Retrieved on April 20 2019 from: https://www.independent.co.uk/news/uk/home-news/uk-cyber-attacks-protection-same-priority-terrorism-isis-british-citizens-gchq-head-jeremy-fleming-a7990311.html

How the Swedish army is preparing to defend against cyber attacks.(8 March 2019). The Local. Retrieved on April 20 2019 from: https://www.thelocal.se/20190308/how-the-swedish-army-is-preparing-to-fight-cyber-crime

Littlefield.R (7 June 2017). Cyber Terrorism: understanding and preventing acts of terror within our cyberspace. Medium. Retrieved on April 5 2019 from: https://littlefield.co/cyber-terrorism-understanding-and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53cfbb

McGuinness, D. (27 April 2017). How a cyber attack transformed Estonia. Retrieved on April 5, 2019 form: https://www.bbc.com/news/39655415

Meharchand.D (18 May 2015). 2012 Cyber Attacks Statistics. Hackmageddon. Retrieved on 5 of April 2019 from: https://www.hackmageddon.com/2012-cyber-attacks-statistics-master-index/

Singer.P (1 November 2012). The Cyber terror bogeyman. Retrieve on March 12, 2019, from: https://www.brookings.edu/articles/the-cyber-terror-bogeyman/

P. Paganini ( June 25, 2012) The "cyber war" era began long ago. Security Affairs. Retrieved on April 2nd, 2019 from: https://securityaffairs.co/wordpress/6776/security/the-cyber-war-era-began-long-ago.html

Porter.C (August 24 2018). In Cyber Warfare, the Front Line Is Everywhere the U.S. Government Isn't. Retrieved on April 20 2019 from: https://www.lawfareblog.com/cyber-warfare-front-line-everywhere-us-government-isnt

Russia claims to be fighting off western cyber attacks. (November 14, 2018). UAWire. Retrieved on 20 of april in 2019 from: https://www.uawire.org/russia-repels-western-cyber-attacks

Walker. D. ( 7 February 2019). What is cyber security?. ITPRO. Retrieved on March 12 2019, from: https://www.itpro.co.uk/security/28133/what-is-cyber-security