Cybersecurity challenges for Human Rights Defenders in Gulf Cooperation Council (GCC) countries

By

Zainab Al Sairafi

Submitted to Central European University

School of Public Policy

In partial fulfillment of the requirements for the degree of Master of Arts in Public Policy

Supervisor: Cameran Ashraf

Vienna, Austria

2022

Author's Declaration

I, the undersigned Zainab Al Sairafi hereby declare that I am the sole author of this thesis. To the best of my knowledge, this thesis contains no material previously published by any other person except where proper acknowledgment has been made. This thesis contains no material which has been accepted as part of the requirements of any other academic degree or non-degree program, in English or any other language.

This is a true copy of the thesis, including final revisions.

Date: June 27,2022

Name: Zainab Al Sairafi

Signature: Zainab Al Sairafi

Abstract

Human rights defenders in the Gulf Cooperation Council (GCC) countries are exposed to privacy violations and surveillance in cyberspace, which prevents them from practicing their human rights work with high professionalism and restricts civil society space in these countries. However, these challenges faced by human rights defenders due to the absence of cybersecurity in Gulf Cooperation Council GCC countries have not been mapped so far. This thesis analyzes the problem of the lack of cybersecurity for human rights defenders in the Gulf Cooperation Council GCC countries to determine the impact of cybersecurity threats on human rights activism. Secondary data collected from research papers and reports issued by human rights organizations will be analyzed, along with primary data collected from four face-to-face semi-structured interviews with human rights defenders from the Gulf Cooperation Council GCC countries who are living in exile for political reasons and two online interviews with an expert in digital rights who works with international human rights organizations. This thesis finds that human rights defenders in the Gulf Cooperation Council GCC countries do not have cybersecurity, as governments have controlled cyberspace by using surveillance technology to prevent them from continuing their human rights work.

Keywords: Cybersecurity, GCC countries, Human Rights defenders, Surveillance technology

Acknowledgment

Words cannot express how profoundly grateful I am for the love and support I have received from my beloved family. My husband Sayed Yusuf Almuhafdha has always been my pillar of support and patience. My three beautiful daughters Fadak, Raghad, and Ghadeer, were my sources of motivation throughout the course due to their immense understanding and the comfort that they provided me to study far away from them.

My Father Abdul Jalil Al Sairafi, and my Mother Ibtisam Al Nasser, your love and prayers were the sources of my strength.

My second Father Abdul Jalil Almuhafdha, who inspired me and encouraged me to study. To your absent spirit that is present in my heart.

Table of Content

1 Introduction

Many current studies and research projects are looking at cyber security since users and activists on the Internet cannot utilize their smart gadgets without the danger of being hacked and tracked. The global growth in Internet users has raised the extent of the issue and the complexity of attaining cyberspace security. Internet attackers have a plethora of methods and processes for penetration; even when protection and security programs and systems are in place, the security environment may be penetrated and thwarted.

This study focuses on the cybersecurity problems faced by human rights defenders in Gulf Cooperation Council countries. My study purpose is to discuss the absence of cybersecurity in GCC countries in order to identify the influence of cyber security on human rights work, looking to the threats to human rights defenders' privacy, freedom of speech, and free flow of information in the GCC countries.

To achieve the goal of the research, face-to-face semi-structured interviews were held with four exiled human rights defenders, who faced obstacles in their human rights work within their countries back home, due to the penetrations they were exposed to in cyberspace, which threatened the quality of their human rights work and have risked the lives of victims who communicated with them and reported about a violation they were subjected to. Furthermore, two face-to-face semi-structured online interviews with an expert in digital rights who works in international human rights organizations.

1.1 Objectives of the Research

The purpose of this research is to analyze the lack of cybersecurity for human rights defenders in the GCC countries to determine the impact of cybersecurity on human rights activism. Freedom of expression, when governments buy surveillance and hacking software, secretly install it on human rights activists' devices, then prosecute them on charges of cybercrime, insulting the government, and defaming the country.

This study aims to demonstrate the challenges of the absence of cybersecurity in the Gulf Cooperation Council countries, and the consequences thereof, and calls upon the United Nations Human Rights Council of the United Nations Mechanism, which is responsible for the promotion and protection of all human rights around the world, to enact laws related to the protection of space. The research aims to define the problem of cybersecurity in the Gulf countries that affect Human Rights Defenders and call upon the Human Rights Commission of the European Union to make sure that technologies sold from Europe to authorial governments will not violate local European convention and standards, such as Human Rights defenders guidelines and Trade guidelines. The research discusses the prevention of the export of surveillance and spyware programs from Europe to the GCC countries to monitor the activities of human rights activists, risking their lives, exposing them to ill-treatment, torture, detention, deprivation of travel, and many forms of human rights violations.

1.2 Research problem

The research examines the problem of the absence of cyber security for human rights defenders in the countries of the Gulf Cooperation Council. Where human rights defenders in the Gulf Cooperation Council countries are exposed to the violation of their privacy in cyberspace, and monitoring of their local and international human rights activists. When repressive governments use malicious spyware technology and software that infiltrates their smart devices and copies files and private data and monitors the electronic activity of the human rights activist and his work in communicating with local and international organizations to document violations committed by the state against human rights.

The problem of the absence of cybersecurity due to espionage and surveillance by repressive governments of activists affected the quality of human rights work and caused security prosecutions by the authorities against activists and the people who communicate with them. Thus, activists are prevented from continuing their human rights work and communicating with local and international human rights organizations, as they are being pursued by the security, arrested, and imprisoned under the electronic crime law. This research discusses this problem by analyzing the cybersecurity challenges faced by human rights defenders in the Gulf Cooperation Council countries, first by examining the extent to which human rights defenders enjoy the freedom of opinion and expression in accordance with international conventions and treaties signed by the countries of the Gulf Cooperation Council. and second, the technology and surveillance technologies that governments purchase to combat terrorism and crime but use to censor and spy on activists and human rights defenders. And third, how these technologies work in the devices of human rights defenders, and how their smart devices are hacked, and personal files and data are infiltrated.

1.3 Research questions

The main research question in this study is: What are the cybersecurity challenges for human rights defenders in the Gulf Cooperation Council countries?

The main question in this study aims to verify the cybersecurity challenges of human rights defenders and the impact of the absence of cybersecurity on human rights work in the Gulf Cooperation Council countries. Other sub-questions fall under this main question:

1- Do human rights defenders have freedom of opinion and expression following international conventions and treaties signed by the countries of the Gulf Cooperation Council?

2- What is the surveillance and espionage technology used in the Gulf Cooperation Council countries?

3- How do surveillance and espionage technology work in devices of human rights defenders?

1.4 Research instrument

The research instrument used is analyzing information from academic research papers related to the definition of cybersecurity, freedom of expression and surveillance, and electronic surveillance techniques in the Gulf Cooperation Council countries, in addition to analyzing information and data in reports issued by human rights organizations on cybersecurity, and the exposure of human rights activists to surveillance and espionage in GCC countries. Consequently, this secondary information was combined with the primary information resulting from a set of interviews with human rights activists from the Gulf Cooperation Council countries. They were hacked into cyberspace by spyware and surveillance programs that their governments used to monitor their human rights work and prevented them from continuing this work. Which made them migrate to Europe and the United Kingdom.

1.5 Data collection

This research used interviews to answer the research questions because it is the most effective and appropriate method for this research. The interviews with human rights defenders from the Gulf Cooperation Council countries helped to explain, understand, and explore the opinions and lived experiences of cybersecurity. Local Human Rights Defenders thus have a greater and deeper understanding of the problem. The testimonials were valuable to my research because they reflected real experience, a personal experience from the victim personally allowing me to understand all the technical details and issues and what impact this has on a personal level.

Two parts of the interviews were conducted, the first part was a semi-structured face-to-face interview with 4 activists and human rights defenders from the Gulf Cooperation Council (GCC) countries who were exposed to intrusions in cyberspace by means of malicious software used by their governments, to penetrate their smart devices to spy and monitor their activities and human rights work. All activists shared their personal experiences and how they were exposed to the hack in cyberspace and how this affected their human rights work. The second part is a semi-structured online face-to-face interview with digital rights professionals working in international human rights organizations, in projects specialized in studying and analyzing the work of surveillance technology and continue to check the devices of human rights defenders to verify the presence of any malware. During the interview, they focused on the technical aspect of software work and how to penetrate smart devices. And the necessary precautions for human rights defenders to take to reduce the risks of penetration in cyberspace.

The semi-structured interviews consisted of 16 questions, starting with a question about the background of human rights activists, the activist’s concept and definition of cybersecurity, and the challenges and difficulties they face in the cyberspace that affected his human rights activity and work and knowing how they were hacked before Spyware and surveillance programs, how they can detect these intrusions, the protection programs they use to prevent future breaches, and how the absence of cybersecurity affects human rights work. While the interview with the digital rights specialist consisted of a set of 12 questions, starting with the question about the background of the activism in the digital right, how they define cybersecurity in GCC countries, how could spyware hack activists' devices, how they discover the Spyware on activists' devices, how can an activist know that their device was hacked, the role of the international organization that they worked with in discovering the surveillance technology, what are the techniques programs used to protect activists' devices and their vision and recommendations to solve this problem, and if there is a need for international conversion from the human rights council about cybersecurity.

In these interviews, a lot of in-depth information was collected. Where the interviewee had enough space to add depth and relevant information. The interviews are designed to gather a richer source of information from a small number of people who have enough experience to convey their experiences and opinions about the impact of cybersecurity on the quality of human rights work in the GCC countries. The duration of the interviews ranged from 30 minutes to 60 minutes. All interviewees are displaced activists from the Gulf Cooperation Council countries who have been subjected to security violations in cyberspace, forcing them to migrate from their homeland to the United Kingdom, the United States, and Europe and seek political asylum. Governments in the Gulf Cooperation Council (GCC) countries have brought various and varied charges related to cybercrime to these activists, which caused them to be imprisoned and prevented from practicing their human rights work.

The interviews are with human rights defenders from the Gulf Cooperation Council countries living in exile, who have had their smart devices hacked by malicious techniques used by governments in the Gulf Cooperation Council countries to control cyberspace. Thus, the researchers obtained information from direct and live experiences. It was not possible to interview human rights defenders living in their home country because their smart devices still contained spyware and surveillance, which would expose them to accountability, and put me at risk of electronic surveillance. As for the other interviews, they were with digital rights specialists who worked in international human rights organizations as part of projects designed to examine the devices of activists and human rights defenders in the Gulf

Cooperation Council countries, to detect malicious spyware and know how it is work and how to protect against it. In addition to their work in raising technical awareness among human rights activists and conducting courses and workshops to educate activists on the importance of updating operating systems and periodic examination of smart devices, and how to protect against spyware and surveillance programs used by governments.

2 Literature Review

This chapter will present the literature review. Firstly, introduction about cybersecurity. Secondly, define cybersecurity from different resources, which will show the various definitions of cybersecurity. Thirdly will discuss the Freedom of Expression and Internet Censorship in the GCC countries by illustrating the international and national constitutions, and the three most common methods adopted for implementing censorship on websites in the GCC countries. Fourthly, discuss the cyber-surveillance technologies in the GCC countries and export spyware to repressive countries. The regulation that governs the trade in surveillance technologies from Europe. lastly trade of spyware and surveillance software produced by the Israeli company NSO Group.

2.1 Cybersecurity

The most critical issue in cybersecurity is the danger of being hacked, which would result in the data being given to a third party, destroyed, and a violation of the individual's right to personal privacy. The present state of cybersecurity, in which users cannot use computers or smartphones without danger, is the subject of many ongoing studies and research initiatives, in addition to the expenditure of millions of dollars to defend cybersecurity on a worldwide scale. [1] Even the most sensitive and secure systems are often victimized by cyber thefts of

[1] Garfinkel, Simson L. "The cybersecurity risk." *Communications of the ACM* 55, no. 6 (2012): 29-32.

data and penetration attempts. Both the rising worldwide interconnection and the huge development in the number of electronic hacking tools are contributing factors to the increasing complexity and difficulty of cybersecurity. [2] This is the case despite the rapid development of new ways of protection and safe encryption software, attackers on the Internet have many tools and mechanisms to penetrate, where they can hack through applications that process data or by working on the operating devices on which the applications run, as well as through networks or other loopholes that enable them to penetrate, even in the case of providing protection and security programs and systems, the hacker can circumvent the security environment by various means such as social engineering and supply chain to achieve their goals. In addition, attackers on the Internet have many tools and mechanisms to penetrate, where they can hack through applications that process data Because contemporary civilizations are becoming more reliant on the many types of modern technology available to them, the problem of ensuring the safety of their cyberspace is becoming an issue of ever-increasing importance. [3]

2.2 Defining Cybersecurity

Cybersecurity is a term that has a wide range of applications and various definitions, but there is no fixed definition of cybersecurity, which hinders technological and scientific progress. One of the comprehensive definitions of cybersecurity was the result of a group of discussions with a group of academics and graduate students about cyber security for scientific research that they conducted by Craigen, Diakun-Thibault, and Purse "Cybersecurity is the organization and collection of resources, processes, and structures used

[2] Garfinkel, Simson L. "The cybersecurity risk." *Communications of the ACM* 55, no. 6 (2012): 29-32.
[3] Garfinkel, Simson L. "The cybersecurity risk." *Communications of the ACM* 55, no. 6 (2012): 29-32.

to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights."[4]

To define cybersecurity more accurately and comprehensively and to a comprehensive analysis of cybersecurity, the research will list a set of different definitions of cybersecurity. According to Edward Amoroso "Cyber Security involves reducing the risk of a malicious attack to software, computers, and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on." [5] While Oxford University Press defines cybersecurity as "The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this."[6] As for the comprehensive concept of cybersecurity, according to International Telecommunication Union "It is a set of tools, policies, security concepts, security safeguards, guidelines, risk management methods, procedures, training, best practices, assurance and techniques that can be used to protect the cyber environment, organization, and user assets." [7] Additionally, Public Safety Canada describes cyber security as "The set of technologies, processes, practices, response and mitigation measures designed to protect networks, computers, software, and data from attack, damage, or unauthorized access to ensure confidentiality, integrity, and availability." [8] Cybersecurity in a Glossary of Common Cybersecurity Terminology defines as "The activity or process, ability or capability, or state

[4] Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. "Defining cybersecurity." *Technology Innovation Management Review* 4, no. 10 (2014).

[5] Amoroso, Edward. *Cyber security*. Silicon Press, 2006.

[6] Oxford University Press. 2014. Oxford Online Dictionary. Oxford: Oxford University Press. October 1, 2014.

[7] ITU (International Telecommunication Union). Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). (2009).

[8] Public Safety Canada. *Terminology Bulletin 281: Emergency Management Vocabulary.* Ottawa: Translation Bureau, Government of Canada. (2014).

whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." [9]

The various definitions disclose that cybersecurity depends on obtaining security in the cyberspace, and regardless of the different definitions of cybersecurity by researchers, universities, and study institutes, agreed that cybersecurity is the protection of computers, electronic devices, and networks from any attacks or external practices that infringe privacy legal.

2.3 Freedom of Expression and Internet Censorship in Gulf Cooperation Council (GCC) countries

The Gulf Cooperation Council countries are members of the United Nations, which requires them to respect the Universal Declaration of Human Rights. [10] Article 19 of the Declaration of Human Rights states that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinion without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." This article is currently regarded as an important source in international law, and the right to free speech has been established in international law as a result of the approval of this article by the General Assembly of the United Nations. [11] The right to free expression is also protected in the International Covenant on Civil and Political Rights, which states that "everyone shall have

[9] DHS. 2014. A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. October 1, 2014.

[10] Hakmeh, Joyce. "Cybercrime Legislation in the GCC Countries." International Security Department, Chatham House (The Royal Institute of International Affairs) (2018).

[11] The United Nations (1966) International Covenant on Civil and Political Rights (ICCPR), adopted December 16,1966, G. A Res.2200A(XXI). Universal Declaration of Human Rights, Res. no 217, adopted by the G>A. December 1948.

the right to freedom of expression, this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or print, in the form of art or through media of his choice." [12] Restricting freedom of opinion and expression affects other basic human rights, as preventing the dissemination and expression of ideas, the flow of information and community participation, and encouragement of discussion deprives the community of the right to participate in decision-making. [13]

In giving freedom of expression in the national constitution in Gulf cooperation council countries, this research will look at the national constitution articles regarding freedom of expression in GCC countries except for the Kingdom of Saudi Arabia, which does not have a written constitution.

In Bahrain, Article 23 states that "Freedom of speech and freedom to carry out scientific research shall be guaranteed. Every person shall have the right to express and propagate his opinion in words or writing or by any other means, in accordance with the conditions and procedures specified by the law" [14] In Kuwait, Article 36 states "Freedom of opinion and scientific research is guaranteed. "Every person has the right to express and propagate his opinion verbally, in writing, or otherwise, in accordance with the conditions and procedures specified by law." [15] In Oman Article 29 states "The freedom of opinion and expression thereof through speech, writing and other means of expression are guaranteed within the

[12] Ali, Salaheldin M. Ibrahim. "Media Regulations in Gulf Cooperation Council Countries: A Global Perspective." *International Journal of Media and Mass Communication (IJMMC)* 1, no. 1 (2019): 144-157.

[13] Ali, Salaheldin M. Ibrahim. "Media Regulations in Gulf Cooperation Council Countries: A Global Perspective." *International Journal of Media and Mass Communication (IJMMC)* 1, no. 1 (2019): 144-157.

[14] Hakmeh, Joyce. "Cybercrime Legislation in the GCC Countries." International Security Department, Chatham House (The Royal Institute of International Affairs) (2018).

[15] Hakmeh, Joyce. "Cybercrime Legislation in the GCC Countries." International Security Department, Chatham House (The Royal Institute of International Affairs) (2018).

limits of the Law." [16] In Qatar Article 47 states "Freedom of expression of opinion and scientific research is guaranteed in accordance with the conditions and circumstances outlined in the law." [17] In UAE Article 30 states "Freedom of opinion and expressing it verbally or in writing or by other means shall be guaranteed within the limits of the law." [18]

However, the authorities in the Gulf Cooperation Council (GCC) countries have imposed censorship on the Internet through their secure computing system. Internet censorship is one of the most common methods used by governments to control the media, and this behavior has been justified by governments under the National Security Protection Act and terrorism laws. Human rights activists, journalists, and political activists have been the government's main target. These groups have been denied the right to freedom of opinion and expression on the Internet and have been targets of government censorship of the Internet. [19]

Shishkina and Issaev illustrate that the philosophy of the Internet is to make it a place free from any outside interference, whether governmental or otherwise, but in the countries of the Gulf Cooperation Council, freedom of opinion and expression and the right to access information on the Internet is a complex matter. [20] Rather, it is a big problem and challenge among the most significant changes that societies in the GCC countries experienced during the Arab Spring, were the increase in online activity, and the impact of virtual environments

[16] Hakmeh, Joyce. "Cybercrime Legislation in the GCC Countries." International Security Department, Chatham House (The Royal Institute of International Affairs) (2018).

[17] Hakmeh, Joyce. "Cybercrime Legislation in the GCC Countries." International Security Department, Chatham House (The Royal Institute of International Affairs) (2018).

[18] Hakmeh, Joyce. "Cybercrime Legislation in the GCC Countries." International Security Department, Chatham House (The Royal Institute of International Affairs) (2018).

[19] Shishkina, Alisa, and Leonid Issaev. "Internet censorship in Arab countries: Religious and moral aspects." *Religions* 9, no. 11 (2018): 358.

[20] Shishkina, Alisa, and Leonid Issaev. "Internet censorship in Arab countries: Religious and moral aspects." *Religions* 9, no. 11 (2018): 358.

on citizens' social attitudes. [21] This increase has generated concerns within the GCC countries about issues of national, economic, and political security, and the preservation of societal and cultural values, thus imposing restrictions on practices in online virtual spaces. [22] Digital social networks played a major organizational role during the Arab Spring revolutions, as human rights activists exploited the digital network and the flow of information, communicating without monopoly or direct control of the state, to organize protests and call for people to demand them. Fundamental rights. [23]

The three most common methods adopted for implementing censorship on websites in the GCC countries is the, firstly **“packet filtering”** methodology, where the government send TCP packets that contain words and terms that are considered controversial, or politically tense. These terms are subject to government control. Secondly, topics are often related to religion, politics, or human rights. Saudi Arabia and the United Arab Emirates use the **"religious filtering"** methodology, which is used to filter religious content that does not comply with the official religious beliefs of the state. The government of the United Arab Emirates also adopted the urban method and restrictions on any content that contradicts the policy, belief, or culture of the state. Thirdly, the governments of Qatar and Saudi Arabia have also banned the use of online applications like Telegram, FaceTime, and Snapchat in their countries. The third method of control is the **"packet filtering technique"**, which has been applied in the United Arab Emirates, Saudi Arabia, Qatar, and the Sultanate of Oman. It

[21] Shishkina, Alisa, and Leonid Issaev. "Internet censorship in Arab countries: Religious and moral aspects." *Religions* 9, no. 11 (2018): 358.

[22] Shishkina, Alisa, and Leonid Issaev. "Internet censorship in Arab countries: Religious and moral aspects." *Religions* 9, no. 11 (2018): 358.

[23] Shishkina, Alisa, and Leonid Issaev. "Internet censorship in Arab countries: Religious and moral aspects." *Religions* 9, no. 11 (2018): 358.

is a technique that relies upon. Which rely on algorithms that match and block keywords such as blocking pornographic apps. [24]

2.4 Cyber surveillance technologies in Gulf Cooperation Council (GCC) countries

It is abundantly clear that there are loopholes in the laws that have been issued by the European Union on the export of surveillance and spying software and technologies to authoritarian governments. [25] Wenzel Michalski, head of Human Rights Watch's Germany office, stated that "weak EU standards have allowed companies to export spyware to repressive countries, which has helped them quell dissent." [26] The European Union (EU) must fix the flaws in its trade policy and stop becoming a party to human rights abuses. Human Rights Watch and seven other rights groups wrote a letter to the European Union stating that the European Union should pass stricter restrictions on the matter to put an end to the practice of exporting to authoritarian governments electronic surveillance technology that was developed in Europe. [27] Numerous hacks in cyberspace that violated human rights and standards for the right to privacy were uncovered using a variety of software and hardware. These surveillance technologies were found to be against illegal norms, as these programs can hacked smart devices, just like the Fin Spy program that was manufactured by the German company Fin Fisher, it can record calls, collect contacts, copy text messages, emails, geolocation, and other data, in addition to downloading all the image and video files that are stored in the mobile phone. In addition to the Remote-Control System (RCS), which is what

[24] Rahimi, Nick, and Bidyut Gupta. "A Study of the Landscape of Internet Censorship and Anti-Censorship in Middle East." In *CATA*, pp. 60-68. 2020.

[25] Human Rights Watch.EU: Strengthen Rules on Surveillance Tech Exports. New York. USA. Human Rights Watch. (2020).

[26] Human Rights Watch.EU: Strengthen Rules on Surveillance Tech Exports. New York. USA. Human Rights Watch. (2020).

[27] Human Rights Watch.EU: Strengthen Rules on Surveillance Tech Exports. New York. USA. Human Rights Watch. (2020).

the Italian business Hacking Team supplies to government agencies, they also sell a suite of spyware for remote monitoring. In addition, there are a variety of programs and tools that can hack into computers and mobile devices like smartphones for espionage, surveillance, and information collection. These tools are manufactured, offered for sale, and created. [28]

Citizen Lab, a Toronto-based research organization, has found that government agencies in more than 30 countries in the world use a Fin Spy, and among these countries are the Gulf Cooperation Council countries such as Bahrain, Oman, and Qatar. It is also known that 21 countries, including Saudi Arabia and the United Arab Emirates, use the remote-control system affiliated with Hacking Team. Governments in the Gulf Cooperation Council countries record calls and monitor e-mails of all individuals who have political opinions contrary to the state system. The UAE's use of Fin Spy and RCS was confirmed during their investigation of prominent Emirati activist Ahmed Mansoor. This surveillance information was used to convict him on cybercrime charges in 2018 and he was sentenced to ten years in prison. [29]

In 2016, the European Commission proposed several significant amendments to the regulation that governs the trade in surveillance technologies. The European Parliament has broadly approved these changes. But in June 2019, the European Council systematically dismantled it. Countries including the Czech Republic, Cyprus, Estonia, Finland, Ireland, Italy, Poland, and Sweden have rejected these e-commerce reforms, citing economic fears. While the European Commission has tried to work on drafting amendments in preparation for

[28] Human Rights Watch.EU: Strengthen Rules on Surveillance Tech Exports. New York. USA. Human Rights Watch. (2020).

[29] Human Rights Watch.EU: Strengthen Rules on Surveillance Tech Exports. New York. USA. Human Rights Watch. (2020).

the work of resuming negotiations, these amendments are still not sufficient to restrict electronic monitoring policies. [30]

Human rights activists have been the target of government surveillance in many nations that are members of the Gulf Cooperation Council (GCC). A few legal loopholes have, for several years now, making it possible for oppressive regimes to purchase items created in the European Union (EU) that are designated as having dual-use. These items contain a wide variety of invasive and all-encompassing surveillance technologies in their many forms. In their attempts to crush human rights activists, journalists, and opposition groups, these governments have turned to the use of technology. The organizations have urged the European Union to pass legislation requiring companies to implement human rights due diligence and requiring states to deny export licenses for electronic surveillance technology if there is a significant risk that it could be used to violate human rights. Additionally, the organizations have urged the European Union to pass legislation requiring states to deny export licenses for electronic surveillance technology. Following the provisions outlined in the Act. [31]

There are also concerns from human rights organizations about whether EU countries are facilitating the trade of spyware and surveillance software produced by the Israeli company NSO Group, which sells ls these technologies to the Gulf Cooperation Council countries for huge sums of money, such as the Pegasus spy and surveillance software. The Pegasus mobile spy and surveillance software, produced by the Israeli company NSO, has been largely used in the Gulf Cooperation Council countries, with the encouragement and support of the Israeli

[30] Human Rights Watch.EU: Strengthen Rules on Surveillance Tech Exports. New York. USA. Human Rights Watch. (2020).

[31] Human Rights Watch.EU: Strengthen Rules on Surveillance Tech Exports. New York. USA. Human Rights Watch. (2020).

government, under the pretext of fighting crime and terrorism. The Pegasus program has been sold for more than $100 million in the United Arab Emirates, Saudi Arabia, and other Gulf states that actively pursue regime opponents and human rights activists. These huge sums paid by the governments of the Gulf Cooperation Council countries to purchase such programs encouraged the continuation of the production and development of spyware. The Pegasus 3 app, developed by the same company, can break into cell phones, replicate their information, and use it remotely for imaging and recording purposes. This is done by searching for security holes in smartphones and computers and vulnerabilities in the rapidly developing mobile phone industry and then breaking into them without the need for help from phone or computer makers. Spyware reaches the phone within a few hours after the phone number is entered by the intelligence agencies. The spyware can also be controlled remotely by the same company that produced the NSO spyware, where the company's employees can check the data collected or stop the program from working on the compromised device. [32]

NSO works with government agencies only, it does not work with people or organizations, and it sells the spyware and surveillance programs that it produces legally to the governments of countries, and it does not differentiate between democratic governments or authoritarian governments. The Kingdom of Saudi Arabia, Bahrain, Oman, and the United Arab Emirates were among the major countries that signed contracts with the company. Despite that, there is a ban on signing contracts with the State of Qatar due to political differences with the State of Israel. Among the activists who were infiltrated in the cyberspace by NSO's Pegasus program is the Saudi journalist and journalist Jamal Khashoggi, who was subjected to spyware and surveillance because of his critical opinion of the Saudi government, and this spying ended with killing, which caused great opposition by many employees of the company NSO, for the

[32] Dahir, Bilal. Israel encourages and mediates sale of NSO spy software to Gulf states. Arab Website 48.2020

unethical use of Pegasus software, and several of them resigned and left the company due to the unethical exploitation of this technology. Regardless of this, the company did not stop the spyware program in the Gulf Cooperation Council countries but stated that these programs are significant in the battle against crime and terrorism. [33]

6 Finding and Discussion

This chapter will provide the finding reached in this research to answer the research questions and analyze material gathered through a series of interviews with human rights defenders and digital rights professionals from the GCC, who have moved to the UK and Europe due to political and security concerns. The first four interviews with human rights defenders focus on gathering information about the cybersecurity challenges they have faced while carrying out their human rights work, how they have been hacked in cyberspace, and the precautions they take to reduce the risks of lack of cybersecurity. The last two interviews with digital rights specialists focused on the techniques and malware that governments in the Gulf Cooperation Council (GCC) use for hacking and surveillance. And the role of protection programs in cybersecurity, in addition to their vision and suggestions to solve the problem and maintain the continuity of human rights work.

1- The human rights defenders in the Gulf Cooperation Council countries do not have cybersecurity, where governments have controlled cyberspace, and smart devices have hacked with spyware and surveillance programs purchased from Europe and Israel. These programs worked to infiltrate the devices and thus reveal all the information and data contained in these devices, which led to charges of cybercrime against activists. This has prevented activists from exercising their human rights work and made it difficult to preserve and exchange information with local or international human rights organizations.

[33] Dahir, Bilal. Israel encourages and mediates sale of NSO spy software to Gulf states. Arab Website 48.2020

2 - Human rights defenders do not enjoy the freedom of opinion and expression, although the countries of the Gulf Cooperation Council are members, of the European Union, they do not respect the Universal Declaration of Human Rights and international treaties that provide for the right to freedom of opinion and expression, whether orally, in writing, in print, or any form. One form of dissemination of information, i. criticism of government policy or exposing a human rights violation, exposes human rights defenders to scrutiny and legal accountability.

3 - The GCC countries used various techniques and programs to spy on activists and human rights defenders, which they purchased from European and Israeli companies. The Gulf Cooperation Council, which made it continue to develop and modernize it to achieve a higher level of espionage and surveillance.

4 - Surveillance and spying technology works in the devices of human rights defenders in various forms, but most of them are done by exploiting the gaps in the smart device, and they are often gapping in the operating system. Hacking and monitoring programs can also track the online activity of the activist on the websites, the emails that are received and sent, and the geographical location. The spyware is installed by installing other seemingly legitimate programs. Or through links sent via message boxes or chat programs. Spyware may be installed in the device without any action.

The first interview was with Y.J, a blogger and activist from the Kingdom of Bahrain to talk about his extensive social media activities and experiences. After the Bahraini government began harassing activists, often using programs and technologies to digitally hack activist computers and monitor their work and activities, they were forced to flee Bahrain and seek political asylum in the British capital, London. They had trouble practicing their human rights activity inside the Kingdom of Bahrain due to a threat of espionage and penetration in cyberspace. They pointed out that these hacks were designed to violate the privacy of activists, access the information saved on their devices, and find out more about their activities and the people and entities they communicate with.

Y.J took precautionary measures online, such as being careful about accepting or accessing any anonymous link provided by an untrustworthy person or entity and using security tools to avoid any infringement or hacking. Despite these measures, Y.J was alerted by a group of activists working in technology and digital rights who were seeking to identify Gulf Cooperation Council activists~~,~~ whose names were on a list of watchers in cyberspace, that his device had been hacked by the Pegasus program. This program was being used by the Bahraini government to spy on political activists and human rights defenders. Y.J shared his dissatisfaction with the lack of internet security for activists in Bahrain, which puts them at risk as well as the individuals with whom they come in contact. This is considered a major obstacle to the activities of militants. Y.J also believes that activists have no space for cybersecurity and that their privacy is being violated in a variety of ways. Y.J believes that the periodic screening of the smart devices of political activists and human rights defenders is a violation of privacy as well because these checks require examining all private files on smart devices and following up on the process of data transfer on the Internet in a certain period.

Therefore, Y.J pointed out political activists and human rights defenders have neither security nor privacy in cyberspace, so it is important for the activist to use protection programs to prevent monitoring and hacking, and to keep sensitive and important data away from cyberspace. Y.J hopes that legislation will be passed by the European Union that restricts the sale of spyware and surveillance software to repressive governments in the GCC countries, while imposing monitoring of how governments use these technologies. The Kingdom of Bahrain bought these programs and technologies under the pretext of protecting the Internet from cybercrime by tracking down criminals and hackers, however, they also use these technologies to find and spy on human rights activists.

The second interview was with B.J, who is a journalist and media activist based in the United Kingdom. They understand cybersecurity as defending citizens against flaws that allow hackers to infiltrate and breach electronic gadgets and mobile devices. These flaws often infect computers after clicking on specific URLs sent via e-mail or messages on social networking sites.; Moreover, they believe cybersecurity is continuing concerning cyberspace privacy B.J has been subjected to a lot of cyber-hacking efforts in various forms and graphics, such as bogus messages with links and files intended at hacking. Many of those who violate their rights and wish to contact the media to share their concerns and suffering are scared to speak in cyberspace for fear of being exposed to any infiltration, or retaliation that would compromise their security. B.J uses the Internet with extreme caution, they do not accept any messages or links from an untrustworthy site or person. They also attempt to examine their devices regularly to ensure that they are clear of any malware or monitoring software.

B.J contacted the Forbidden Stories organization, which is a non-profit organization dedicated to "continuing and publishing the work of other threats, prison, or murder." to do a check on their equipment. B.J also noted that certain human rights groups in the United Kingdom offer free services to search to inspect their gadgets and install a security application to secure their privacy and prevent them from hacking. B.J. believes that companies that sell spy and surveillance programs do not verify how countries use them, even though these companies export and sell surveillance and spyware programs to GCC countries to limit terrorism and monitor terrorists, while the Gulf Cooperation Council countries use these programs to monitor human rights, politicians, and terrorists. B.J. also feels that the concern of a lack of cybersecurity should not be over, but that human rights activity should be continued.

The third interview was with human rights activist Y.S. from Saudi Arabia, who started they activism of defending economic rights in 2000 when they started using the Internet in Saudi Arabia. Y.S. defined cyber-security as a tool used to preserve people's rights in cyberspace, but like other types of security, governments, repressive, and unjust regimes use it to monitor and suppress activists, politicians, reformists, and revolutionaries. Y.S. mentioned that they came from an environment in which institutional work was not allowed, and the people were deprived of any institutional work for civil society, so the alternative work available was the Internet and the virtual world. Therefore, the targeting that occurred in the virtual world was stronger than targeting in real life. Y.S. participated in various groups containing dozens of activists inside the Kingdom of Saudi Arabia, but after the government began to ordering monitoring cyber intrusions, these numbers began to decrease, trust on the Internet and programs decreased dramatically, and it became clear to activists that whoever owns real space also owns cyberspace.

Furthermore, Y.S. said that there are a variety of hacking and phishing attempts, such as controlling personal email and websites. But the first official hack was in 2018 when Pegasus NSO hacked them hacked by Pegasus NSO. Y.S feels that privacy has been reduced and considers it non-existent in cyberspace. Y.S takes many precautions while using cyberspace to ensure the most significant degree of protection for the people who communicate with them, and because they believe in the importance of continuing human rights work and activity, no matter how high the cost.

However, these precautions are expensive, both mentally and financially since Y.S uses many different devices to communicate with activists and victims to reduce the rate of penetration. They also use a set of protection programs, and periodically check their devices from spyware and surveillance programs in human rights organizations that provide this service to activists and human rights defenders. they recently filed a case in the United Kingdom after he felt that he had been hacked many times and considered that his silence might be a reason that these penetrations continue in cyberspace. Thus, they filed a case against the company that exported the spyware to the UAE (United Arab Emirates) and the Saudi government.

Y.S believes that winning the case legally is important but highlighting the problem of cybersecurity in media is also too important, When the problem of espionage and penetration in cyberspace is discussed in court, it gives the problem a great level of attention from the international community.

The fourth interview was with S.W., a child, and family rights activist from the Kingdom of Bahrain. S.W described cybersecurity as the process of securing computers and smart devices against attacks in cyberspace from outside. They shared they were practicing activities in the field of children's and family rights comfortably, and they did not expect any attack in cyberspace because she did nothing illegal, and they were doing humanitarian work in protecting families and children, which cannot be considered a crime. In 2016, they began posting information related to crimes committed against children, which generated a commotion in the media. As a result, she became worried about the significance of protecting clients' right to privacy. The information that S.W had released in cyberspace regarding a slew of atrocities that were committed against minors led to their being questioned about those publications. Because S.W lacked any kind of technical or technological expertise, they did not use any protective software on their devices. They found out much later that they had been under surveillance by the authorities. Every one of their private files as well as the files of the individuals with whom they worked were being spied on. Because of the espionage conducted on their mobile devices, they were falsely accused of betraying their country, which resulted in her incarceration as well as the filing of further accusations against them Later, they were the victim of an assassination attempt that took the form of a deliberate automobile accident, which resulted in their suffering shattered bones in both their hand and legs. Because of this, S.W was forced to leave their own country and seek political asylum in the United Kingdom to protect their life and to continue their work in the field of human rights without interference.

The fifth interview was conducted with A.A the activist in freedom of expression and digital rights from Kingdom of Bahrain. For more than 30 years, they worked with many international organizations such as Security and Human Rights Watch and conducted workshops to educate people about basic human rights and digital rights. A.A. were arrested and imprisoned by the Bahraini authorities because of their human rights activities in the real and cyber space.

According to the A.A., there is more than one way to detect the presence of a hacking or spying program on activists' devices. The first is the finch method: by sending a specific message to the activist that contains a link that downloads a specific file or downloads the virus onto the device and thus the device becomes infected with the spyware malware. The second method, which is considered the most dangerous one, is Zero Click, which was created by some hackers, and the Israeli company NSO bought and sold it to governments. This computer virus does not require sending any link or jQuery, the only thing that this malicious computer virus needs to penetrate is a phone number, and thus it directs commands through the Internet from any place or country to the smart device and hacks it. This penetration occurs through certain vulnerabilities in smart devices

A.A said that a leaked list was delivered from the NSO spyware company, containing 50,000 numbers, among the numbers that were considered potential targets for espionage through the Pegasus spyware program, and there has been no additional information provided in the list except the mobile number. A.A. carried out a technical analysis of some of the phone numbers mentioned in the list of human rights activists, and it confirmed that approximately 40% of these phone numbers were hacked.

A.A pointed out that other methods that have been adopted to detect spyware and surveillance programs in the devices of human rights activists was the analysis report program of the operating system, which would provide a full report on what happened to the system, such as information about the programs used in the smart device., and detailed information about the wired and wireless networks that were used to access the Internet. By analyzing this information, it is determined if the device has been hacked by a malicious virus. The other methods that A. A pointed out are based on connecting the device to be examined to a private network and monitoring the device's internet traffic for two days to two weeks, and then checking if there is any contact with spyware programs.

A.A. stressed the importance of having technical awareness among activists and human rights defenders, to protect against any penetration, by following some precautions, such as noting the battery work, if it runs out very quickly, which will indicate the presence of other activities or operations in the device, as well as precautions not to opening any links or messages sent by people with untrusted or known faces, besides to passing the issue of privacy and not giving identical personal information on every website, because that could lead to having social engineering, where the hacker can arrange a scheme or trick by which they can hack the smart device through Match personal information on different sites. Activists and human rights defenders must also keep sensitive and valuable information away from smart devices because the danger of penetration in cyberspace has increased dramatically due to the rapid development of hacking programs.

A.A. believes in the importance of exposing these cyber hacks in the media to put pressure on governments and the international community to enact stricter and clearer laws regarding the sale of hacking programs to repressive governments. Especially the cases that were filed by human rights activists against companies selling spyware are not clear. This is because most of the spyware that was used to monitor and spy on activists and human rights defenders in the GCC countries was issued by the NSO company. NSO sold spyware programs only to governments, with a need for approval from the Israeli government. Besides that, there are no representative offices for this company in the countries where Cases have been brought against them in court. Furthermore, these programs are considered strategic defense weapons, and preventing their sale requires approval from the Israeli Ministry of Defense. This complexity in the case's procedures shows the difficulty of having a successful case in court, but the human rights defenders find the large focus of the media on the problem is getting the attention of the international community.

Finally, A.A. confirmed that there is no monitoring of the use of spyware and surveillance programs by companies producing these technologies, as there is no evidence to prove that the decision to monitor and spy on activists went through all the legal frameworks and procedures that it requires, such as the authorization of the prosecution or the court ruling. However, these technologies tend to be purchased and used by repressive governments without applying the standards and policies for the use of these technologies, and without oversight and accountability from the producing company.

The sixth interview was with M.M., a human rights activist and digital security consultant from the kingdom of Bahrain, who has worked in various human rights organizations for 20 years. M.M. found digital security in the Gulf Cooperation Council countries as being based on strengthening control in cyberspace through attracting international expertise and building and purchasing high espionage techniques. As for the use of censorship and spying on human rights defenders, it is not a new topic for authoritarian governments, which were practicing it through physical censorship and prosecution, but electronic censorship is considered new because individuals, in general, have become more connected to the Internet and technologies, so censorship has been replaced from Physical control to electronic control. Hacking mechanisms depend on the weaknesses of operating systems in smart devices, as companies specialized in monitoring are looking for loopholes in the operating system that enable them to implant and activate malicious programs in the device. One of the most important dangers of electronic censorship now is that it is cross-border and does not require the presence of the person to be hacked in the same place as the hacker. M.M worked on technologies used by governments such as the Pegasus hack program, and these technologies do their work silently. This was discovered after examining a group of human rights defenders from the Gulf Cooperation Council countries, that some monitoring programs in the device have been operating for many years, some of which reached 10 years. It is difficult to gauge the amount of information that has been stolen from these devices because these malicious viruses are able to penetrate all files in a device, even secret programs that are encrypted.

M.M has made various reports in different countries of the world about digital rights and surveillance technology and believes that companies who are exporting surveillance technologies will improve their malware and change their selling policies to gain more benefit. As the spy programs which have been sold to GCC countries, were worth millions of dollars, and the manufacturers will continue to make and develop these programs to achieve higher profits. Despite the range of complaints that were submitted by smart device companies such as Apple, against the manufacturers of malware. Take any official action regarding the production of these malicious technologies. Therefore, it is important for activists and human rights defenders to take precautions to reduce risks, and the activist must know that they are target for hacking at any moment.

As for the role of the European Union in restricting the sale of this malware, M.M said that the ability of the European Union to control companies located outside Europe is weak. For example, the Israeli company NSO, which the European Union recently investigated with companies about the misuse of its software in Monitoring human rights activists, but the company did not take any real action or change in its policy. On the other hand, the European Union can impose conditions and laws on companies producing spy and surveillance software located in Europe. An example of this is the company Fine Fisher in Germany, which has been closed in Germany, as a decision from the European Union due to selling surveillance technology to repressive governments where they use this technology to hack political and human rights activists.

M.M says there are three important measures that activists and human rights defenders must take continuously, firstly, update the operating systems of their smart devices, as a lot of malwares that is used in penetration depends on the presence of holes in the operating system, and constantly updating the operating system reduces the presence of these gaps Vulnerabilities that can penetrate smart devices through it. Second, the use of electronic virus protection programs, even if these programs will not be able to prevent malware developed to penetrate smart devices, but they will prevent a wide range of viruses and technologies that can infiltrate and hack the device and spy. Third, the frequent shutdown and restart of smart devices constantly. As some malicious electronic viruses disappear from the device after it is completely closed.

Finally, M.M. asserts that censorship cannot be completely prevented on cyberspace, as censorship in cyberspace is used to pursue criminals and terrorists, but as is the case in the Gulf Cooperation Council countries, repressive governments abuse the censorship technology in cyberspace. Imposing restrictions on the use of this technology and monitoring its use in the country will reduce the monitoring of human rights defenders.

Conclusion

The global growth in Internet users led to making cyberspace more active and complicated, the human rights defenders in GGC countries used cyberspace to make their human and political work more active but their governments used Surveillance technologies and hacking software to control the activities of human rights defenders in cyberspace.

The study discussed the challenge of the absence of cybersecurity for human rights defenders in GCC countries. and to achieve the goal of the research, four face-to-face semi-structured interviews were held with human rights defenders, and two face-to-face semi-structured online interviews with an expert in digital rights.

This study's primary and secondary data revealed that there is a lack of cyber security in Gulf Cooperation Council countries, where activists and human rights defenders are vulnerable to espionage and monitoring in cyberspace by authoritarian regimes. These countries spend money on spyware, surveillance software, and technologies that exploit security flaws in computers and smart devices. These technologies are sold for a huge amount of money by European and Israel companies for the sake of combatting terrorism and crime, but there is no control or oversight over how these governments employ their technology. Authoritarian regimes utilize these technologies to control cyberspace, prohibit human rights defenders from engaging in human rights advocacy.

Consequently, human rights activists are being charged with cybercrime, imprisoned, and prosecuted. Some of these activists opted to move to Europe, the United Kingdom, and America to continue their human rights and political work, while other activists were imprisoned and tortured in their home countries.

Many human rights defenders in Europe and the United Kingdom have filed lawsuits against companies that sell these technologies to Gulf Cooperation Council countries, particularly those who obtained evidence proving the existence of spyware and surveillance programs through periodic checks by human rights organizations' projects. My recommendation Regarding these issues, the lack of cybersecurity in Gulf Cooperation Council countries should be highlighted in the media, and companies that develop surveillance and espionage techniques should be held accountable, as should laws that define the conditions for selling such technologies, monitor how they are used by states, and prohibit their sale to authoritarian governments.

Although the Gulf Cooperation Council members have signed international accords guaranteeing freedom of speech, local regulations restrict this right. As a result, criticizing government practices that violate agreed-upon international human rights principles is a crime punishable by defenders. Activists agree that controlling and managing the internet has become more complicated. As a result, the governments have greater power to spy on, monitor, and control the activism work.

My suggestions for future research on cybersecurity include other regions for example East Europe, East Asia, or other countries such as Iran or Turkey. Furthermore, since my research was mainly focused on human rights defenders, I would recommend the next research would target author categories, such as state presidents, diplomats, and parliamentarians. This research used interviews as a method to collect data from human rights defenders and digital rights experts. The following research might interview surveillance technology companies that produce or sell the technology.

in addition, in this research, the problem was mainly about the absence of cyber security for human rights defenders in the countries of the Gulf Cooperation Council, but in the next research, I suggest that the focus and problem could be on the accountability of the espionage companies that sell software to repressive governments that use these technologies not to protect internet crimes but target dissents, civil society, diplomats and members of parliaments. which is against the aim and the goal of producing these technologies. in addition, it is against local laws, and guidelines of the countries that host these companies to allow these companies to function.

Bibliography

Aboul-Enein, Sameh. "Cybersecurity challenges in the Middle East." *GCSP* 17 (2017): 5-49.

Ali, Salaheldin M. Ibrahim. "Media Regulations in Gulf Cooperation Council Countries: A Global Perspective." *International Journal of Media and Mass Communication (IJMMC)* 1, no. 1 (2019): 144-157.

Alshabib, Haifa Nasser, and Jorge Tiago Martins. "Cybersecurity: Perceived Threats and Policy Responses in the Gulf Cooperation Council." *IEEE Transactions on Engineering Management* (2021).

Amoroso, Edward. *Cyber security*. Silicon Press, 2006.

Assembly, UN General. "Universal declaration of human rights." *UN General Assembly* 302, no. 2 (1948): 14-25.

Baldwin, David A. "The concept of security." Review of international studies 23, no. 1 (1997): 5-26.

Brey, Philip. "Ethical aspects of information security and privacy." *Security, privacy, and trust in modern data management* (2007): 21-36.

Cerf, Vinton G. "Internet access is not a human right." *New York Times* 4 (2012): 25-26.

Chawla, Ajay. "Pegasus Spyware–'A Privacy Killer'." *Available at SSRN 3890657* (2021).

DHS. 2014. A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. October 1, 2014

Garfinkel, Simson L. "The cybersecurity risk." *Communications of the ACM* 55, no. 6 (2012): 29-32.

Hankey, Stephanie, and Daniel Ó Clunaigh. "Rethinking risk and security of human rights defenders in the digital age." *Journal of Human Rights Practice* 5, no. 3 (2013): 535-547.

Human Rights Watch.EU: Strengthen Rules on Surveillance Tech Exports. New York. The USA. Human Rights Watch. (2020).

ITU (International Telecommunication Union). Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). (2009).

Joseph, P. Mani, and Barry M. Lunt. "IT in the Middle East: An overview." In *Proceedings of the 7th conference on Information technology education*, pp. 25-30. 2006.

Hakmeh, Joyce. "Cybercrime Legislation in the GCC Countries." International Security Department, Chatham House (The Royal Institute of International Affairs) (2018).

Kemmerer, Richard A. "Cybersecurity." In 25th International Conference on Software Engineering, 2003. Proceedings., pp. 705-715. IEEE, 2003.

La Rue, Frank. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression." (2011)

Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. *Hide and seek: Tracking NSO group's Pegasus spyware to operations in 45 countries*. 2018.

Moise, Adrian Cristian. "Cybersecurity and Human Rights." *Universul Juridic* Suplim (2018): 160-164.

Oxford University Press. 2014. Oxford Online Dictionary. Oxford: Oxford University Press. October 1, 2014

Public Safety Canada. Canada's Cyber Security Strategy. Ottawa: Public Safety Canada, Government of Canada. (2010).

Rahimi, Nick, and Bidyut Gupta. "A Study of the Landscape of Internet Censorship and Anti-Censorship in the Middle East." In *CATA*, pp. 60-68. 2020.

Rossini, Caroline, and Natalia Green. "Cybersecurity and Human Rights." *Access Date & Address (18.04. 2021): https://www. gp-digital. org/wp-content/uploads/2015/06/GCCS2015-Webinar-Series-Introductory-Text. pdf* (2015).

Shires, James. "The implementation of digital surveillance infrastructures in the Gulf." *Digital Activism and Authoritarian Adaptation in the Middle East* (2021): 16.

Shishkina, Alisa, and Leonid Issaev. "Internet censorship in Arab countries: Religious and moral aspects." *Religions* 9, no. 11 (2018): 358.

Stepanova, Ekaterina. "The role of information communication technologies in the "Arab Spring." Ponies *Eurasia* 15, no. 1 (2011): 1-6.

Tully, Stephen. "A human right to access the Internet? problems and prospects." *Human Rights Law Review* 14, no. 2 (2014): 175-195.

Wagner, Kevin M., and Jason Gainous. "Digital uprising: the internet revolution in the middle east." *Journal of Information Technology & Politics* 10, no. 3 (2013): 261-275.

International Reports

The United Nations (1966) International Covenant on Civil and Political Rights (ICCPR), adopted December 16, 1966, G. A Res.2200A(XXI). Universal Declaration of Human Rights, Res. no 217, adopted by the G>A. December 1948.

Appendix

Interview questions with the Human Rights defenders

1. What is your activism background?
2. How do you understand cybersecurity?
3. Did you face any cybersecurity challenges while working on human rights issues?
4. Does cybersecurity affect human rights and how?
5. Have you ever recognized spyware in your devices?
6. How did you discover the spyware in your devices?
7. How does this affect your personal freedom and privacy?
8. Do you feel safe using your devices (mobile phone or computer)?
9. Do you feel safe browsing the internet?
10. What are the steps to protect your devices and to protect the victims contacting you, do you use malware programs or encrypted programs?
11. What is the border between using these programs and protecting actual crimes on the internet that are happening every day?
12. Do you think legal measures and action should be taken against the countries using these spyware programs against activists or against the surveillance companies that sell these Technologies such as EU guidelines, and why?
13. Do you agree with the concept of balancing rights or proportionality which exists in the European Center for Constitutional and Human Rights (ECCHR) for example?
14. From your perspective how can we solve this problem despite all challenges?
15. What do you think the governments in Europe and UK should do to protect human rights defenders' digital security?
16. How can the academic community help to solve the problem from your perspective?

Interview Question for the technical specialists

1. What is your activism background?
2. How do you define cybersecurity?
3. How could spyware hack activists' devices?
4. How did you discover the Pegasus virus on activists' devices?
5. How can an activist know that his /her device was monitored when there is no noise in the line and the device works normally and probably?
6. What was the role of the front-line organization /amnesty technical team in discovering the virus?
7. How can two-step authentication prevent activists from being hacked?
8. What are the techniques /programs used to protect activists' devices?
9. What will be your advice to activists on the ground or in exile, how can they be safe or educated on their digital security?
10. What is your message to the academic community to raise awareness of cybersecurity issues?
11. What is your vision and recommendations to solve this problem, is it by binding western companies selling these technologies to dictators?
12. Are we in need of international conversion from the human rights council regarding cybersecurity?