CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Master in International Security Systems

Master thesis

2021 **Anastasiya Neskoromna/Rieger**

CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Master of International Security Systems

Anastasiya Neskoromna/Rieger

Impact of COVID 19 on Security Policies of States in the Area of Cyber Security

Master thesis

Prague 2022

Author: Ms. Anastasiya Neskoromna/Rieger

Supervisor: prof. David Erkomashvile, Ph.D.

Academic Year: 2021/2022

Abstract

The SARS-Cov-19 or in different wording the global Covid pandemic outburst have created an unprecedented scenario for various organizations, agencies and structures.

The COVID-19 pandemic in 2020 has become an extraordinary and shocking event for the world community and the global economy. On the part of the authorities, the COVID-19 pandemic is accompanied by sometimes harsh and ambiguous decisions, the consequences of which are felt by people in many countries of the world: movement between countries was stopped, businesses and enterprises were closed, the restriction was created, those who were sick or at risk of infection were isolated. There was also no possible assumption regarding how long such a mode of life will last. Many factors as a consequential chain of reactions from the pandemic in the aggregate have created a pleasant environment for altering and modifying the cybercrime landscape.

This work aims to analyze the factorial presence of modification in the sphere of cybercrime, cybersecurity, and governmental responses. Based on the results of the analytical assessment, it is highly recommended that different governmental structures should collaborate more on inner domestic collaborative levels among units and on external international levels among multiple governments. The creation of unified international legislation to protect entities and individuals is also highly recommended.

Abstrakt

SARS-Cov-19 nebo v jiném znění globální propuknutí pandemie Covid vytvořily bezprecedentní scénář pro různé organizace, agentury a struktury.

Pandemie COVID-19 v roce 2020 se stala mimořádnou a šokující událostí pro světové společenství a globální ekonomiku. Ze strany úřadů provázejí pandemii COVID-19 někdy tvrdá a nejednoznačná rozhodnutí, jejichž důsledky pociťují lidé v mnoha zemích světa: pohyb mezi zeměmi byl zastaven, podniky a podniky uzavřeny, omezení byl vytvořen, byli izolováni ti, kteří byli nemocní nebo jim hrozila infekce. Nebylo také možné předpokládat, jak dlouho takový způsob života potrvá. Mnoho faktorů jako následný řetězec reakcí z pandemie v souhrnu vytvořilo příjemné prostředí pro změnu a úpravu prostředí kybernetické kriminality.

Tato práce si klade za cíl analyzovat faktoriální přítomnost modifikací v oblasti kybernetické kriminality, kybernetické bezpečnosti a vládních reakcí. Na základě výsledků analytického

hodnocení se důrazně doporučuje, aby různé vládní struktury více spolupracovaly na vnitřních domácích kolaborativních úrovních mezi jednotkami a na externích mezinárodních úrovních mezi více vládami. Důrazně se také doporučuje vytvoření jednotné mezinárodní legislativy na ochranu subjektů a jednotlivců.

Keywords

Zero Trust
Zero Knowledge
SARS-Cov-19
SUNBURST
SolarWind
Cyberthreat
Zero-Day Exploits
Cybercrime
Cybersecurity
Malware
Ransomeware
Big-game Hunting (BGH)
DDoS XSS

Declaration of Authorship

1. The author hereby declares that he compiled this thesis independently, using only the listed resources and literature.

2. The author hereby declares that all the sources and literature used have been properly cited.

3. The author hereby declares that the thesis has not been used to obtain a different or the same degree.

Prague 03.01.2022 **Anastasiya Neskoromna/Rieger**

Acknowledgments

The author is grateful especially to those who supported me on this long journey. To my family and loved ones.

Table of Content

Impact of COVID 19 on Security Policies of States in the Area of Cyber Security

Introduction

The initial purpose of these work is to investigate and identify the prospects of perpetual correlation including direct and indirect opportunities and features of SARS-COV-19 global pandemic outburst and the consequential effects firstly, on the cyber security sector, including current state, developmental stage in process, and future prospects of revitalizing the field, upcoming prospects; secondly, the alteration of cybercrime landscape, the new features and strategical decision of modernization and hybridization techniques, incorporation of cybercrime activities into governmental structures as a part of the strategical superiority and as a new stage of warfare; Thirdly, the responses of international communities and governmental responses, the possibilities of securitization against this types of threat, the legislative incorporation into the systematical approach, the prospects of multi-government collaborative relationship for the purposes to the cyber threat preventive measures.

The focus and the themes examined and implode within this project will include the following:

1. The direct correlation of COVID-19 global pandemic outburst and its consequential chain of events impact on cybersecurity landscape, modification and boost of cyberthreat and cybercrime.
2. The mechanisms employed by the governments and governmental respond on a geopolitical level; employment of cyber preventive measures on governmental and legislative levels.

This work will attempt to conduct a comprehensive analytical assessment of the impact of the COVID-19 pandemic on various aspects of society: socio-political relations, economic processes, socio-demographic situation and geopolitical consequences.

With the proliferating number of online communication, the activity of cybercriminals as well magnifies and undergoes a transformational process of deviant forms of behavior in cyberspace and the emergence of new youth criminal subcultures in the virtual world.

The difficulty in solving cybercrime is that cybercriminals often act in conditions of non-obviousness, using modern IT technologies and vastly available tools on a dark-net.

Cybercrime could be considered an act of social deviation when a criminal purposefully aiming at causing economic, moral, cultural, political, social, and other types of damage to an individual or organizational structure, the state, through any technical means.

The scope of this work will be aiming at the analytical assessment of structural changes in the period since the start of the global pandemic outbreak at the beginning of 2020 up to the current period of the end of 2021.

The assessment will include various tools and features for the purposes of in dear analysis and adequate evaluation of situational circumstances related to the governmental perspective and changes in the cybercrime landscape; as well this paper will provide a piece of information on adoptive preventive measures from a cybersecurity perspective on battling global boost of cybercrime.

Chapter 1: Research Structure

1.1 Aims and Objectives

1.1.1 Research Aims

1. What was the organization's preparedness for the unpredictable global pandemic outburst and conversion towards remote working?
2. What issues were encountered in the way of transition?
3. How has the ingrained situation provided a lucrative environment for alteration of cybercriminal activity landscape, adapting and developing new hazardous tools and trends of attacks?

1.1.2 Research Objectives

The research objectives include analysis of the in-dept available quantitative information on fluctuations in cybercrime sector, for the period since the beginning of global pandemic outbreak SARSCovid-19 in early 2020 up to the current timeframe scilicet last quarter of 2021, specified and divided into categories relevant to this research, which will be following:

1. What are the major influencing factors instigated by pandemic and their attestation of correlation to the rapid increase of cybercrime activities worldwide?
2. What were the governmental measures imposed during that period of time vis-à-vis the cybercrime and preventive measures to reduce the criminal activities?
3. What are the implications posed by cybercrime activities on communicational and collaborative levels, including personal, inter companies, and governmental levels?
4. What are the development programs are in process with the intention of cybercrime reduction, namely cybersecurity elaboration such as Zero Trust, Zero-Knowledge security solutions, Fluctuation ledgers, and various preventive mechanisms?
5. What would be the best solutions to reduce cybercrime activities and strengthen cybersecurity measures, the prospect phases of implementation?
6. What would feasibly be adapted perspective in the next five to ten years on governmental inter-country, intra-country levels, basing the assumption on the current analysis of legislative trends of cybersecurity for the last five years?

1.2 Research Question

What is the layer leveled impact of the global pandemic outbreak of SARSCovid-19 on generic cybersecurity? What are the potential chain effect prospects in the field of cybersecurity and the evolution of cybercrime? What are the possibilities of future advancement of cybercrime threats in light of current cybersecurity measures?

1.3 Literature Review

1.3.1 Introduction

The primary objective of the proceeding dissertation is to analyze the conventional structural changes and abnormalities caused under the assertive impact of the pandemic crisis SARS-Covid-19, from 2020 through 2021, on the structural and organizational context of cybersecurity and security policies on a governmental level. The further examination would be focusing on two primary divisions of contextual analysis, theoretical and practical approach. Imprimis the research will provide a decomposition of theoretically structured vital components that may directly or indirectly have affected the structural, organizational context of security policies in the area of Cybersecurity due to the pandemic outbreak of SARSCovid-19.(Buill-Gill, D, Kemp, S, Miro-Llinares, M, Castano, N, 2020, pp. 49-52) Following the primal causes of boosted cybernetics attacks in the years of the pandemic and the vital need for Zero Trust Architecture models in identity protection.

1.3.2 Focus of the study

The focus of this preliminary study will be based on the change development of the security and cybersecurity challenges faced by governmental authorities around the world, arisen as a consequential complication of the global pandemic outbreak SARSCovid-19. The complication could be considered in two main frameworks; first, the challenges considering remote workplace. (Turner, C, Turner, C. B., Shen, Y, 2020, pp. 23-24) The majority of the global corporations and governmental structures were not adequately prepared for the altogether mowing in the direction of remote monitoring and operational collaboration, which led to a challenge considering a proper securitization of the hubs, working ledgers and secure identification of personnel. (Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X., 2021, pp. 2-3) Which made companies vulnerable for the cyber threats, such as misconduct of the communication channels and

plunder of financial assets or potentially valuable data and information.(Accounts Chamber of the Russian Federation, 2020)

Second, the rise of criminal activity is directly connected with the issues of unemployment. According to the United States Department of Labour, in only just six weeks, more than 30 million American citizens filed for unemployment subsidies, and by April 2020 official civilian unemployment rate was around 14.7%, which is drastic and considered to be the highest since the end of Great Depression. (U.S. Department of Labor, 2021, p. 2) (US Bureau of Labour Statistics, 2021)

1.3.3 Significance of the Research

Alongside the global change in a societal structure, the structural norms and principles of conducting social interaction as well as the business manner communicative interaction, the pandemic of SARS-Cov-19 had an unprecedented collision in the cybersecurity and cybercrime sector. The set of unique circumstantial matters has produced new altered community behavioral patterns and prompted the boost of cyber-crime activity alongside the already unstable societal relationship world. (Khan N.A., Brohi S.N, Zaman N., 2020)

In late 2020 and the beginning of 2021, Cisco Systems inc. conducted a series of research Which then assessed and reorganized data into a comprehensive Cisco Cybersecurity Reports directional towards analysis of current situation so called, the “new normal” considering remote workspace, as well the identification of possible new technological solutions that will help companies to adapt to this conditional state. (Cisco Secure Systhems inc, 2021, pp. 5-8, 32-34) During the pandemic, the growth of cybercrime was provoked by the economic situation itself: people lost their jobs, criminals became more active, there was a particular overflow of IT specialists towards cybercrime due to the unstable financial situation. On the one hand, with time, cybercriminals have created new tools and schemes, and the temporary situation of unpreparedness among companies for the remote work environment gave an opportunity for new strategic models development; the cybercriminal began to attack more and more businesses, which massively switched to a remote workplace. The conditions were favorable for cybercriminals; approximately 60% of organizations surveyed by Cisco said they were not ready for the security and data protection requirements associated with the transition to telecommuting. (Cisco Secure Systhems inc, 2021, pp. 5-8, 32-34)

Cybersecurity has come to be perceived as an essential and critical characteristic of business, governmental, and societal communication and will play a key role in economic recovery after the crisis.

1.3.5 Geopolitical Issues and Impact on Societal Structure

From the geopolitical standpoint, the Covid-19, with its consequential aftermath in the form of augmentation of cybercrime worldwide, had a proximate effect on multi-governmental relations. With the rise of attacks proximity on the healthcare and financial industries, the allegations appeared on global scenery that governmental authorities of specific countries endorse and even assist in some forms of specified cyberattacks, as well incorporate cyber units as a part of a fully sponsored governmental organization for the purposes of espionage and information theft. (UK National Cyber Security Centre, 2020) As an accusation of Cozy Bear attack on COVID-19 Vaccine Data 2020, with an intention to pilfer vaccine and informational data about treatments, to advance Russian vaccine program, supposedly attacked United Kingdom, United States, and Canadian organizations.(CSE Government of Canada, 2020) (UK National Cyber Security Centre, 2020)

If assumed from a different perspective, the national governmental structures is an utmost priority due to the fact that without some form of governmental structure, there would be anarchy, therefore in any form of national crisis, the governmental figures of high importance such as president, congress, government level offices, are highly valuable for the prospects of the state, therefore are the primary objects for protection and preservation, as well are primary targets for attack. In the particular case of preservation of governmental officials in the face of the global pandemic SARS-Cov-19, it would be reasonable to assume that the initial testing regarding vaccine was primarily made, nevertheless to ensure and reinforce positive outcome afterward, the vaccination, the detailed information regarding the health condition of every individual, in these case governmental officials, must be gathered; therefore any chronic illnesses, or acute illness and symptoms, must be scrutinized, consequently classified and stored.

Therefore, from the prospect of the attack on Vaccine centers, the hackers were not gathering the common information regarding regular citizens but instead gathering prioritized confidential information regarding the governmental officials. Nevertheless, it is just an assumption.

As well as an infamous SUNBURST Malware Supply Chain Attack 2020 was a part and catalyst for the significant data breach as a part of SolarWind cyberattack reverberating on more than eighteen thousand detachments of businesses and governmental organizations. (The Guardian Labs , 2020) (Nakashima E., Timberg C., 2020, Washington Post) (Lohrmann D., Lohrmann D., 2021)

The perceptible victims comprise:

- Microsoft
- Deloitte
- Intel
- Cisco
- The National Nuclear security Administration
- The Department of Energy
- The State Department
- The Department of Homeland Security
- Administrative Office of the United States Courts; Case Management/Electronic Case Files
- Department of Justice
- Department of Labour
- Department of Treasury
- Department of Agriculture
- Department of Commerce
- Department of Defense
- Department of Health and Human Services

(Lohrmann D., Lohrmann D., 2021)

The fact that cybercrime and cyberattacks became incorporated by some countries as a part of hybrid warfare bears witness to the certitude volatility of the global economy and effective and efficient adaptation to circumstances matters. The process of globalization, which consists of the universalization and integrity of the world, accompanies the development of cybercrime; it is of great importance to study the forms of control over the integration, taking into account the technological capabilities that states have. Nevertheless, the various states perceive other countries as neither friends nor foes but as potential rivals, therefore the information tracking is utmost priority, as in the famous saying on Nathan Mayer Rothschild: “Who owns the information, owns the world itself.”

The tracking and monitoring of an adversary may empower many different varieties of tools, in some way even not completely ethical.

According to Eugene Kaspersky current global situation in the world is getting more fragmented even despite globalization, and the geopolitical situation is very far from perfect. The speakers at United Nation Governance Forum 2020 featuring Ms. Latha Reddy Co-Chair and Global Commission on the Stability of Cyberspace, and Eugene Kaspersky a cybersecurity expert and the CEO of Kaspersky Lab, emphasize the importance of multi-government collaboration in the sphere of cybersecurity.(United Nation Internet Governance Forum, 2020) (Buxton D., 2020)

According to an ITU the Internet telecommunication Union, since the start of the pandemic in 2020, there has been an approximately 10% increase in internet bandwidth usage, which is considered to be the largest increase in a decade. (UN Internet Telecommunication Union, 2021) Nevertheless, the cybercrime and cyber-incidents during the same period of time had increased by 69% of complaints only from the American citizens. (Federal Bureau of Investigation Internet Crime Complaint Center, 2020, p. 3) As well the Tech Support Fraud in 2020 complaints increased by 171% loses from total of sixty countries, compared to 2019. (Federal Bureau of Investigation Internet Crime Complaint Center, 2020, p. 13)

The speakers of U.N. Governance Forum 2020 have emphasized four main vectors for standing up and reducing cyber-crime:

1. Firstly, practical and strategic convergence maintains adequate information circulation and facilitates the shared experience and potential threat preventive measures.
2. Secondly, the presence of some level of trust in multi-party collaborative and separate party participants' legal and jurisprudential systems.
3. Thirdly, a broad-based partnership across technological, defense, trade, services, and other critical vital areas.
4. Fourthly, a considerable multiplicity of efforts to build and maintain in nations cognitive perception of this positive effects of collaborative actions.

(Reddy L., Internet Governance Forum, 2020)

Nevertheless, at the current state of geopolitical bipolarity, it is near too impossible to talk about those kinds of collaborative perceptions; certain countries would be opposed to the idea of creating another legally recognized international defense body to uphold the cyber issue. (Reddy L., Internet Governance Forum, 2020)

1.5 Methodology

1.5.1 Research Approach and Objectives

This work would revolve around the combination of the qualitative and quantitative methodological construct. By combining multileveled techniques and types of examinations, the author aims to inquire and ascertain the multidimensional structure of the issue at hand, explore and analyze the topics from different perspectives of arduous patterns and construct, and the future prospects of transformation and hybridization. (Lamont C., 2015, pp. 26-32)

From the qualitative vista as a first step would be examined scholarly articles concerning the direct and indirect correlation between global pandemic SARSCovid-19 as an aggravator for the boost of cybersecurity crime. The author will focus primarily on the analysis of triggering factors for the rapid increase of cybersecurity issues. The analysis will consist of the following steps: firstly, the impetus correlation of the consequential governmental measures aka restrictions in the form of stringent lockdowns and the formation and refinement of new hybrid types of cyberattacks activities, with the focus on the existing models of cyberthreats—secondly, the delayed governmental restrictions in regards to those mentioned above. Thirdly, the preventive measures and the types of the preclusive algorithms and structural elaborative machinery solutions, for the securitization of the potentially valuable data and information, as governmental engendering solution similarly a private one inclusive. (Lamont C., 2015, pp. 94-108)

From the quantitative perspective, this paper will analyze the cardinal number of data collected during the period of the firstly initiated lockdowns starting from March 2020 up until now November 2021, in two countries pivotal to the research. Russia, due to factorial implications and accusation by the US and European Union for orchestrating a targeted national government-sponsored cyberattack attack on vital economic fields of multiple sovereign states. (Lamont C., 2015, pp. 116-123) The US due to its advanced e-commerce platforms market and a relatively weak protection system. Due to the system of social security numbers, which is de facto a national individual identification number for multiple purposes, the cybercriminals have an opportunity by snitching one number to get access to all of the individual's credentials, therefore committing identity theft. (The United States Social Security Administration, Puckett C., 2010) This number is often required when applying for a job, in banks for opening accounts, renting apartments, as well as when providing medical services. Following Aete Group's research, almost half of the US residents, precisely 47%, have experienced identity theft in the year 2020; (Aite Group LLC,

Giact Refinitiv Company, 2021, pp.10, 41) This was a 42% increase in losses from identity theft which is $712.4 billion in the year 2020, in contrast to the loses of $502.5 in the year of 2019. (Aite Group LLC, Giact Refinitiv Company, pp. 9)(Lamont C., 2015, pp. 116-123)

1.5.2 The Research Approach

For the reliability and validity of the structural, contextual framework the research literature of the following dissertation will be submerged into two structural categorizations:

1. First, the structural analysis of a postulate employed in the discipline of cybersecurity, governmental structural scope, as well the systematic study of description and methods empowered by the research.
2. The second category will be entirely devoted for the primary research and analysis of the current issue at hand of this work velidelicet.

The combination of two conceptual approaches will allow conducting multidimensional research reliable for the in-depth analysis and formulation of structurization rational accession towards multilayered issues that this paper focuses on providing answers to the issues at hand. (Lamont C., 2015, pp. 46-51)

1.5.3 Research Outcome

For the purposes of the in-depth analysis and evaluation of topics at hand the structure of the epistemological research will the a road of empirical behaviorism and naturalism. As a part of philosophy, the primary task of epistemology is a reflection on what is considered cognition and knowledge. (Lamont C., 2015, pp. 13-18) However, modern information processes and technologies, colossally mediating the relationship between the recipient of the information and its source, this factor significantly increase the possibilities for manipulative influence and bias on consciousness. (Mamchur E. A., 2010, pp. 51-64) Most commonly accepted that the structure of natural science presupposes methodological reductionism. (Mamchur E. A., 2010, pp. 71-75) According to the generic interpretive outline, the affirmation that the internal pattern of an object or some form of phenomenon, depict theoretically, compose and provides a causal explanation for the observed macro-phenomena, determines the macro-characteristics of these objects. (Della Portages D., Keating M., 2008, pp.3-11) Nevertheless, some of the social sciences tend to associate with the basic causal and explanatory level of statements some macrostructures of the social systems. (Mamchur E. A., 2010, pp. 49)

The research aims to establish the correlative capabilities for prospects of cybersecurity and identify the potentiality of cybercrime deviation within the next decade, with a focus on the nearest five years of development. To analyze the extension of governmental response towards present challenges and the challenge yet to come in the field of cybercrime. As well the potentiality of inhibition or assimilation of malicious cyber practices with the adequate level of modification into the governmental practices for the purposes of securitization of the state actors.

1.6 Theoretical Consideration; Practices or Applications

By inducing the theoretical framework of a holistic approach, the paper aims to analyze the nature of role performance, variations in the social choice of state actors, by complying the as a tool is an integral part of a specific methodology, which can be called humanistic sociology high is considered to be a separate area of sociological knowledge framework. (Feurer, R. and Chaharbaghi, K., 1994, pp. 49-56) (Lamont C., 2015, pp. 134-141) The methods applied in the theoretical consideration framework will be based on the social constructionism model and critical theory. For the purposes of analysis, the paper will conduct a case study survey evaluating the stress point level in regards to the socio-normative changes and structuring changes as o consecutive chain reaction posed by global modification from the pandemic SARSCovid-19 on structuring behavioral, and communicative patterns of individuals. (Lamont C., 2015, pp. 134-151) The survey will address the communal changes with the focus on ongoing challenges of cybersecurity processes that individuals might have experienced in the past, since the start of the remote working, as well such issues as the training provided by the employer for the identification and prevention purposes of cyberattack and possible hacks; the amount of unidentifiable push notification received and various cyber incidents that participants might have experienced. (Orcher L. T., 2017, pp. 9-24)

With the view of theoretical consideration, the research will be revolving around the intermingle of practical epistemological theories. For the practical application of the findings, the research aims to conduct a multidimensional understanding of co-dependent correction of multiple theoretical variables to causally describe an observable macro phenomenon, in this case, the boost of cybercrime issues worldwide. (Lamont C., 2015, pp. 21-24)

Nevertheless, social science tends to associate with the basic causal and explanatory level of statements some macrostructures of the social systems. (Weber C. 2014, pp. 18-21) Global structures are aimed at self-preservation; it is pretty logical positioning, while the source of change is the activity of small groups, local forms of consciousness, and communication that change the societal structure within the inside steady but gradually. For instance, in this case we can refer to the lively dynamics of global communal dissatisfaction that arises in society under the influence of restriction measures posed by governments. (Gostev A. A., 2017, pp. 334-342)

Cybercrime Discussion

Cybercrime is commonly known as an illegal activity conducted utilizing computers and the internet; various types of cybercrime activities may include privacy violation, identity theft, financial extortion due to the personal data theft, fraud activities, intellectual data trafficking, data encryption and manipulation, espionage, cross-border crime, phishing, as well as malicious interference through computer networks in the operation of various systems. (Gordon, S., Ford, R. 2006, pp.13-17) It is volatile and potentially may harm the individual's or communal financial health as well as the security, privacy prospects in general. The sources of cyber threats have a white variety of potential origins, such as hackers, business competitors, national governments, terrorists, industrial secret agents. (Bossler, A. M.; Berenblum T., 2019, pp. 495-497) Moreover, all the cyber threats could be categorized by multiple criteria, for instance, the attacker's resources, organization, or funding. There are also three types of potential cyber threats:

- Unstructured Threats. This means the attacker individual or a small unstructured group of individuals has no organizational or managing pattern, and betake a widely available on a dark-net cyberattack tools, which is easily detectable, and usually exploits the documentation system vulnerability such as Zero Day Exploits. (Cybriant Computer&Network Security Management, 2018)
- Structured Cyber Threats. Most commonly, a well-prepared and coding trained individual or a group. With well-planned patterns of behavior and systematic preparation for the specific attack, it has available funding. Usually focuses on the attacks of a particular individual of an organization, with the extortionist motives on the sensitive information carefully gathered. (Cybriant Computer&Network Security Management, 2018)

- Highly Structured Cyber Threat. It is an extensive organization with considerable funding available and planned beforehand for which purposes and in which stream it will be used. Most commonly, it is a long-term purposeful attack exploiting any available resources at hand such as social, technical, and insiders information help. (Cybriant Computer&Network Security Management, 2018)

According to CTU (Counter Threat Unit) in 2021 ransomeware landscape still continues to thrive, and there is an 8% increase in Quater1 and Quater2 compared to the same period in 2020. (Secureworks Inc. CTU, 2021, pp. 5, 29) Moreover, the zero-day exploits flourish as well due to the boost of the online market developments. A zero-day exploit or 0-day is a previously unknown vulnerability in a software system, or the fix for that has not been developed yet, that attackers exploit in network attacks.(Secureworks Inc. CTU, 2021, pp. 21-22) The terms origin is associated with the fact that vulnerability becomes publicly known before the release date by the software manufacturer. These vulnerabilities can potentially be exploited on running copies of the application without the ability to protect against it. (Secureworks Inc. CTU, 2021, p. 52)

As was discussed previously, in addition to hackers seeking to profit by stealing personal and corporate data for a ransom, some of the countries are now incorporating and using cyberattack tools to infiltrate other governments and launch attacks on critical infrastructure as well to diminish the public image of the states by leaking some sensitive classified data. Cybercrime nowadays poses a severe threat to the private sector, business corporations, individuals, governmental structures, and the sovereign states. It is most likely to presume that government-sponsored attacks are expected to rise, with attacks targeting the critical infrastructure of particular concern. As we can observe in the case of SUNBURST malware supply chain attack, or in other words, 2020 United States federal government data breach, the APT (Advanced Persistent Threat) targeted attacks are becoming more and more volatile.(Kaspersky Lab., 2018) (Jenkinson A., 2021, pp. 19-23) According to the US Governmental investigation concluded that attack was carried by the Russian Government-sponsored hacker group Cozy Bear. (Kantchev G., P. W. Strobes 2021) (Sanger,D. E., Perlroth, N., Schmitt, E., 2020)

The research will employ the interdisciplinary concept as a way to employ main features of science and intellectual activity. Interdisciplinary interaction is a diachronic and emergent element that characterizes manifestation dynamics and allows to embrace new forms of organization of scientific knowledge. In this work, the results of the activities of

law enforcement agencies in combating cybercrime activities, incidents, and attacks in 2020 are presented for analysis; in comparison with the same period, it will reveal the key trends in the development of cybercrime at the stage of adaptation and integration of society and the state to the current situation. The findings would be based on the provisions of the dialectical method of scientific knowledge of social and legal reality in a pandemic as a reflective theoretical assessment for exploring contradictions in findings. By assessing analytical comparison and synthesizing scientific publications, the key elements of the research were formulated. Particular attention should be paid to the systematic approach for the purposes of explaining the dynamic indicators of changes in the cybercrime landscape.

The purpose of this work is to consider the peculiarities of the drastic alterations and purposeful developments of cyber-crime during a pandemic, ascertain the problem of ensuring cybersecurity stability and enhancement; as well to focus on an integrated approach and timely response of prevention measures to limit mass victimization, and especially across vulnerable segments of the population and vital governmental infrastructures. (DiFate, V., 2007) (Kelly, Thomas, 2016)

From the perspective of theoretical consideration this work will include as such Comparative Politics science, by comparing and contrasting political phenomena in different political systems of chosen countries for the assessment; Among such observed phenomena would be political processes, relations, institutions, political culture regarding cybersecurity implications. (*Wiarda Howard J., Graham Lawrence S. , 2002,* pp. 2-7, 103-108)The empirical data assessment would be conducted beforehand of any assumptions or theories are put forward; This is required to increase the objectivity of the conclusions and assumptions. (Caramani Daniele, 2017, pp. 21-29)

In addition, the conclusions for this work would be made based on a comparison of some aspects and features of political phenomena, which would be not entirely accurate since they would be based on empirical data. Considering the fact that there are three types of variables - dependent, independent and interfering; There is a relationship between the first two since the independent variables usually reflect the characteristics of the environment, they affect the changes in the dependent variables. (Inglehart Ronald, Welzel Christian, *2002,* pp. 143-151) Comparative political science provides a valuable opportunity to consider the standard and distinctive features of different political systems and regimes, compare their advantages and disadvantages, especially their acceptability or unacceptability for specific countries and peoples, the perception of these regimes from a different

comparative point of view. (Caramani Daniele, 2017, pp. 21-29) This aspect is of particular importance for this work that acmes to evaluate so-called transitional, mixed and hybrid regimes, and process of adaptation. (Inglehart Ronald, Welzel Christian, *2002,* pp. 144-156)

As well this paper will provide analysis from Multi-level Governance perspective for better understanding of how governmental structures interact and react on a specific hazardous situations, from the side of collaborative interaction and time frame of reaction. (Elgar Edward , Edited by: Enderlein Henrik , Wälti Sonja , Zürn Michael, 2010, pp. 17-32) For the purpose of conducting a thorough analysis, the paper will be primarily focused on the capabilities of intergovernmental structures and intercommunicating aptitude of specified countries as Russia and the United States.

1.6.1 New Types of Cyber Attack, Trends 2020-2021

This subchapter will be dedicated to various types of cyberattacks that are currently the most common. To understand the significance of the issue at hand, there is a need to understand the rooting of the problem and its validity of propagation. the rise of potential cyber attacks and data breaches became immanent challenge during the world pandemic of SARSCovid-19 due to the various factors.

Cyberattack Trends of 2020-2021:

1. **Malware/Ransomware**

Malware is a generic term for any malicious software that targets an application or operation of a programmable device, service, or network for the extortionist and compromising purposes, includes ransomeware as well as computer viruses. (Humayun, M., Niazi, M., Jhanjhi, N. et al., 2020, pp. 3-11) Cyber attackers and hackers usually use the malicious viruses and programs to extract data, consequently which they can use to obtain financial gain from victims. This data breaches could range from financial information data to medical records, social security numbers, emails, and passwords - anything can be compromised and then used for biased purposes of blackmail. (Chin Eian I, Ka Yong L, Yeap Xiao Li M., et al., 2020, pp. 3-11)

2. **The Big-game Hunting (BGH)**

Massive ransomer campaigns became more alluring for cybercriminals, primarily due to the circumstantial ecosystem created by the pandemic. (Ali Khan N., Nawaz Broh S., Zaman N., 2020, pp. 1-4) The vast majority of companies went from offline to online remote working

space without proper arrangements and system modification, consequently creating a significant opportunity for cybercriminals to get access to the company's sensitive information and databases through the employees. (Crodstrike **Holdings, Inc**, 2021, pp. 19, 24-25, 31)

Furthermore, even when new protective systems and codes were in place, unfortunately, it has not undergone the proper testing due to the lack of time for the design and transfiguration; This provided an opportunity for Zero-Day Exploits. (Secureworks Inc., 2021,, pp. 21-22)

3. Zero-Day exploits

Zero-Day exploits have become more and more applicable, especially during the current worldwide situation with the COVID-19. The Zero-Day Exploits denotes that unresolved system or program vulnerabilities, on which developers had zero days to fix the defect, as well it could mean the malicious programs against which as of yet defense mechanism has not been developed. These vulnerabilities become publicly inquired before the software manufacturer releases a bug fix; therefore, cybercriminals could potentially exploit the vulnerability on cyber copies of an application, sans the aptitude to defend against it. (Edelman Serge, Herley Cormac, Oorschot Paul C., 2013, pp. 41-46)

4. DDoS Attack

Distributed Denial of Services (DDoS) In this type of attack, hackers resort to the usage of fake bot users' identities to disrupt and crush the proper functioning of the system or organizations' website in order to discontinue communication channels. (Douligeris C., Mitrokotsa A., 2003, pp. 190-193)

A hacker attacks a computer system to disrupt a server's operation and bring it to halting, therefore creating the conditions under which common users attempting to access the website of the ecosystem will not be able to access the provided system servers or the process of accessing will be very challenging.Feinstein L., Schnackenberg D, Balupari R., Kindred D, 2003, pp. 303-314 Failure of the system can also be progress for cybercriminals towards mastering the system. In case of a state of emergency, the software could potentially give out any critical classified information - for example, a version or part of the program code. (Dutta S., Lanvin B., 2019, USA. 210-235) Nevertheless, it is often a measure of economic pressure: the loss of a simple service that generates income, bills from the provider, and

measures to avoid an attack that significantly hit the target's pocket. (Douligeris C., Mitrokotsa A., 2003, pp. 190-193)

5. Cross-site Scripting (XSS)

All of the attacks employed by cybercriminal groups and individuals, bear malicious intentions with purposeful intact for extortionists reasons. A type of attack on web systems consists of introducing malicious code into a page issued by a web system, or covering the transfer from original site page to crafted by cybercriminals alternative page with malicious intentions. (Grossman J., Fogie S., Hansen R., Rager A., D. Petkov P., 2007, pp. 3-7)

1.7 Literature Review

In the year 2020, the rapid expansion of cyberspace was caused by the new world-spreading disease SARSCovid-19. In comparison with previous years, in 2020 and 2021, there are much more activities that are taking place in cyberspace, which is understandable due to the socio-changes brought by healthcare restrictions on free movement, and social interaction imposed by multiple governments in different countries in order to stop the spread of the disease. The preventive measures contributed significantly to crime reduction opportunities on the outdoor such as robberies, physical violence, vandalism, and many others; nevertheless, with people spending almost all the time indoors, it cultivated the perfect basis for cybercrime opportunities and evolution of cybercrime activities. (Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X., 2021, pp. 2-6)

The pandemic was an accelerator of digitalization of society have brought a lot of changes and shifted the domination in cyber-community and cyberspace.

In accordance with the Center for Strategic & International Studies (CSIS) findings and the cyber threat report provided by the cybersecurity company Deep Instinct, on significant cyber incidents, in the year 2020, the ransomware attacks increased by 435% in comparison to 2019 and the malware attacks increased by 358% overall. (DeepInstinct, Center for Strategic & International Studies (CSIS, 2021, pp. 5-13) (DeepInstinct, Center for Strategic & International Studies 2021)

Currently we are in alarming state of cybersecurity statistic and prospects not so bright as one could expect. This general drastic situation is a call to actions forthwith, presently there is no time to spare. With the gradual scale of world advancement, the use of ubiquitous

computing constantly magnifies; consequently, there is an increase with the same ratio of the potentiality of cybersecurity threats, cyber-attacks, and privacy issues. In light of the recent outbreak of the SARS-Cov-19 pandemic, an extensive amount of social interaction has shifted into online space, with the number of online users increasing daily.

Digitalization and globalization facilitates the transition to the online environment ecosystem of multiple industries such as healthcare, businesses, education, and allows individuals and companies proceed with online purchases, get more information and data as well to share it.

1.8 Surveys

An anonymized survey will be conducted with the view of gathering quantitative data for the analysis on the current state of the situation in spheres of cybercrime and cybersecurity explored earlier in the academic literature review, with the intention for potential identification of ulterior areas of research, for the investigation and analysis, as well for comparison of issue and findings discovered in a literature review. The practical approach would be to appeal to the target audience through business and employment oriented online service Linkedin, due to the professionally-oriented magnification in the community of users and social media. The choosing preference of analysis and conducting information on/from social media platforms is due to several reasons.

- First of all, social media is an excellent tool for marketing and helps promote commercial products and services through visual content communication; various global companies promote their commodities on social media.
- Secondly, social media undergoing modification from being only entertainment platforms to becoming partly an e-commerce platform, allowing merchants to sell their products directly to the end consumers, which is significant support for small business owners, and artisans. Nevertheless, with these changes comes a variety of implications for businesses (including those who provide space for trade and those who trade) and more profitable opportunities for cybercriminals.

The survey will be focused and divided into two categories, dedicated towards two target groups, and conducted in two separate sections.

The first section of the survey would focus on those who are either experts in the field of cybersecurity, such as threat intelligence personnel, analysts, developers, or the procurers of cybersecurity technologies, which would be mainly conducted through Linkedin.

The second section of the survey would be dedicated to category number two and would focus on the working employees who, due to the SARSCovid-19 pandemic and governmental restrictions, are compelled to work remotely. Furthermore, what issues in cyberspace and cybercrime training they have encountered since the start of home office working.

1.9 The Applicable Tools

This section will be focused on parsing of the tools utilized in research conduction.

Google Forms

Google forms are a very efficient tool for conducting a survey; from many benefits provided by this platform, one of the time is that survey could be created quickly, with the most valuable and easy-to-use tools and features. It is pretty straightforward with no price limit or restrictions of the tools limit to create a survey.

The other beneficial feature is that Google Forms has an automated email notification function, which will inform the originator of a survey when someone fills out the survey, making it easier to monitor and track the process of conducting the data up to time. Compared to many other alternative survey platforms and applications that can only provide information regarding the survey only if the originator logged in to the account, therefore, it is challenging to access the information from other devices in real-time.

Thirdly, a very lucrative factor of using Google Forms is that this does not require any monetary investment; the platform is entirely free from charge, unlike other platforms that have a free poling limit of usage and require the user to pay a subscription fee.

Video Conferencing Tools

For conducting the interviews, the author will be using video conferencing tools such as Microsoft Teams and Zoom Meetings for the purposes of its effective and efficient features; both programs are free of charge and relatively stable on an internet connection, which is very suitable for the long distance communication especially during the pandemic era, with constant lockdowns all around the world. The Zoom meeting supports google calendar, and Microsoft Teams has its notifications and calendar, which is efficient to utilize.

Linkedin

Linkedin is an efficient and stable platform for professional communication, business, collaboration, and employment purposes, operating via websites and mobile app. For the purposes of this paper, it is viewed as an alternative tool to get in touch with professionals in

reliable industries, such as cybersecurity analysts, secure technological developers, Zero-Knowledge, Zero Trust security specialists, IT professionals.

This platform is valuable for conducting thorough research and analysis, for compiling a quantitive amount of reliable data and information.

Google Sheets

For the purposes of precise calculative estimates of the research quantitative findings of surveys, this work will be using google sheets. It is quite common and precise tool for comfortable and convenient use and accurate calculations of the results. The application interface is similar to the Microsoft Excel interface and is compatible with Microsoft Excel file formats. The user can work independently with tables editing, configuration and share with other users to collaborate in real-time.

1.10 Data Collection and Analytics Methodology

The data collected for this project will use an unconventional approach, primarily analyzing the Quantitative and Quantitative data separately from each other for the clearance of results; subsequently, the analysis would employ benchmarking against the collected data groups to discern if there are any similarities that could be compared or if there any differences in the data that may help the further research analysis.

Quantitative Analysis

From the Quantitative analysis prospect, the project will utilize RStudio, and Google Sheets, to analyze the average percent of responses concerning each specific question in the survey, with the focus on simple linear regression to analyze how strong the relationship between two variables, in case of this paper correlation between the global pandemic outbreak SARS-Cov-19, its consequential chain reaction complication in the form of governmentally posed restriction in different states as a preventive measure from the spread of the disease, and the drastic increase in internet-related crime, in forms of cybercrime, cyberattacks, and cyber-incidents all around the world since the beginning of pandemic up until the current period, last quoter of 2021. (Lamont C., 2015, pp. 116-128)

As well, the research and analysis will utilize for the survey perspective firstly a correlation test to ascertain if the variables are related absent the hypothesizing cause-and-effect relationship. Supposing the testing will prove relevant to the statistical component of the findings, the analysis will employ directly pertinent componential tool the regression test for

the analysis of the cause-and-effect relationship inter variables. (Lamont C., 2015, pp. 116-128)

Qualitative Analyses

For the qualitative analysis, vista will be used for the purpose of evaluating the contextual imagery, behavioral patterns of individuals, language, and observation; some of the data is contextual to the quantitative research, basing analysis on a crime statistical analysis, secondary data evaluation such as scholarly articles, interviews, forums, and international professional conferences regarding the germane topics to the research.

Foremost, the research will focus on the content analysis of the conducted information by categorizing and discussing the propriety of the collected data by standardizing its meaning into variables that would be analyzed separately. Afterward, finding the correlative patterns on whether of if how the variables communicative perception is conducted alongside the research. (Lamont C., 2015, pp. 94-103)

Thematic analysis will focus on the identification of fractions of patterns and correlative effects, specification on the purposes of examining the data conducted, and identification of broader themes and patterns. (Boyatzis, Richard, 1998, pp. 25-41) The steps of the Thematic approach will be following:

1. Familiarization, meaning thorough analysis and overview of the collected data.
2. Coding. It does not necessarily mean the encryption manipulations with the data, but the specifying the understanding of the particular patterns found along with the research and assigning them specific features and codes for the inception of a general singularity and simplifying the navigation through the data. (Boyatzis, Richard, 1998, pp. 25-41)
3. The themes Generation. By identifying the patterns alongside the data, the project will generate the specified themes followed by assumptive speculation in regards to each of the themes. (Resor, Williams C., 2017, pp. 10–11.)
4. Themes reviewal. A thorough analysis of the usefulness and accuracy of the data. This would help to find the additional characteristics and missing characterizations for the further formulation and profound evaluative measures in the research. (Resor, (Thomas J., Harden A., 2008)
5. Definition and naming of the themes. Formulation of a qualitative answer that the themes prompt to support, and in what way it helps to understand the data conducted. (Thomas J., Harden A., 2008)

6. Writing up. Formulating the thematic analysis and the establishment of a hypothetical research question. Evaluative and perceptive drafting with intentive purposes consequential for the analysis and inclination of the various detection of essential features. (Boyatzis, Richard, 1998, pp. 25-41)

1.11 Ethical Consideration

From the perspective of ethical consideration, the encountered issues regarding cybersecurity during the Covid pandemic pose drastic challenges on companies, individuals, and governmental bodies worldwide. The specificity of the research question and proposed questions in a survey can pose challenging ethical issues regarding informational data consent and confidentiality of provided information. The author intended to contemplate the participants with the intention of the collection of information through the survey and the initial purposes for the use of that information. For the purposes of confidentiality, the survey will be anonymized, therefore protecting personal privacy, no names will be disclosed, any relations to some organizations will be classified.

The survey research will include detailed information on how the acquired data will be applied for the evaluative process to inform and explain to the participants the principles implied in the research operation. For privacy purposes, the survey will include a confidentiality statement detailing the researchers' commitment to the privacy of any data gathered and the provision of anonymity or any information relevant to the respondent.

In this section, the author will be focusing on the protection of identity digital private company solutions. The privacy concerns are one of the utmost priorities of social interaction, hoverer with a rapid change of world scenery due to the pandemic; however, it became much more challenging and multi-layered complicated. Conditioned modification of intercommunion and cooperation among companies and inside the companies itself opens new horizons for potential cyber-attacks.

1.12 Limitations of the Methods Applied

Limitation for the Researcher and to the Methodology

Several challenges could pose some limitations for the research and evaluation of the project; consequently, the final version of findings may alter the research outcome, or it would not be able to be fully complete.

1. Size Sample. The issue at hand is that a sample size provided in the survey could pose a challenge if there are fewer respondents than expected; hence it may affect the accuracy of the research. Nevertheless, the projects' primary focus is qualitative rather than quantitive data analysis, and the project would be focused on the qualitative evaluation of the responses; therefore, it should be a moderate issue.
2. Relative limitation of available scholarly data. Lack of previous research due to the novelty of a problem at hand or insufficient amount of data may limit the research findings and analysis. It is arduous to evaluate and give a realistic return properly and possible suggestive solution to a problem based on an insufficient amount of data; due to the neoteric contingent apparition of Covid-19, there is only a limited amount of scholarly data available on this specific topic of the research, limited by a time frame of fewer than two years. Therefore, proclaiming presumptuous prognoses based on a relatively diminutive amount of information is not fully comprehensive.
3. Potentiality of Bias. As there is a potentiality of bias, inasmuch as it is an innate feature of individuals towards a specific outcome and findings, the research will be conducted in an objective add a conclusive way to limit the offset of the findings. All findings and statements would be endorsed by arguments and evidence of findings to avoid generalization, therefore with the purpose of limiting the potential bias to the extent of acceptance.
4. The Survey issues. In general, people tend to overestimate their ratings when filling out such questionnaires. In order to collect more accurate data, the following steps were taken.
    - First, a preliminary screening was carried out, during which participants were selected through the analysis. The main selection criterion was the desire and willingness to share data on their current state of affairs in the study area.
    - Second, during the questionnaire design, some effort was made to make all questions easily understandable for the respondents. The questionnaire was also accompanied by a glossary explaining any unfamiliar concepts or terms used in the questionnaire.

There is also a dispersion of data formats and sources that create a dynamic inconsistency in regards to the proper formation of cybersecurity preventive measures. Companies store the potentially sensitive data on a unified ledger, and the multi-party collaboration process, for instance, between manufacturer and client, involves every layer asset of the data. This

situational outcome may potentially endanger not only one party if the breach occurs on their side, but all the other participants of multi-party collaboration integrity would be compromised.

The most recent and most massive in an aptitude attack on governmental structural sovereignty was the 2020 United States Federal Governmental Data Breach. The cyberattack began no later than March 2020. (The Guardian Labs , 2020)

The attackers exploited software vulnerabilities from at least three US software developers: Microsoft, SolarWinds, and VMware. A supply chain attack on Microsoft's cloud service provided attackers with one way to hack victims, depending on whether the victims purchased the services through an intermediary. (Nakashima E., Timberg C., 2020, Washington Post) (Lohrmann D., Lohrmann D., 2021)

Destructuralization of chain components, relative provision of anonymity for cybercriminals, and lack of unified fluidity across judicial systems around the world provide an ideal milieu for the flourishment of cybercrime activities.

According to PwC's Global Economic Crime and Fraud Survey 2020, most disruptive fraud events by industry cybercrime gained leading positions in the Governmental and Public Sector with an increase of 17%, Health Industries by 16%, and Technology&Multimedia and Telecommunication with an increase by 20%. (PricewaterhouseCoopers, PwC network, 2020, p. 4) Finishing up the second in Financial Services sectors with an increase of 15%, and Industrial Products and Manufacturing by 15%. (PricewaterhouseCoopers, PwC network, 2020, p. 4) The survey was conducted to obtain and analyze quantitative information, from more than 5000+ participants, along ninety nine different countries. (PricewaterhouseCoopers, PwC network, 2020)

Chapter 2: Analytical Framework Assessment Covid-19 Impact on Cybersecurity

2.1 Introduction

The section will focus on the analytical assessment of information gathered from scholars' articles, the statistical evaluation provided, and the data gathered from the survey; afterward, the section will be focused on the presentation of the detailed report findings.
The methodological qualitative and quantitative findings will be assessed from the epistemological perspective for the purposes of segmentation and parsing examination.
The primary purpose of the survey is to gather raw data and information directly related to the initial purpose of this project:

1. Is there a direct correlation between the global pandemic SARSCovid-19 and the developing implications in cybersecurity sectors?
2. How did the challenging pandemic health situation across the globe affect the boost in cybercrime?
3. What are the prospects of the future development in cybersecurity, that same way in cybercrime?

The survey has a role of a supportive argument for this project; therefore, this section will analyze the results obtained in the process of conduction following the descriptive methodology and Data Analytic methodology (Section3.5). The descriptive analysis will be focusing on the most relevant answers provided directly issued and relevant to the focus of this research project.

2.2 Analytical Assessment

The McAfee which has released a new global report, The Hidden Costs of Cybercrime, the assessment focuses at the most significant financial and less obvious impact. According to the findings of this report, cybercrime has cost the global economy more than $ 1 trillion dollars , or arrpoximatelly 1% of global GDP, according to the findings of this report, prepared jointly with the Center for Strategic and International Studies (CSIS). (Malekos Smith Z., Lostri James A. E. Lewis, 2020, pp. 3, 6) Compared to 2018 data, this indicator has grown by more than 50%, at that time the cost was about 600 billion US dollars damage to the global economy. (Malekos Smith Z., Lostri James A. E. Lewis, 2020, pp. 3, 6)

McAfee's research and analysis has revealed a lack of awareness of cyber risks across the organizational structure, and due to that fact, companies and individuals are vulnerable to advanced social engineering cyber attacks. One of the primary challenges is that once a personal computer has been compromised, it is rarely possible to detect the bias problem in time, therefore stopping the virus from spreading. (Malekos Smith Z., Lostri James A. E. Lewis, 2020, pp. 3-10) According to the produced report, in December 2020, around 56% of organizations participating in the survey acknowledged that their companies do not have a plan for preventive measures and prompt response to cyber threats. (Parachute Technology, 2021)

2.2 Survey and Findings

2.2.1 Number of the Respondents by Industry:

This question's initial purpose is to obtain the data and provide an analytical assessment; therefore, it is done to analyze whether there is a connection between the industry and Figure cybercrime activities. Unfortunately, due to the insufficient amount of time limitations and data, it is impossible to provide a complete result of the connection. Nevertheless, the chart shows overall number of the respondents by occupation sector the industry that they work in. The top occupation sectors of survey participants on the first place is Management Sector with 18%.

After that, on the second place is IT Sector with 14% of the respondent from that sector. Following in third place was divided among Security (Cyber) sector and Education and Research with 11% each.

Following that the respondents account for 7% each sector from E-commerce and Real-estate.

Lastly the remaining industries bu respondents which account by 4% each sector are Healthcare, Public, Governmental, Media, Communication, Manufacturing, Automotive, and Banking & Finance. Further assessment regarding the relevance would be provided with the next graph.

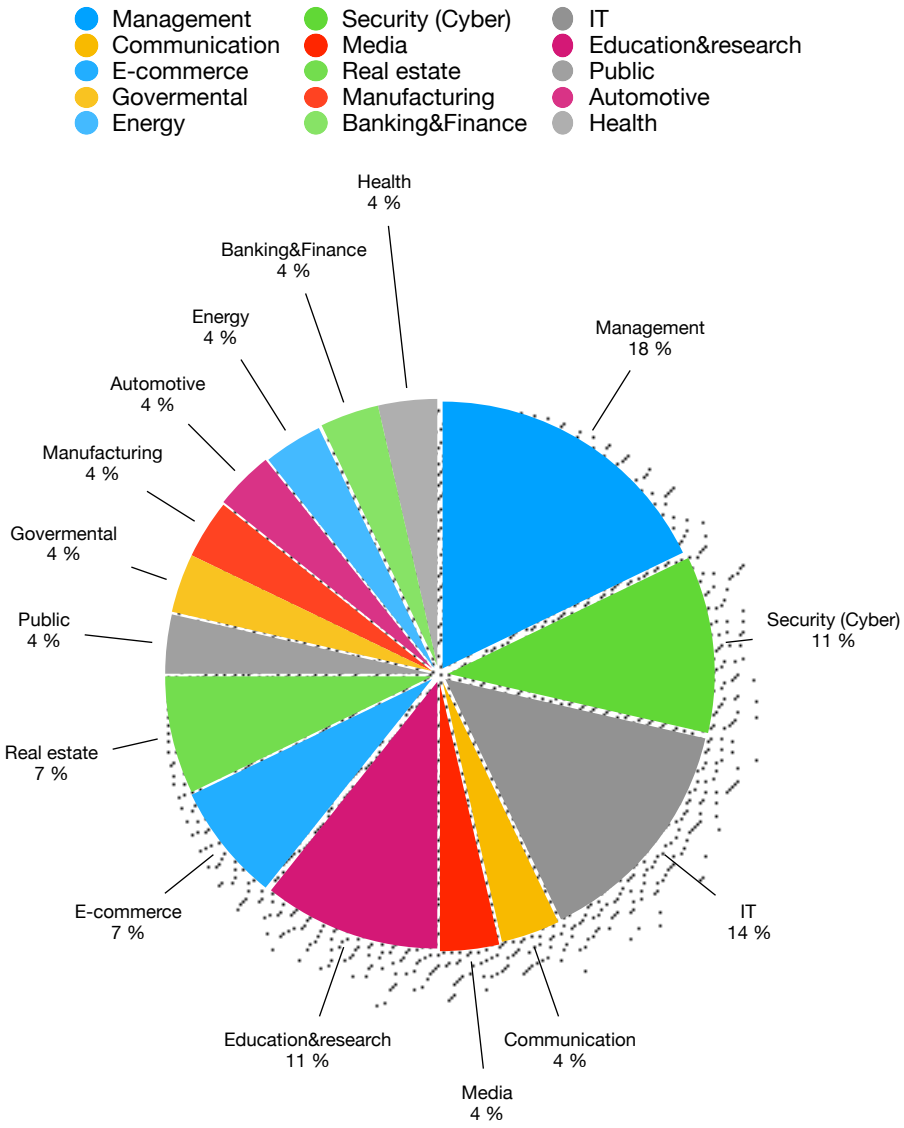

Figure 1. The devision of respondents according to the occupation sector.

2.2.2 Technologies Implemented to Assure a Remote Working Process:

The purpose of the question regarding the tools and features provided b employers to assure and secure the work process out of office premises to the online collaborative space was to understand the level of alacrity for the galvanic situation worldwide pandemic. As well as to evaluate how likely are, the companies will conduct themselves undergoing critical situations, in these cases from the perspective of the cyber threat, and how likely they are to get off easy with a slight fright, rather than being a victim of cybercrime.

Considering the technological implementations by employer side the tools were provided to the respondents of survey were as following:

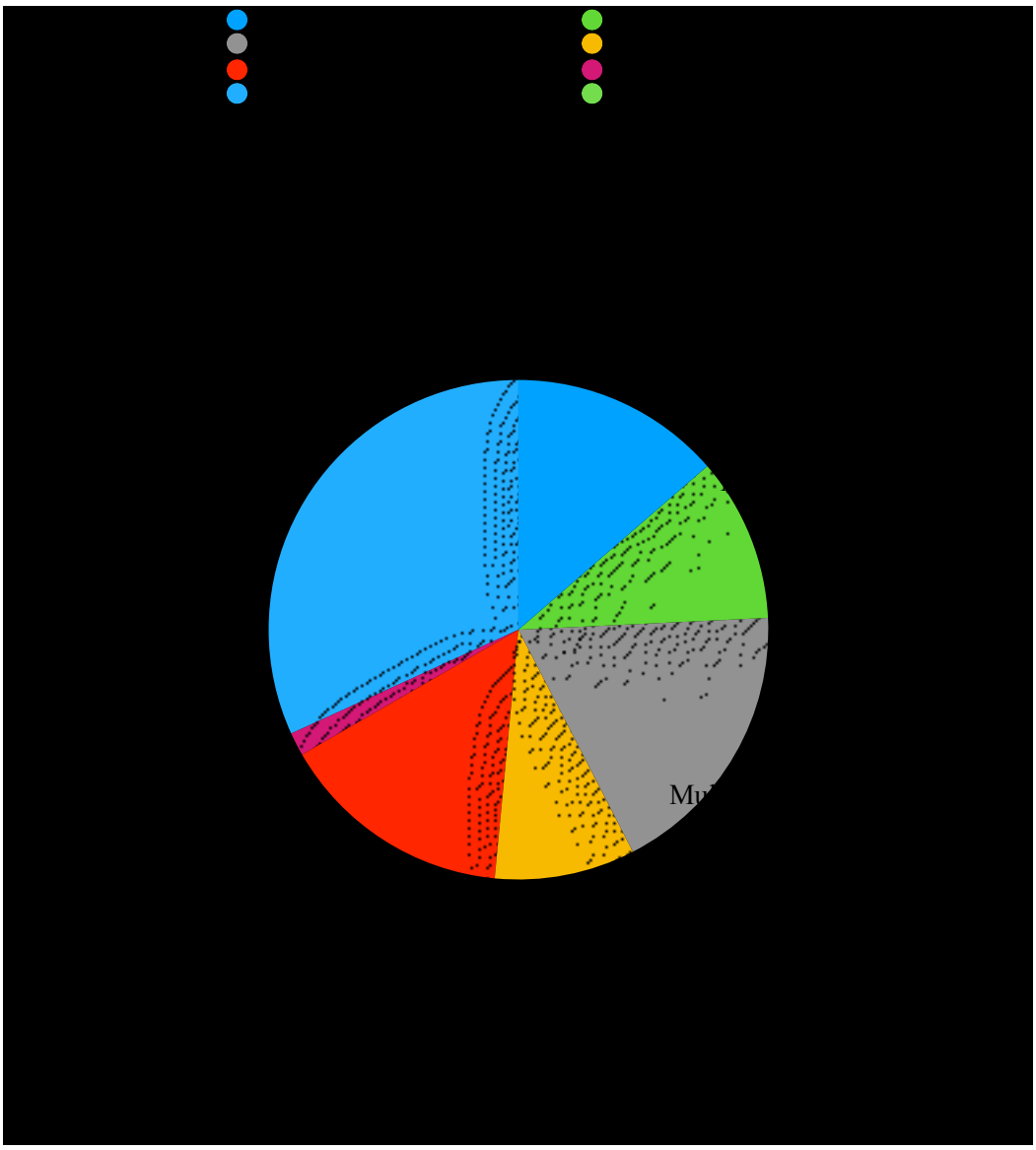

Figure 2. Technology that have being implemented to assure and secure the remote working process.

As a top tool provided by the employers side were the video conferencing tools such as Zoom, Microsoft Teams and other collaboratively effective video providers employed regarding to the companies regulations as 32% of the respondents implied that information.

On the second place is more elaborative feature that signifies higher level of promptitude and preparedness to such kind of situations, the Multi-Factor Authentication with 18% at the surveys evaluation an extended authentication, a method of controlling access to something in which a user must present more than one proof of an authentication mechanism to gain access to information.

Following on the third place the 15% positive responds the Drive Encryption tools with the ability to translate data on a disk into an unreadable code that an illegal user cannot easily decrypt. Disk encryption uses special software or hardware that encrypts every bit of storage; One of the most relevant tools for business communication. (Techopedia, 2017) The complexity of the disclosure determines the reliability of the encryption algorithm further going; There are also different degrees of strength of the encryption algorithm, as well different standards govern them. (Techopedia, 2017)

Following the 14% of the survey respondents voted for the classical security tools against the cyber threats such as already initially installed on their security devices as Avast antivirus system, phishing training provided by the employer, firewall, the Nmap a free utility designed for a variety of customizable scanning of IP networks with multiple number of objects, purposefully to determine the condition of objects of the scanned port network as well as their corresponding services; even though the fact this network mapper is already 20 years old it is still up and coming pithing the frequently used tools for the cybersecurity protection on internet. (Nmap Scripting Engine. Nmap.org. [Online Source] 2021)

Ensuing the participants voted for the Network segmentation with the 11% following, which is is a logically or physically separate part of a network; These tool helps dividing the network into segments and carried out to optimize network trafficking and increase the network's security as a whole. (Network Segment Definition, 2005, [Online Source] Accessed: 13.12.2021)

Subsequently follows the Cloud collaborative tools with the percentage of 9%, the tool widely used among companies ensuring a secure log in as well it is a way of sharing and collaborating computer files using cloud computing, whereby documents are uploaded to a central “cloud” for storage, from where others can access them. These collaboration technologies located in the cloud allow users to upload, annotate, as well as to collaborate on documents and subsequently even modify the document itself to evolve and alter the document for various purposes. A significant amount of companies and corporations have moved to the cloud for collaboration in the recent years. (Yang C., Lan S., Wang L., Shen W., Huang G. G. Q., 2020, pp. 45938-45947)

Position at the last place by the survey voters splitting the tie are the CAD tools with 2%. This was a quite expected result due to the reason that the CAD tools are not commonly mentioned or known as a protective feature. According to the IGI Global, Pennsylvania, USA: “Computer-Aided Design is mostly used as an automated system that implements, creates, designs information technology for performing design functions is an organizational and technical system designed to automate the design process, consisting of personnel and a complex of technical, software, and various aspects of automating its activities.” (IGI Global, 2021, [Online Source] Accessed: 10.12.2021)

2.2.3 Network Access and a Security Guidelines.

The majority of the survey participants, precisely 81%, have access to an online workspace

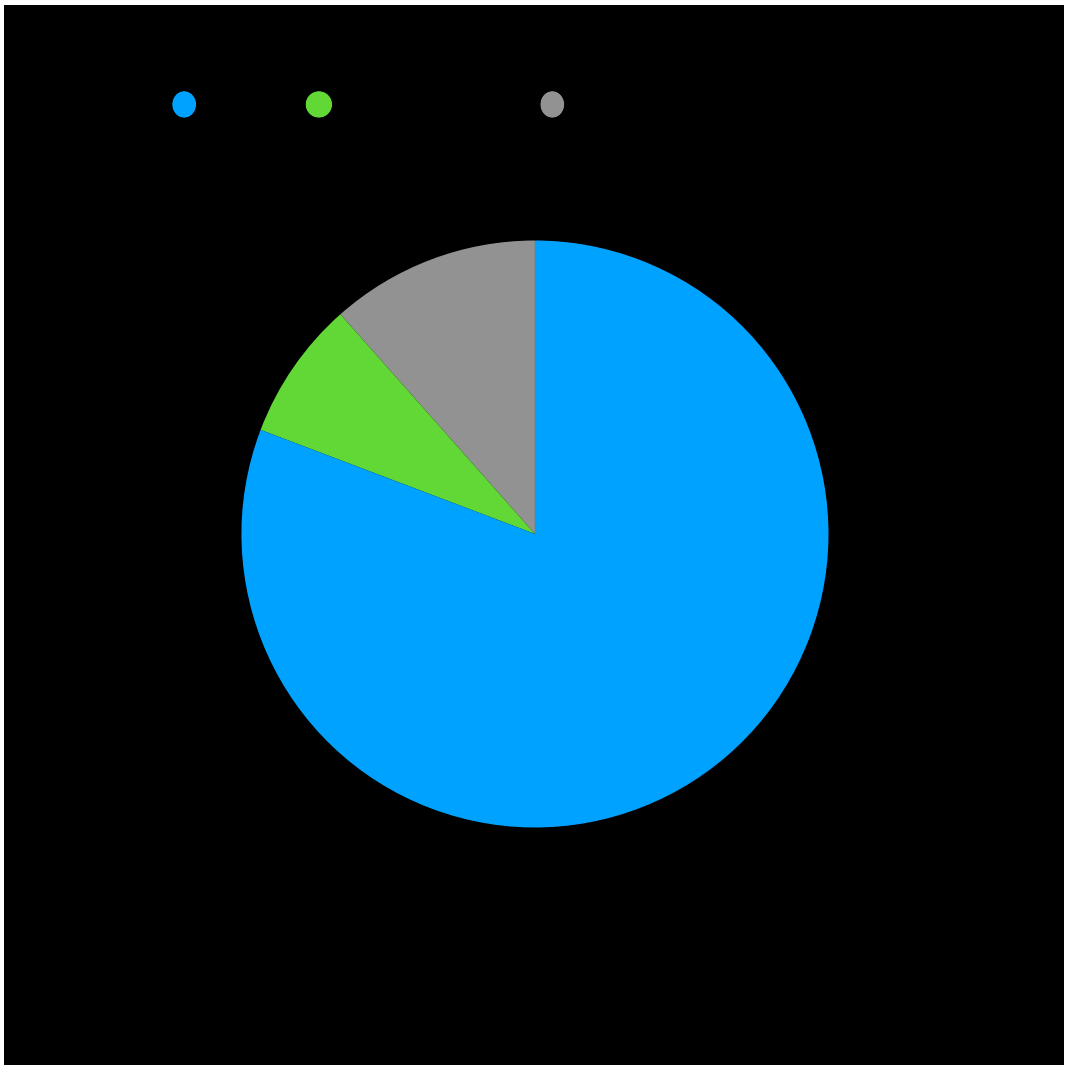

Figure 3. What is the participants security access and security guidelines?

through the VPN; unfortunately, VPNs is quite vulnerable to an attack called website traffic

fingerprinting, which is considered to be a passive intercept attack. (Skowron M., Janice A., Mazurczyk W., 2019, pp. 1-11) Although the adversary, in this case, the hacker, only observes encrypted traffic from the VPN, he can still guess which website is being visited because all websites have specific traffic patterns. (Skowron M., Janice A., Mazurczyk W., 2019, pp. 1-11) As well, the WebRTC technology, which is enabled by default in majority of browsers, makes it possible for a third party to interfere, determine and distinguish the IP address of the current VPN. (Feher B., Sidi L., Shabtai A., Puzis R., Marozas L., 2018, pp. 2-7)

The 12% of survey participants use Third Party Cloud Solution access which is becoming more secure than standard VPN; alongside with the implementation of Zero-Knowledge and Zero trust solutions, cloud computing, SDP, Etherium based solutions, and multiple endpoint protection capabilities.

About 8% of respondents use DirectAccess connections created automatically by the computer for intranet, that is running on a relatively standard alternative version of classical VPN, a new component in Windows operating systems. (Shinder T., 2009)

2.2.4 Experience of Cyber Incidents or Cybercrime since the Start of the Pandemic SARS-Cov-19:

The chart describes the personal encounter of the survey participants with cyber crime incidents. Cyber extortion is an increasingly widespread type of criminal activity of individuals or an organized cybercriminal groups using modern computer tools, equipment, and technologies for the purposes of their illegal activities. As can be observed on the chart, the majority of the participants have experienced cyber incidents since the start of the pandemic; out of twenty-seven respondents, twenty-five had experienced some of the cyberattack, which is in comparison with the following graph regarding the cyber incident experiences prior five years before the pandemic, only fifteen of participants said that they have experienced. Therefore the percentage correlation is 92,59% during the pandemic of SARS-Cov-19 and 55,5% prior to the pandemic, respectively.

The top position in the chart of cyber incidents is divided among the three forms of attacks, Phishing, Computer Viruses and DDoS with 24% of votes each. These types are quite common form of cybersecurity attacks, it is a set of deliberate purposeful set of actions by an intruder, particularly cybercriminal aimed at violating one of the three properties of

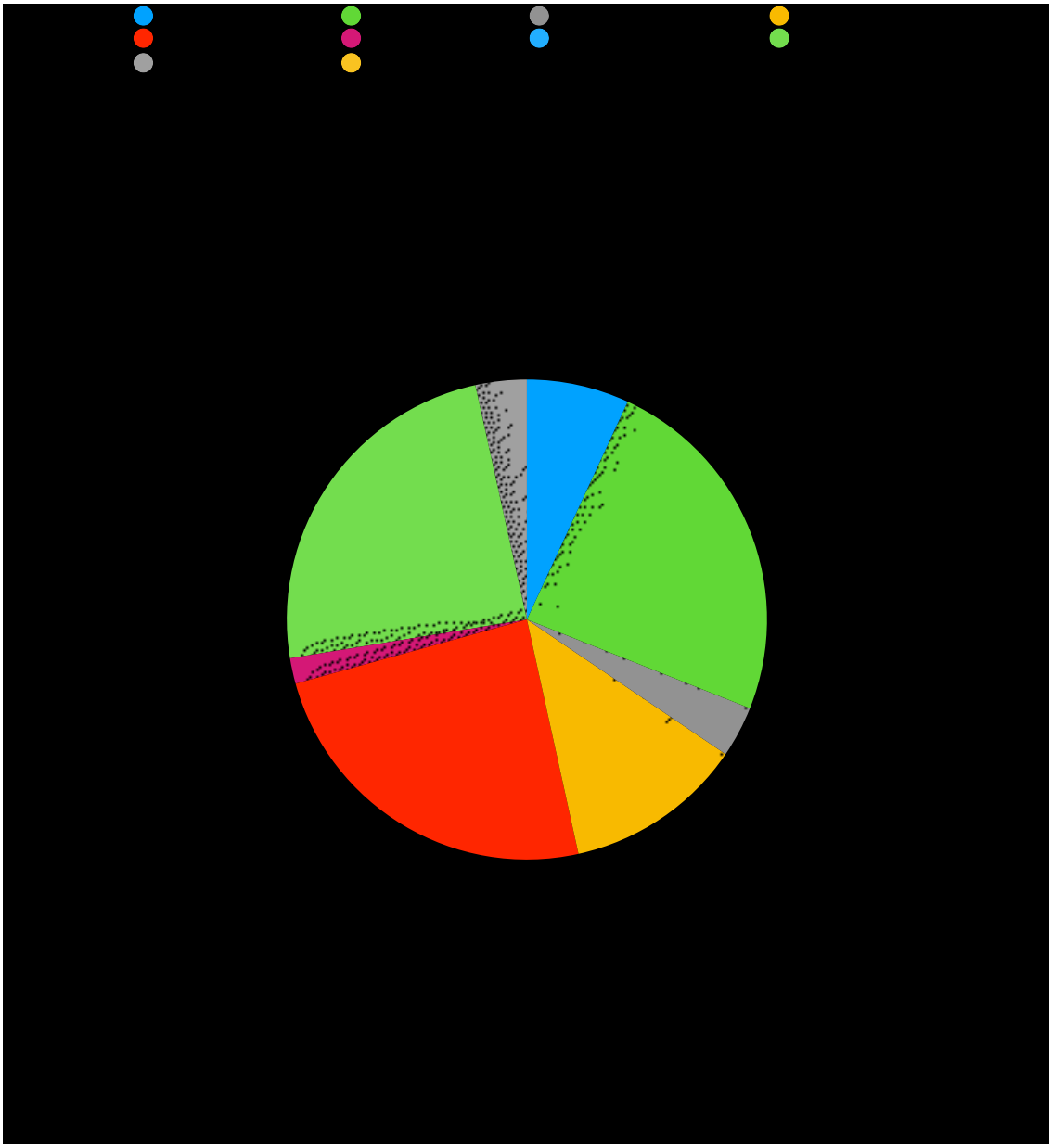

Figure 4. The encounter of Cyber incidents or cybercrime directly by the participants since the start of global pandemic SARS-Cov-19.

information - availability, integrity, or confidentiality, consequently for the purposes of monetary extortion. (Douligeris C., Mitrokotsa A., 2003, pp. 190-193)

In second place with 12% of votes is Ransomware, which is quite interesting that despite time limitations and audience pick limitations, there is still a presence of the voters that have experienced Ransomware.

Following the data theft is 7% of participants have experienced that. Succeding as it goes Identity Theft and Password attacks with 3% each respectively, and closes its the 2% out of chart the MITM Attacks (Man-in-the-middle) a method of compromising a communication

channel; in these particular case an attacker, connects to a channel between counterparties, consequently interfering with the transmission protocol, deleting or distorting information for biased purposes. (Elakrat M. A., Cheon Jung J., 2018, pp. 780-783,)

2.2.5 Prior encounter with the cybercrime before the pandemic outbreak:

The figure below has a purpose of explanative evaluation and compartment of the results with the Figure 3. To assert and analyze the change in cyber crime trends prior to the beginning of the pandemic and time of the pandemic up to the current time.

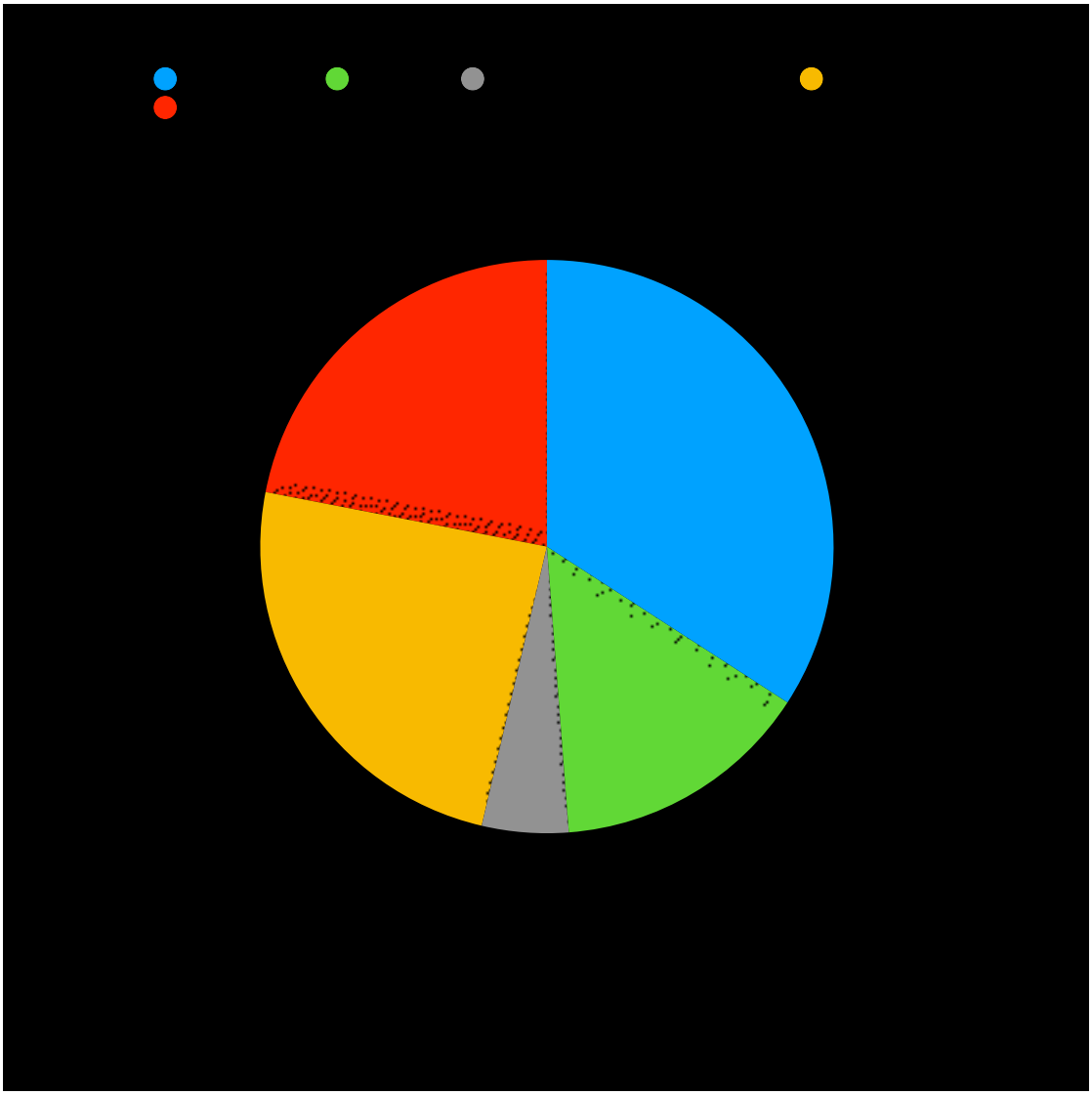

Figure 5. Have any of the respondents ever experienced cyber incidents and cyber-attacks five years primes the beginning of the Global pandemic SARs-Cov-19?

The charts portray the division of cyber incidents that participants of the survey had encountered prior to the pandemic. It can be noted that Phishing was and is one of the most common incidents encountered, with 34%. Following after are DDoS attacks with 24%.

After the 22% of participants have not experienced any cyber security issues in the last five years before the pandemic.

The percentage of malicious virus attacks was relatively lower than during the pandemic; 15% of participants experienced that threat.

The interesting fact is that 5% of participants have encountered Cross-Site scripting prior to the global pandemic and not after. Considering the report provided by HackerOne platform stated that: " Cross-site Scripting (XSS) continues to be the most awarded vulnerability type with US$4.2 million in total bounty awards, up 26% from the previous year." (HackerOne, 2020)

However, the fact should be noted that some many computer security incidents become possible initially through the user's fault, such as the use of outdated software, transition to unknown external resources, and similar failures. (CichonskiP., Millar T., Grance T., Scarfone K., 2012, p. 55-68)

To limit the possibility of the risk of cyberattacks on the security of a computer system, the user should follow the basic cyber security rules; (CichonskiP., Millar T., Grance T., Scarfone K., 2012, pp. 27-36) which are a set of preventive forensic knowledge generated from the analysis of modern cyberattack incidents such as:

1. It is necessary to monitor the relevance of anti-virus programs; (CichonskiP., Millar T., Grance T., Scarfone K., 2012, pp. 27-36)

2. Do not follow external links received from unknown users; (CichonskiP., Millar T., Grance T., Scarfone K., 2012, p. 25)

3. It is necessary to use only licensed software with the ability to update timely. (CichonskiP., Millar T., Grance T., Scarfone K., 2012, pp. 33–40)

4. It is advisable to regularly make backup copies of files to an external medium that is not permanently connected to the computer system; (CichonskiP., Millar T., Grance T., Scarfone K., 2012, pp.68)

5. Electronic media should not be used in unknown devices and vice versa. (CichonskiP., Millar T., Grance T., Scarfone K., 2012, pp. 68)

2.2.5 What is the weakest link in a security of the remote working process:

According to the respondent's assessment, the weakest link of the collaborative remote working process is considered to be the Personal Access Equipment with 48%, such as

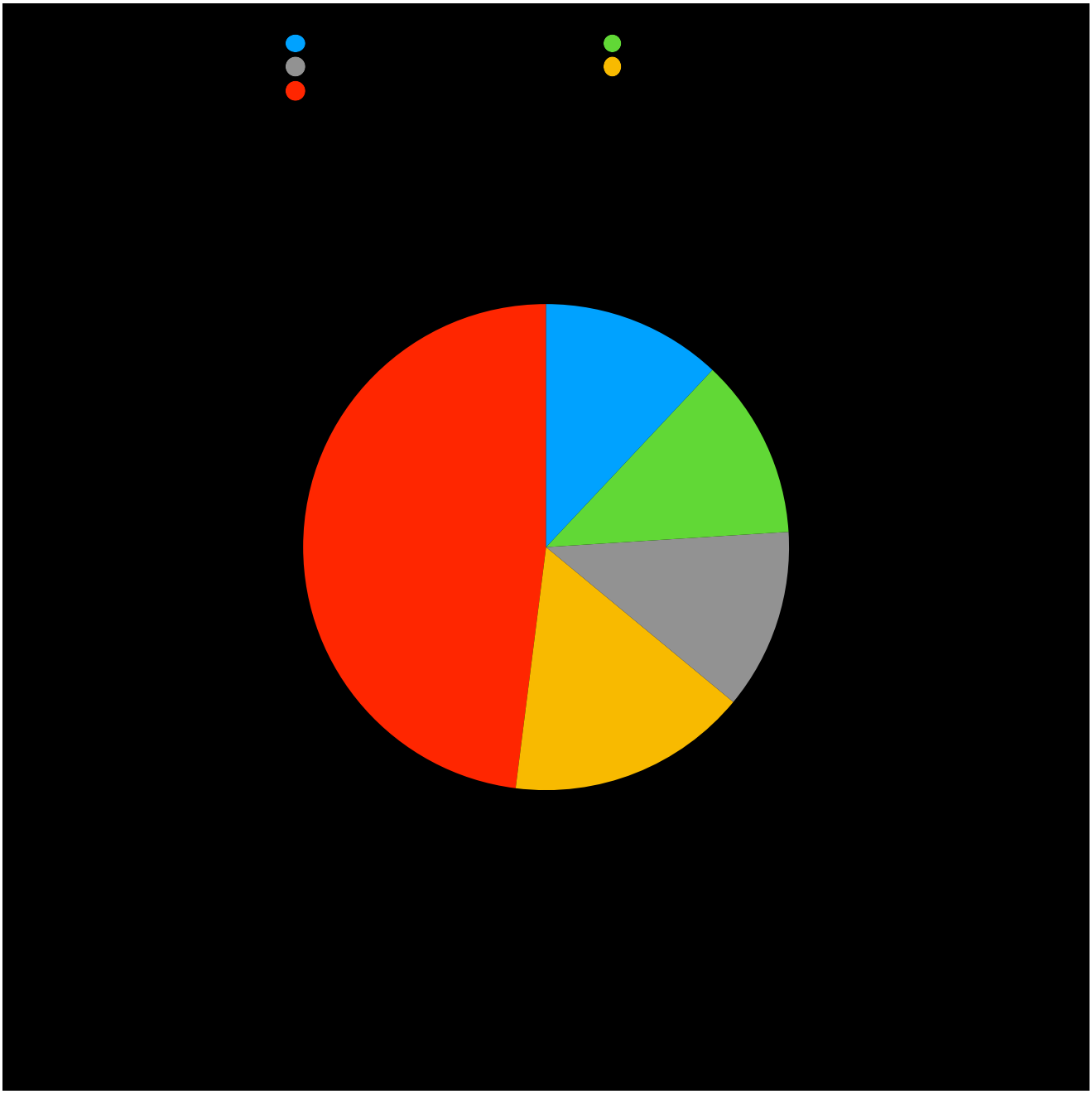

Figure 6. Weakest link in the security of the remote working process.

personal computers, laptops, and other personal devices used for the log-in and access to the online company ecosystems. For the reasons that hackers could easily compromise personal equipment, the valuable information could be accessed through the compromised device, or the companies technology could be damaged, and consequently could affect the networking collaboration and proper function of the company.

The second weakest link in a remote working process according to the respondents is the human error with 16% of total, considering the fact of lack of supervision and overall relatively relaxed atmosphere of remote work there is a higher percentage chance of human error. This could potentially compromise confidential organizational data and information through unintentionally or intentionally leaking important, critical, or confidential information; this is one of the most hazardous threats to an organization in a situation when transferring employees to remote work. (CichonskiP., Millar T., Grance T., Scarfone K., 2012, p. 54)
The unauthorized access, managed service providers and usage of public Wi-Fi each gained 12% of respondents concerns.

2.3.1 Security guidelines provided by the employer regarding the remote working collaboration issues and hazards.

The challenges, possible implications and potential dangers of remote collaboration, are much higher and less secure than corporate networks. Information security risks associated with remote collaborative workspace include interception of passwords and confidential data, data theft as well as hacking of routers, and redirecting users to potentially malicious sites. (CichonskiP., Millar T., Grance T., Scarfone K., 2012, pp. 6, 35-40)
At the same time, attacks using social engineering methods are hazardous. For instance, if an employee made a mistake and got caught, for phishing, other information security systems could hedge him, consequently forward to the phishing training program. (Mimecast Limited, 2021) A entirely different issue is getting access to the corporate network - even if the username and password were lost, access using a remote connection could be limited. (CichonskiP., Millar T., Grance T., Scarfone K., 2012, pp. 6, 35-40)
According to the survey 58% of participants have received some form of regulatory explanation, training or instructions regarding the potential hazardous situations that may appear during the remote working process and how to avoid or cope with that situation.

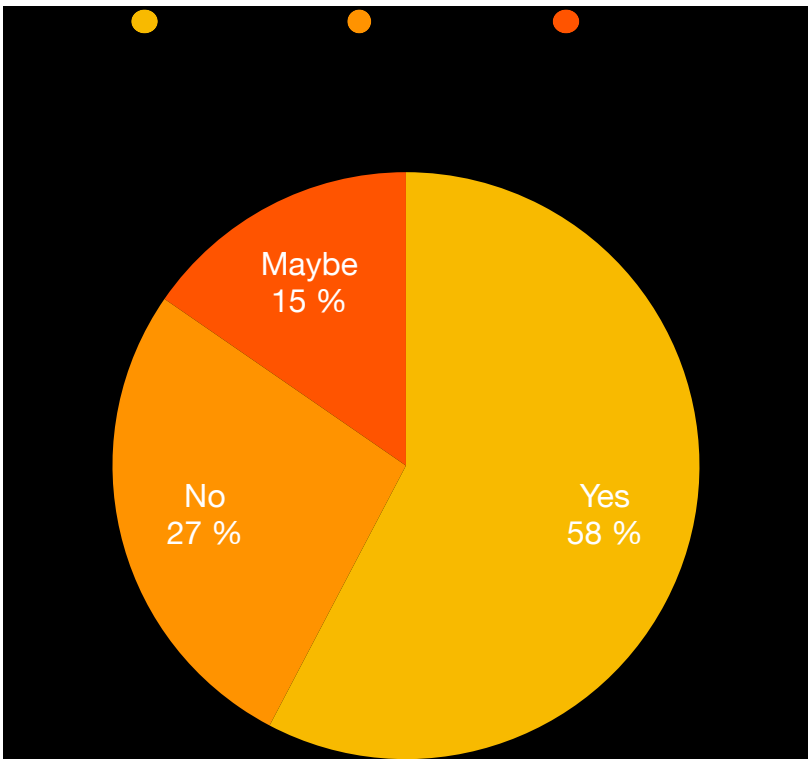

Figure 7. Did participant ever received any security guidelines from your employer regarding remote working potential cyber issues and hazards?

About 27% of participants have not received any specified guidelines regarding the remote working process. And 15% of the participants, to the following question remained unsure whether their organization have provided some form of explanatory procedure at all.
There were a continues increase in attacks exploiting the SARS-Cov-19 theme in 2020. (Angara Technologies Group, 2020) In these particular case, these include double attacks that exploit the coronavirus theme in phishing emails, and banners, and attacks on hospitals and various medical facilities testing or treating coronavirus patients. Attackers actively use email to distribute phishing links and malware in attachments and produced documents. (Angara Technologies Group, 2020) Moreover, their effectiveness is relatively high since users receiving relatively legal looking newsletters regarding the SARS-Cov-19 update or information, and used cannot always recognize something malicious from background purposes. Additionally, the consequential chain reaction is in place, while the number of infected people growing, the range of such threats will also only grow.

From initially technical point of view, remote working and remote users access had become a major issue for companies that have never experienced workeflow in this format before and switched to it in a hurry. One of the primary mistakes the organizations confected that they

did not protect the remote connection channel, configure two-factor authentication, and distribute redundant access to corporate resources. (U.S. Department of State, 2020, pp. 10-15)Therefore, as a result, the traffic of remote sessions could be possibly intercepted by intruders, and employees of the company may potentially and unknowingly provide hacker disposal of confidential data they were not supposed to work with according to their position. (U.S. Department of State, 2020, pp. 10-15)

2.3.2 Prospects of further development in cybersecurity and protection of information in residing company.

For the purposes of scientific curiosity, the question of the awareness of ordinary staff employees was presented in a survey regarding the company's strategic diversification and future direction, upon the company's further development in cybersecurity and ways of protecting vital informational access.

In a point of that, 58% of participants answered affirmatively that the company where they are employed is planning to undergo some strategical cybersecurity changes for securitization purposes.

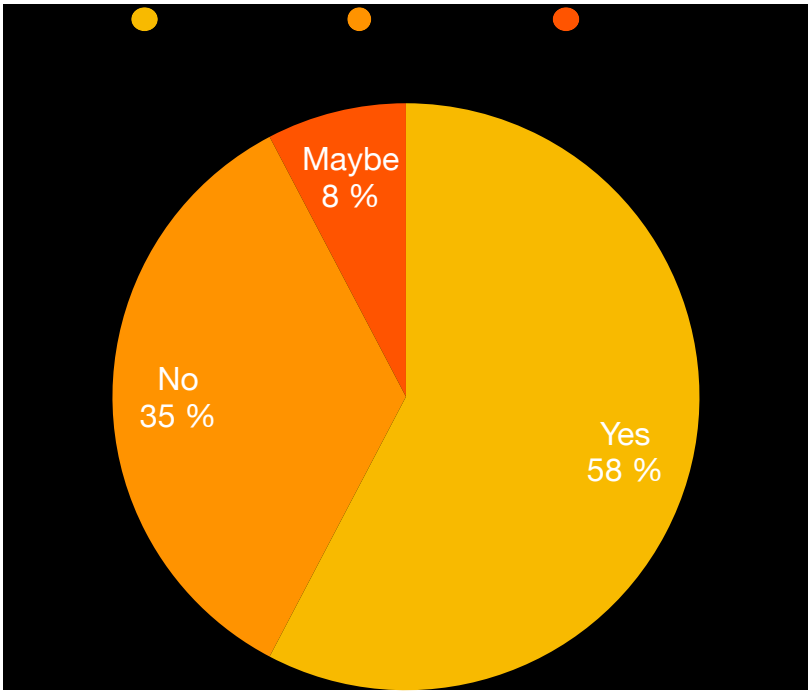

Figure 8. Does your company proceeds with further development in cybersecurity and protection of information?

In the second place, 35% of the respondents answered negatively, which can be interpreted in a way that their employer will not make any additional changes to the structural equity of the company in the nearest future. And lastly 8% of the respondents were not sure regarding the future prospects and development of the corporate protection strategy. Majority of the companies on the market and governmental agencies had to rebuild their systems, processes of operation and communication, exceptionally quickly, and while the security issues, were considered, unfortunately they were not an utmost prioritized. Before the introduction of the self-isolation regime by various governments, some companies did not intend to ever result to using remote access collaboration process their employees. (Malekos Smith Z., Lostri James A. E. Lewis, 2020, pp. 4-5, 7, 12) (Kamal-Chaoui L., Allain-Dupré D., 2021, pp. 14-17)

2.3 Conclusion of the section

Regarding the factorial exponential division in the survey section, the assessment could conclude that overall the survey participants, the global pandemic SARS-Cov-19, directly and indirectly impact a worldwide cybersecurity landscape. From the presence of a direct impact, the exponential increase in phishing through emails spreading the fake news or fake information regarding the SARS-Cov-19 motivates users to follow the links and open emails containing viruses and malicious codes that extort the data from users computers for ransom purposes and monetary extortion purposes. The DDoS XSS attacks have also increased in the year 2020 with the beginning of the pandemic, mainly targeting healthcare and manufacturing industries.

The presence of indirect correlative effects of the global pandemic outbreak generated the governmentally posed restrictions, which has affected business section operational processes; Consequently resulting in massive layoffs of employees and bankruptcies of small businesses. That situational outcome produced a solid flow of Unstructured and Highly structured cyberthreats. From the unstructured threat perspective, people who have lost their jobs resorted to cybercrime for monetary purposes; With the help of the vast availability of tools on the darknet, it is possible to accomplish this to some degree. From the perspective of highly structured cyber threat, government-sponsored cybercrime organizations or company-sponsored cybercrime organizations, due to the weak preparedness of contextual cybersecurity strategies of agencies and businesses while moving to the online working

space, gave an opportunity to infiltrate the systems of the targeted entity structure and leak the confidential and valuable information for personal interest.

Chapter 3: The Implications Posed by Cybersecurity Threats for the Governments

This section of the research project would be revolving around comparative assessment in regards to the research findings and analytical investigation, to ascertain if there is any subject matter for the comparison such as similarities, differences, or unexpected outcomes with the literature review, statistical assessment provided by scholars articles and statistical infrastructure platforms and the personal expectations of the findings.

3.1 The direct correlation of Covid-19 on cybersecurity Issues

According to IBM X-Force Threat Intelligence Index Report 2021, the top three industries targeted by cybercriminals in the year 2020 by attack volume, are the Finance and Insurance that ranked first, on the second place is the industry of Manufacturing, and closing the top three is the industry of Energy. (Singleton C., 2021, pp. 5, 34)

The digitalization simultaneously creates additional risks in supplementing new opportunities; The global pandemic outbreak was catalysis to the online ecosystem, which has also expanded the field for cybercrime and altered its landscape. However, in parallel, cybercrime countermeasures on the part of businesses and the governments began to be more actively discussed and possibly implemented in the nearest future; unfortunately, the legislation passing and technological development and implementation is a time-consuming process. (Gercke M., 2012, pp. 102-106) Looking from the prospects depending on the size of the business organization, presumably it would be much more challenging and problematic to attack large companies that have a higher level of securitization and information protection, hoverer not impossible. However, it would be enough for the small businesses with weak or undeveloped securitization systems to be overpowered by cyberattacks by means of standard email phishing or DDoS.

In accordance with the IBM X-Force thereat Intelligence Index Report 2021, the primary three types of cyberattack in 2020 are (Singleton C., 2021):

1. Ransomeware which constitute 23% of all they cyberattacks and cyber incidents committed and reported in the year of 2020. (Singleton C., 2021, p.7)
2. Data theft compared to the year of 2019 has increased by 160% in the year of 2020. (Singleton C., 2021, p.7)
3. Unauthorized Server Access has increased by 233% in 2020 compared to the year of 2019. (Singleton C., 2021, p.7)

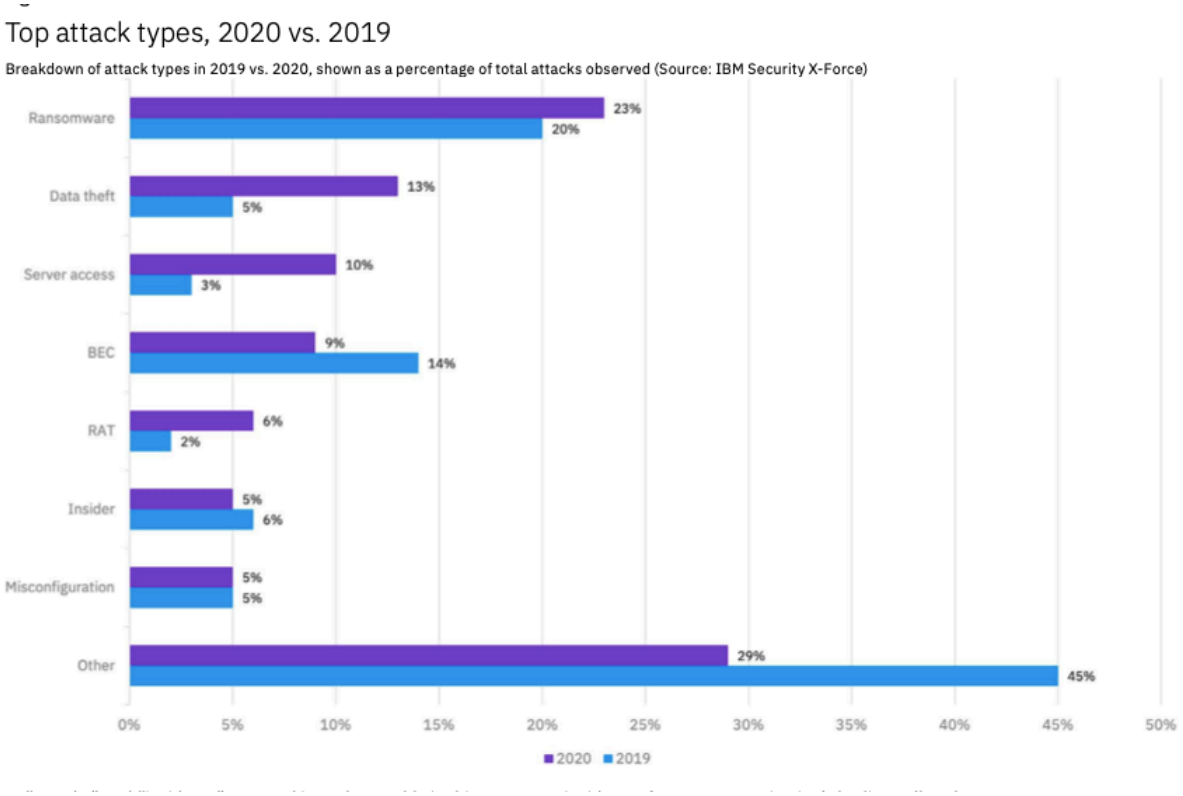

Figure 9. Provided by IBM X-Force thereat Intelligence Index Report 2021, Top Attack Types, 2020 vs. 2019. (Singleton C., 2021, p. 7)

Regarding the vector of the attack there is multiple variations , nevertheless for the year 2020 analysts from IBM have had identified the most collectable by cybercriminals, which are following:

1. Scan-and-exploit which constitute 35% of attacks in 2020. Port scanning is an interlocutory procedure commonly used by cybercriminals to distinguish vulnerable hosts, users for the purposes of a successful attack. (CrowdStrike Falcon, 2021, p. 49) Therefore is does not require much of attentive presence of cybercriminal but at the same time can produce reasonable and desirable outcome. (Singleton C., 2021, p.7)
2. On the second place is phishing with 33% of attacks and slight increase compared to the year of 2019 which was 31%. (Singleton C., 2021, p.7)
3. Credential theft is on the third place in evaluation for the year of 2020, nevertheless it has decreased in percentage, and fall from 29% of attacks in the year of 2019 to 18% in 2020. (Singleton C., 2021, p.7)

According to the statistical analysis, almost 59% of cyberattacks use the double extortion strategy for the purposes of securing their ransom. (Singleton C., 2021, p.8) This strategy assists cybercriminals in the way that if they use the segregate approach, the targeted

organization can opt for the variant to recover the lost data from backups and refuse to render the financial demands. However, with the double extortion strategy, there is a process not only of encrypting potentially sensitive information but also to render it close to impossible to access at all; there is a process of complete exclusion. (Singleton C., 2021, pp. 8, 47) Considering the survey, the respondents have emphasized the fact of the augmentative effects in cyber incidents that they have encountered especially during the time of pandemic.

3.2 Governmental Implications as Consequence of Cyber Threat

Regarding the governmental response toward the augmentation of the potentiality of cyberthreats and the complicate and more elaborative features produced by the attackers on the example of the US, the first component of Cyber Command, the US Air Force Cyber Command, in 2006 was announce the devision formation. (Todd Lopez C., 2006) (Secureworks Inc., 2021, p.18) In 2009 the United States Cyber Command or USCYBERCOM was created. (Nakashima, E., 2016,) In late September 2020 the U.S. cyber Command were participation in a takedown of TrickBot, the malicious ransomeware worm targeting the U.S. healthcare systems and hospitals using a trojan malware Ryuk. (Secureworks Inc., 2021, p.18)

Currently, due to the fact that ransomware has drastically increased worldwide and skyrocketed in the U.S. in the year 2020 compared to the year 2019; (BitSight Statistics, 2020, pp. 2-6) the Ransomeware Disclosure Act was introduced on October fifth by U.S. Senator Elizabeth Warren (D-Mass.) currently in pending. (Ross E., Warren D., 2021) The bill mandates the organizations and individuals who have been subjected to the cyberattack and paid the ransom to disclose all the information regarding that action and specifies the process within forty-eight hours from the completion of ransom payment. Such as in what currency payment was processed, the amount of ransom demanded, and any critically valuable information regarding the entity demanding the ransom. (Ross E., Warren D., 2021) The other bill that is in pending is Cyber Incidents Reporting Act, according to homeland Security this bill (Congress.gov, 2021): “The Cyber Incident Reporting Act would require critical infrastructure owners and operators to report to CISA within 72 hours if they are experiencing a substantial cyber-attack.”(Congress.gov, 2021) This bill means that entities that operates in critical infrastructure would be mandated to disclose the critical information regarding cybersecurity breaches, leaking or incidents in regards of cybersecurity to the

Cyber Incident Review Office. This legislation is on the subject of the business entities with more than 50 employees. (Congress.gov, 2021)

The interesting case would be Italian experience in organizing cybersecurity which positions in using American model of cyber command. Network Operations Command (Comando per le Operazioni in Rete, COR), since 2020 after the merge with Comando C4 Difesa it was renamed to Joint Cybernetic Operations Command is the joint military unit was created in 2017, the activities of this unit are carried out in the field of cyber security for the purposes of network securitization. (De Tomas Colatin S., 2020, pp. 18-19)

The initial purpose of the organization is to statically dynamic security monitoring and preventive measures for the purposes of the integrity of the network as well the accessibility of information, which is carried out conjointly with other structural units of the military department. Secondly, the unit carries out the examination and statistical assessment and evaluation of the vulnerabilities in cyber networking systems, ensuring rapid preventive measures in case of cyber incidents and minimizing the onset of negative consequences. (De Tomas Colatin S., 2020, pp. 9-10)

Conjoint and incorporated into the military sector, the cybersecurity structure of the Italian Republic ensures the proper supervision and maintenance of military operations and helps at the organizational, technical level, as well acts as a coordinating body between the Italian armed forces and other organizations cybersecurity communities. (De Tomas Colatin S., 2020, pp. 12-17)

3.3 Inactivity of Governments in Response

Overall, the majority of the governments around the world possess some variation of the cybersecurity unit within the governmental disposition; nevertheless, it is not at the capacity to uphold to the development threat of cybercriminal issues. The primary issue at hand is an absence of unified liquidity across the judicial systems around the world. Therefore means that if the cybercriminal operates from the country with no relatively stalled present law regarding the unlawful actions of cybercrime, such as ransomware, extortion, phishing, targeting the countries with the possession of some form of the law regarding this actions, there is no prosecution for the committed actions, and no extradition possible for the criminal. As by the country's law, the entity operates with no existence of evidence that the actions committed are unlawful.

Furthermore, it becomes more complicated with an absence of traction and advanced levels of securing the footprints to trail the connectivity and relations of criminals. Countries adopting the units of cyber force on a governmental level incorporate the cyber activities into the strategical applicability of hybrid warfare and tactical targeted espionage; Nevertheless, denying any direct connection or level of acquaintance toward the active cyber group, operating under the aegis of the cybercrime according to the international standardized systems and perception.

According to the McKinsey evaluative research based on the Global Cybersecurity Index (GCI) rank provided by The International Telecommunication Union and Network Readiness Index (NRI) rank of Portulans Institute, they have established primary factors of successful success governmental cybersecurity strategies. (Global Cyber Strategies Index , 2019) (Fadia A., Nayfeh M., Noble J., 2020, pp. 4-8) (Dutta S., Lanvin B., 2019, pp. 237-250) According to the CSIS Global Cyber strategy Index, 78 countries around the world have a stable National Cybersecurity strategy implemented, guiding the responses to cyber threats; and 113 countries have Privacy strategies, which govern and regulate the handling of personal data. Furthermore, 91 countries of the total have crime cyber security policies and strategies regarding legislation for cybercrime. (Global Cyber Strategies Index , 2019) (Fadia A., Nayfeh M., Noble J., 2020, pp. 4-8) (Dutta S., Lanvin B., 2019, pp. 237-250)

Mckinsey provided a principle elements for the success of a comprehensive national cybersecurity strategy, which consist of five:

- National Infrastructure Protection program, which should identify critical infrastructures for the country's economic and national stability, prioritizes critical cybersecurity and protection sectors. Most commonly, national critical infrastructures are a primary target to distrust stability in the country and consequently economy and society of a nation. (Fadia A., Nayfeh M., Noble J., 2020, pp. 4-5)
- National Incidents Response and Recovery plan should be incorporated. Unfortunately, cyberattacks are inevitable, therefore in case of disruptive consequences of cyber attack, to minimize the drastic effects, provide assistance to the victims, and recover a stable environment as soon as possible. (Fadia A., Nayfeh M., Noble J., 2020, pp. 4-5)
- Specific National Cybersecurity Agency is primarily responsible for the agenda and structure of national cybersecurity strategy. (Fadia A., Nayfeh M., Noble J., 2020, pp. 4-5)

- Definitive laws the cybercrime should be present for preventive purposes, as well the assistance in the investigation process and affirmative action process to counterfeiter cybercrime. (Fadia A., Nayfeh M., Noble J., 2020, pp. 4-5)
- Cybersecurity ecosystem to enable cybersecurity processes at the national level. (Fadia A., Nayfeh M., Noble J., 2020, pp. 4-5)

3.4 Alteration of Cybercrime Landscape

With time passing, every part of humanly incorporated tools has undergone drastic changes for the purposes of adaptation of convenience, as well as the strategical decision-making process. The cybercrime landscape changed from two side perceptual levels; first, the cybercriminal activities, tools of application adaptation, and multilayered threats practice; the second side of the coin is the perception of cyberthreats by all others on the different side of the issues, such as individuals, corporations, and governmental structures. (Singleton C., 2021, pp. 22-24) (Marsh & Microsoft, 2019, pp. 2-4)

The dynamic transfer of employees to remote workspace and the withdrawal of internal services of companies to the network perimeter, caused by the COVID-19 pandemic, has dramatically impacted the cyber threat and cybercrime landscape around the world. (Marsh & Microsoft, 2019, pp. 2-4) An only a limited number of companies that had already practiced remote work mode were at some point prepared to cope with all the difficulties and issues in ensuring security integration into their strategy; The rest of the agencies and companies were faced with a lack of time to adapt and implement all the necessary preventive protection measures. (International Labour Organization, 2020, pp. 1-8, 19-23)

The cybercrime landscape was changing steadily according to the changes in cybersecurity adaptations to bypass the discovered ways of protective tools. However, when the global pandemic stroked, the majority of those who were on the protective side, the companies on the market, governmental structures, and individuals, were not technologically ready for the online premises and new communicative ways; Consequently, the structural implications of inability arose. From the technological perspective, cyber criminals got the upper hand in various possibilities, unstructured unprotected technologies, the inability of potential targets to promptly adapt to the alternative landscape of existence and communication, the credence of human nature. In regards to the credence of human nature, cybercriminals exploit the different tactics; for instance, in the Czech Republic currently the state of alert in the banking systems. (Československá obchodní banka, (ČSOB), 2021) The scheme is quite simple the

criminals make a call on an individual phone and present themselves as an employee of the bank, saying that for the individual account, the loan has been approved, patently the person denies the claim, and then the extortionist asks for the information clarification regarding the account holder, therefore acquiring information necessary for the hack. As well the phishing emails coming under the name of banks. (Uni Credit Bank Czech Republic, 2021) (Československá obchodní banka, (ČSOB), 2021) There were similar cases in Russia, and the criminals even created cross-site and cross-call scripting, which interferes and intercepts the calls and web presence, directing them to the biased website or entity. (Landson G., 2021) (MFC A network of multifunctional centers of the Rostov region, 2021)
Another trend in 2020 is the growth of markets that sells access information to companies' servers. Nowadays, even if hackers are not able to advance their planned attack beyond the vulnerability they found in the company's protective structure and gain access to the server, they could promptly sell that access on the dark-web forum. (Secureworks Inc., 2021, p. 15) It is notable due to the fact that not only the IT structure of the company can suffer, but also companies representation and reputation. (Secureworks Inc., 2021, p. 15)

Potential Prognosis on the base of analysis

Despite the rapidly developing circumstantial adaptation of governmental structures and aspiration for the enchantment of securitization systems, it is still a vague perspective for the secure and stable cyber ecosystem environment. At the same tase cybercriminals evolve and relentlessly develop more enhanced potential cyberthreats. The massive amount of cyber tools available on the vast amplitude of cyber biogueocenosis, the relative anonymity and arduous to track across IPA, lack of relative fluidity across jurisdiction systems around the world provide an exceptional surface for cybercrime to flourish.

It is virtually near too impracticable to eliminate cybercrime, as with offline crime completely; however, it is possible to limit and constrain it to some extent. The only logically possible outcome for the successful limitation of cybercrime would be to establish a multi-party collaboration among governmental sphere and legislation sphere on multiple county levels, the analyze and share knowledge and data acquired, to create a unified legislative system of laws among all the participants in regards specifically to cybercrime and cybercriminals. For enhancement of securitization of this multiple parties collaboration, the principle of zero knowledge and zero trust should be applied. The communication could occur as offline same online on structurally encrypted ledgers, spring only necessary

cryptographically coded information with the particular key with the principles of Rotation/ Caesar Cipher, changing the shift value simultaneously with each coding encryption and decryption.

Chapter 4: Discussion of International Effects and Modifications of Cybersecurity Landscape

4.1 Modification of Cybersecurity landscape

The cybersecurity landscape has undergone drastic modifications and alterations over the last decade. According to Matthew Chang, the Chief Information Security offices at Goldman Sachs, one of the main game-changing alterations in cybersecurity defense posture over the last ten years is the willingness and openness to the information sharing among public and private sectors; according to his mention ten years ago the majority of the sectors perceived cybersecurity and cyber defense field as a competitive edge among rivals. Nevertheless, with the rapidly changing field of cybercrime, the new adaptation of a multidisciplinary approach, and multilayered high profile attacks, there comes a realization that a single body in public or private sector is unable to stand to uphold without additional assistance. As well as the implications posed by the fact that some counties implement the approach of cyber attacks as a part of the hybrid warfare strategy for the purposes of espionage and gathering the information, as well as attenuation of opponents with compromise information on a global arena. Therefore, the information sharing in regards to experiences, the development of defense mechanisms, professional expertise and various countermeasure tactics is not the display of superiority but rather a necessity for those of string common goal protection and securitization of assets and assertion of the further development.

With the more complicate cyber threats

4.2 Direct Chain Impact of Covid-19 on Cybersecurity Issues and Cybercrime

The linkage between the global pandemic of SARSCov-19 and the boost in cybercriminal activity over the past two years is impeccable, and it is portrayed by a chain reaction of the supportive consequential implication. To pursue and further assess the linkages and codependent correlation of the sub-sequential compound, and ongoing governmental respond it would be wise to separate the step-by-step reaction.

Firstly, the pandemic outburst provokes governmental structure to strengthen the control over the population in the form of governmental restriction on movement, the number of people who can communicate in a closed environment, and the time frame limitation for businesses operation.

Secondly, all the above consequently resulted in massive downsizing on the workforce, especially those who were involved in the service industry. For the purposes of clarification, this paper provides an assumptive path of development. According to the statistic of Digest of Education Statistics 2019, in the year 2018, 43% of full-time students and 81% of part-time students were combining education and employment. Considering the fact of the lost financial support, it poses quite a challenge to support the lifestyle, therefore after the fact that unemployment rates are skyrocketing in many countries and demand exceeds the supply of job offers, there is a chance that some unemployed individuals would turn to some extreme measures such as cybercrime cyber fraud. Considering the fact that the world unemployment rate in the year 2020 skyrocketed by 1.1% from 5.37% to 6.47%, this is the most prominent indicator for the last thirty years. North America's unemployment rate jumped by 4.45% from 3.89% to 8.44%.

4.3 Lack of Fluidity Across Jurisdiction Around the World

We are currently facing a lack of fluidity across the judicial system worldwide, which means there is no unified conceptive perception of the cybersecurity field as a whole. The standardization of minimization and lack of responsible bodies that could behold accounted for the issues arising, the absence of the unified intellection in regards toward the securitization. This is all paraphernalia of one side of the coin; if it could be put that way, these are the subjects that interfere with the concept of complete cyber securitization. The cause of this lack of unity is the human behavioral factor, as ludicrous as it sounds, the human perception of the world around them and the constant evolutionary perspective. The fact is that human beings are not initially designed to cooperate. From the psychologically and physiological perspective, the primary driver factors of human behavior as according to Maslow’s hierarchy of needs, the most basic one starts at the bottom are the physiological needs such as a craving for food and shelter, protection from the predators that could diminish the lineage and posterity, and at the top are the needs of self-realization and aesthetic needs. This concept could be viewed from two perspectives; firstly, the middle class living in the developed and developing countries could be viewed somewhere in the middle of the hierarchy of needs, with the possibility of self-realization. Secondly, from the globalized point of view, the human behavioral patterns are directly dependent on the psychological evaluation and sustainable emotional outcome affected by the hormonal emphasis of a superlative effect. The fact of uncertainty of actions of others plays the major

role in the decision making process, different possibilities of outcome produce different behavioral patterns. There is not a single country in the world, with an exception of Vatican, that have never been at war, whether for the resources, religious beliefs, or the supremacy and power. The alliances formed with the preventive purposes to strengthen the possibilities and provide

4.4 Recommendations

The recommendations regarding the future possibilities of securitization of cyberspace could be divided into two subgroups. The first group would be explanatory for the internal prospects within separate states, and the second would aim for the global international prospects of securitization of cyberspace.

Domestic prospects of cybersecurity and reliability protective measures for separate states:

1. Prioritization of Vital Infrastructures for the states should be an utmost priority; the majority of governmental efforts should be aligned to protect these infrastructures.
2. Increase the investment in cybersecurity development.
3. Creation of Cybersecurity National Strategy.
4. It would be beneficial for the government to incorporate or conjoin governmental cybersecurity units with military structures.

Global international recommendation and prospects for securitization of cyberspace:

1. It is vital to create an independent structural committee for the practical assessment of cyber incidents.
2. Should be created some form of unitized international legislation.
3. Enhance the multi parties collaborative and communicative processes for the purposes of gathering knowledge, data, information, and shred experience

4.5 Suggestions for Further Research

This section provides suggestions on further areas of research that could be followed:

1. What could possibly be incorporated by cybercriminals as a next step of the evolution, based on the current development of cybersecurity technologies such as Zero Trust, SDP?
2. What could different new strategies be incorporated by cybercriminals?
3. Investigation of behavioral patterns employed by attackers.

The further area of research would provide more sophisticated results on future prospects of the development and modifications in the landscape of cybercrime and cybersecurity, and will allow to prioritize the possible solution for preventive measures.

Conclusion

Due to the fact that the majority of organizations and governmental structures were not adequately prepared and overall ready for this chain of event reaction caused by pandemic SARS-Cov-19, the transitional period of adaptation took much longer than it supposedly should be; it is still an ongoing process. From the perspective of organizational preparedness, the majority of the companies on the market have experienced an unexpected crash. From the perspective of division, only the global corporations operating worldwide were more or less prepared for the unexpected situational development. Unfortunately, middle-sized companies and smaller-sized companies were not at all prepared for the unfortunate series of events that the global pandemic SARS-Cov-19 has brought. Consequentially, according to the Yelp data gathered, approximately 60% of the business that closed due to the coronavirus pandemic are permanent, which means that they will not reopen in the future. (Sundaram A., 2020) US civilian labor force participation rates have dropped by 1.8% or 4.7 million participants. (U.S. Department of Labor, 2021) The major issues encountered on the way of the transitional period are:

- Technological extemporaneous of securitization. The employers transfer to a remote working space without any or limited guidelines for the work transition, the ways and tools they should incorporate to protect the data and information in a cyber environment. Significant number of the companies did not possess any protective tools at all.
- Massive lay offs. Due to the governmental lockdowns to prevent the spread of the disease, many businesses lost the ability to operate; even though the governments provided monetary support, the small and middle-range businesses could not withhold all of the remaining staff.
- Additional increase of cyberattacks and cyber incidents on middle segment and small segment businesses.
- The monetary issues encountered during the transitional period were due to the panic behavioral patterns observed in the population. The fact of uncertainty and lack of any information regarding the prospects of the situation prompted many people to withhold from additional unnecessary spending.

The majority of operating companies and governmental structures have transitioned to the online environment, with no proper functioning technological background, therefore the field

of cybercrime have ranged wide. Coping up with gradual development of cybersecurity development the cybercrime have adopted a new tactics and strategies, mixing up and enchanting already existing cyber tools. The different type of hackers aiming at different targeted groups without their range, within the three types of cyberthreats:

- Unstructured cyber threats target and exploit document or system vulnerabilities, primarily aiming at individuals and small businesses for extortionist purposes. Hackers usually exploit the widely available cyber tools from the Dark Net, which are easily traceable. Governmental restrictions and isolation have left many people unemployed and forced to look for new sources of income.
- Structured cyber threats are coming from a structured well cyber trained group of individuals, targeting the individuals within the organization or the organization itself as well a massive ransomware campaigns such as Big-Game-Hunt.
- Highly Structured Cyber Threats is an extensive organization with highly structured strategy and considerable fundings at their disposal, using a long-term purposeful attack for obtaining the information. Most commonly supported by a big corporation for the purposes of industrial espionage or the governmental structure for espionage. Such as in the case of the 2020 United States federal government data breach, or SUNBURST Malware Supply Chain Attack 2020, the malware was leaking private information for nine months before it was discovered.

Most feasible the hackers will maintain a strategy of double blackmail continue to demand separate ransoms for data recovery and non-disclosure of that information, and double extortion ransomware strategy when the attackers exfiltrate the private information and then encrypt files on a device, so the victims could not access the files.

Currently, at this stage of the global geopolitical situation, the most feasible changes in the intra-state domestic level modification in cybersecurity legislative and legal perspective pan out in the United States with the significant development perspective in the technological field of protective cybersecurity systems and proffered Bills on protective features such as Ransomeware Disclosure Act and Cyber Incidents Reporting Act. The US is actively engaging in the development and debates for the prospects of securitization of cyberspace. Regarding the international situation on cybercrime, there are prospects for further integration in collaboration regarding that issue; nevertheless, it is pretty challenging and time-consuming to create another internationally recognized and accepted international body for governing cybersecurity and cybercrime issues. Nevertheless, there is a possibility that if

the cybercrime growth continues at that pace of evolvement exponentially, that the would-be created some forms of temporary international collaborative structure for battling the effects of that, under such structures as the UN or NATO. Consequentially, depending on the performance of that unit/structure, the presence of that body may become permanent and would eventually be incorporated into the central figure framework.

Bibliography

Scholarly Articles:

Aite Group LLC, Giact Refinitiv Company, 2021, U.S. Identity Theft: The Stark Reality, Boston, MA 02110

Ali Khan N., Nawaz Broh S., Zaman N., 2020, Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic, TechRxiv Powered by IEEE

Boyatzis, Richard, 1998, Transforming qualitative information: Thematic analysis and code development. Thousand Oaks, CA: Sage

BUIL-GIL, D, Kemp, S, Miro-Llinares, M, Castano, N, 2020, Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK, European Societies, Published Online

Cisco Secure Systhems inc, 2021, Cybersecurity Series of reports: Defending against critical threats, California, Cisco Systhems

Crodstrike Holdings, Inc, 2021, 2021 Global Threat Report, Crodstrike Holdings, Inc

Chin Eian I, Ka Yong L, Yeap Xiao Li M., et al., 2020, Cyber Attacks in the Era of Covid-19 and Possible Solution Domains, Preprints

Douligeris C., Mitrokotsa A., 2003, "DDoS attacks and defense mechanisms: a classification," Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No.03EX795), pp. 190-193, doi: 10.1109/ISSPIT.2003.1341092.

Edelman Serge, Herley Cormac, Oorschot Paul C., 2013, Markets for zero-day exploits: ethics and implications, NSPW '13: New Security Paradigms Workshop, Canada

Elgar Edward , Edited by: Enderlein Henrik , Wälti Sonja , Zürn Michael, 2010, Handbook on Multi-level Governance, Edward Elgar Publishing Limited, Glos, United Kingdom

Feurer, R. and Chaharbaghi, K. 1994, "Defining Competitiveness: A Holistic Approach", Management Decision, Vol. 32 No. 2

Federal Bureau of Investigation Internet Crime Complaint Center, 2020, Internet Crime report 2020, Washington, D.C., FBI National Press Office

Gostev A. A., 2017, GLOBAL PSYCHOMANIPULATION; Psychological and Moral Aspects, Institute of Psychology RAS, Moscow

Grossman J., Fogie S., Hansen R., Rager A., D. Petkov P., 2007, XSS Attacs; Cross-Site Scripting Exploits and Defense, Amoretto Pedersen, United States

Inglehart Ronald, Welzel Christian, 2002, New Directions in Comparative Politics, Routledge, New York, Third Edition, ISBN 9780429494932

HAWDON, J.; PARTI, K.; DEARDEN, T. E. (2020). Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment.

Jenkinson A., 2021, Stuxnet to Sunburst; 20 Years of Digital Exploitation and Cyber Warfare, Boca Raton, CRC Press, 1st Edition

Khan N.A., Brohi S.N, Zaman N., 2020, Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic, TechRxiv Powered by IEEEl, DOI: 10.36227/techrxiv.12278792.v1

Lamont C., 2015, Research Methods in International Relations, Sage Publications Ltd, London

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: a timeline and analysis of

cyber-crime and cyber-attacks during the pandemic. Computers and Security, Volume 105, [102248]. https://doi.org/10.1016/j.cose.2021.102248

Mamchur E. A., 2010, EPISTEMOLOGY YESTERDAY AND TODAY, Russian Academy of Sciences Institute of Philosophy, IP RAS, ISBN 978-5-9540-0180

Orcher L. T., 2017, Conducting a Survey; Techniques for a Term Project, Routledge, Taylor & Francis Group, London and New York, ISBN-13: 978-1-884-58572-2

PricewaterhouseCoopers, PwC network, 2020, Fighting fraud: A Never-Ending Battle; Global Economic Crime and Fraud Survey, PwC network, p. 4

Resor, Williams C., 2017, Exploring Vacation and Etiquette Themes in Social Studies, Primary Source Inquiry for Middle and High School. Maryland: Rowman & Littlefield Publishers. pp. 10–11. ISBN 978-1-4758-3198-6.

Secureworks Inc., 2021, Counter Threat Unit; State of the Threat A Year in Review, Secureworks Inc., Report access through original page.

Singleton C., 2021, X-Force Threat Intelligence Index 2021, IBM Corporation, IBM Security, United States of America

Turner, C,B, Turner, C, Shen Y, 2020, Cybersecurity Concerns & Teleworking in the COVID Era: A Socio Cybersecurity Analysis of Organizational Behavior, Journal of Advanced Research in Social Sciences, Virginia, USA

Thomas J., Harden A., 2008, Methods for the thematic synthesis of qualitative research in systematic reviews, BMC Med Res Method, [Online Source] doi: 10.1186/1471-2288-8-45

Weber C. 2014, International Relations Theory: A critical Introduction, Routledge, Taylor & Francis Group, London and New York, ISBN 9780415713061

Wiarda Howard J., Graham Lawrence S. , 2002, New Directions in Comparative Politics, Routledge, New York, Third Edition, ISBN 9780429494932

U.S. Department of Labor, 2021, News Release: UNEMPLOYMENT INSURANCE WEEKLY CLAIMS, Employment and Training Administration Washington, D.C. 20210, Release Number: USDL 21-2198-NAT

Online Sources:

Buxton D., 2020, The Internet Governance Forum, Transparency, and Stalkerware, Kaspersky Daily, United Kingdom, [Online Source] Accessed: 15.10.2021 https://www.kaspersky.com/blog/internet-governance-forum/37837/

Bossler, A. M.; Berenblum T., 2019, "Introduction: new directions in cybercrime research". Journal of Crime and Justice. 42 (5): 495–499. doi:10.1080/0735648X.2019.1692426. ISSN 0735-648X.

Caramani Daniele, 2017, Comparative Politics, Oxford University Press, United Kingdom, Fourth Edition, pp. 21-29 [Accessed online] Accessed: 01.11.2021 https://books.google.cz/books?id=mgJLDgAAQBAJ&printsec=frontcover#v=onepage&q&f=false

Cohen, Zachary; Salama, Vivian; Fung, Bria, 2020, "US officials scramble to deal with suspected Russian hack of government agencies". CNN. [Online Source] Accessed: 12.11.2021 https://edition.cnn.com/2020/12/14/politics/us-agencies-hack-solar-wind-russia/index.html

Cybriant Computer&Network Security Management, 2018, Types of Network Security Threats and How to Combat Them, [Online Source] Accessed: 23.10.2021 https://cybriant.medium.com/types-of-network-security-threats-and-how-to-combat-them-b6624428b152

DeepInstinct, Center for Strategic & International Studies (CSIS), 2021, Mid-Year Threat Landscape Report, [Online Source] Accessed: 02.11.2020 https://www.deepinstinct.com/news/cyber-threat-report-on-2020-shows-triple-digit-increases-across-all-malware-types

DiFate, V., 2007, "Evidence". Internet Encyclopedia of Philosophy. Johns Hopkins University, U.S.A., [Online Source] Accessed: 25.10.2021 https://iep.utm.edu/evidence/

Dilanian, Ken (December 18, 2020). "Suspected Russian hack: Was it an epic cyber attack or spy operation?". NBC News. [Online Source] Accessed: 10.11.2021 https://www.nbcnews.com/news/us-news/suspected-russian-hack-was-it-epic-cyber-attack-or-spy-n1251766

Government of Canada, 2020, CSE Statement on Threat Activity Targeting COVID-19 Vaccine Development, Communication Security Establishment, [Online source] Accesses: 12.10.2021 https://cse-cst.gc.ca/en/information-and-resources/news/cse-statement-threat-activity-targeting-covid-19-vaccine-development

Gordon, S., Ford, R. 2006, On the definition and classification of cybercrime. J Comput Virol 2, 13–20 https://doi.org/10.1007/s11416-006-0015-z

Humayun, M., Niazi, M., Jhanjhi, N. et al., 2020, Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arab J Sci Eng (2020). https://doi.org/10.1007/s13369-019-04319-2 Humayun, M., Niazi, M., Jhanjhi, N. et al., 2020, Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arab J Sci Eng (2020). https://doi.org/10.1007/s13369-019-04319-2

Internet Telecommunication Union, 2021, 2.9 billion people still offline
New data from ITU suggest ‘COVID connectivity boost’ – but world’s poorest being left far behind, Unite Nations ITU, Geneva, [Online Source] Accessed: 30.11.2021 https://www.itu.int/en/mediacentre/Pages/PR-2021-11-29-FactsFigures.aspx

Kaspersky Lab., 2018, What Is an Advanced Persistent Threat (APT)?, Kaspersky Lab., [Online Source] Accessed: 25.10.2021 https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Kelly, Thomas, 2016 "Evidence". The Stanford Encyclopedia of Philosophy. Metaphysics Research Lab, Stanford University. [Online Source] Accessed: 25.10.2021 https://plato.stanford.edu/entries/evidence/

Kantchev G., P. W. Strobel 2021 "How Russia's 'Info Warrior' Hackers Let Kremlin Play Geopolitics on the Cheap". Wall Street Journal. ISSN 0099-9660. [Online Source] Accessed: 05.11.2021 https://www.wsj.com/articles/how-russias-info-warrior-hackers-let-kremlin-play-geopolitics-on-the-cheap-11609592401

Markoff J., 2009, Weakness in Social Security Numbers Is Found, The New York Times, [Online Source] Accessed: 07.11.2021

Nakashima E., Timberg C., 2020, “Russian government hackers are behind a broad espionage campaign that has compromised U.S. Agencies, Including Treasury and Commerce.” The Washington Post, [Online Source] Accessed: 12.12.2021 https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html

PricewaterhouseCoopers, PwC network, 2020, Fighting fraud: A Never-Ending Battle; Global Economic Crime and Fraud Survey, PwC network, [Online Source] Accessed: 14.12.2021 https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

Reddy L., Internet Governance Forum, 2020 High level Leaders Track Security, UN Internet Governance Forum, [Online Source: Speech], Accessed: 20.10.2021 https://www.intgovforum.org/vIGF/

Sanger, D. E., Perlroth, N., Schmitt, E., 2020, "Scope of Russian Hack Becomes Clear: Multiple U.S. Agencies Were Hit". The New York Times. [Online Source] Accessed:

03.11.2021 https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html

Social Security Bulletin, Vol. 70, No. 3, 2010, [Online source] Accessed: 23.10.2021 https://www.ssa.gov/policy/docs/ssb/v70n3/index.html

Sundaram A., 2020, Yelp data shows 60% of business closures due to the coronavirus pandemic are now permanent, NBCUniversal News Group, CNBC, United States, [Online Source] Accessed: 17.12.2021 https://www.cnbc.com/2020/09/16/yelp-data-shows-60percent-of-business-closures-due-to-the-coronavirus-pandemic-are-now-permanent.html

The United States Social Security Administration, Puckett C., 2010, Administering Social Security: Challenges Yesterday and Today, [Online source] Accessed: 26.10.2021 https://www.ssa.gov/policy/docs/ssb/v70n3/v70n3p27.html

The Guardian Labs , 2020, What we know – and still don't – about the worst-ever US government cyber-attack, The Guardian, [Online Source], Accessed: 15.10.2021 https://www.theguardian.com/technology/2020/dec/18/orion-hack-solarwinds-explainer-us-government

United Nation Internet Governance Forum, 2020, High Level Leaders Track: Security, United Nation, [Online source] Accessed: 15.10.2021 https://www.intgovforum.org/vIGF/

UK National Cyber Security Centre, 2020, News: UK and allies expose Russian attacks on coronavirus vaccine development, [Online source], Accessed:12.10.2021 https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development

List of appendices

Appendix 1: Dissertation Project Proposal

Faculty of social Sciences Charles University of Prague, Master in International security Systems
Master thesis propsal

The proposed title of the thesis:

Impact of COVID 19 on Security Policies of States in the Area of Cyber Security. The impact of Covid-19 on cybersecurity in an organizational contextual level of governmental, national defense, and security policies; distinction on the role of AI in the development of cybersecurity comprehensive autonomous preventive attack systems.

Characteristic of the topic and brief review of current related research:

The researchers intend to relate to the following topic of the world pandemic outbreak of SARS- CoV-19 global impact on cybersecurity's structural, organizational context in governmental, national defense systems, and security policies. The analysis would revolve around the mediating role of artificial intelligence in the development of comprehensive and autonomous cybersecurity systems at the governmental level. The analysis would take an approach following the constructivism and neoliberalism theoretical construct.

The research question that the student intends to address in the thesis:

The research question would follow the theoretical constant of the practical approach; consequently, the posed research question would be as following: In what way did the global pandemic outbreak, directly and indirectly, affect cybersecurity at a globalized governmental level? What is the potential for the future evolution of cybercrime, and what may future potential threats be?

New: What is the layer leveled impact of the global pandemic outbreak of SARSCovid-19 on generic cybersecurity? What are the potential chain effect prospects in the field of cybersecurity and the evolution of cybercrime? What are the possibilities of future advancement of cybercrime threats in light of current cybersecurity measures?

Outline of the proposed line of argument:

The potential threat to the governmental and intergovernmental international relationship stability poses one of the utmost prioritized levels of concern. In the age of purposeful development of Artificial Intelligence, prime of cybernated societal structure, and active intelligence, the dormant neoteric menace, as cyber threat poses notorious magnitude of substantiality and colossal essentiality of preventive measure capacity.

The outbreak of the world pandemic of SARS-CoV-19 has brought the inevitable instability in well- organized societal world structures, on the level of eradicating the stability itself as it was before. The erratic future perspective and the dread of upcoming unknown prospects compulsed various social structures to eradicate the known methods in favor of the one that displays more stable future outcomes; it gave the boost for cybersecurity potential threats and cybercrime. The situation itself was long gone from being perfect even before the pandemic outbreak, the various financial instabilities, potential war outburst, societal structural diversity; the SARS-CoV-19 could be perceived as the catalysis for the boost of cybercrime and potentiality as the next step in the evolution in the cybersecurity field and Active Artificial intelligence itself.

As an instance, on May 7th, 2021, the most extensive pipeline system in the US for refined oil products, Colonial Pipeline, was subjected to a cyberattack by ransomware gang, hitting only business IT department network, extortionists ultimately received from the Colonial 75 Bitcoin which equivalent approximately $4.4 million.

According to the independent research Aite Group, approximately 47% of US citizens in the year 2020 were subdued to financial identity theft. As an ultimate direct impact of the pandemic, consequently resulting in boost and increase of unemployment rate.

Therefore the potential for comprehensive analysis in the field of cybersecurity is immense and presents an extreme prioritization level for the structural well-being of the liberal societal framework.

The following argument will be focusing on two directions. The theoretical perspective will be narrowed down regarding whether the pandemic correlates in an increase of cyber-attacks directly due to the move into online services for the majority of correlative societal communications and collaboration.

The methodological focus of the research will be correlating towards directing the compound between the potential target of dormant cyber threats of private companies and organizations

and its direct relations on the governmental stability and comprehensive preventive measure capacity of the state itself.

Appendix 2: List of Survey Questions

Data work statement:Data gathered by means of this survey will be employed only for the purposes of the master's dissertation and will be anonymized. The information obtained will not be provided to the third party and will be stored for the duration of the assessment and investigation.

Survey Assessment: Correlation of SARSCovid-19 and Cybercrime Governmental Respond

1. What is the age of the participant?
2. What is the occupation sector of the participant?
3. Did you receive any security guidelines from your employer regarding working from home?
4. If the previous answer is "Yes" can you elaborate regarding the examples?
5. What types of technology have being implemented to assure the remote working process secure?
6. What is your network access and security policy?
7. Are the access devices provided and managed by your organization?
8. Has your company adopted a specific collaboration solution?
9. Have you experienced personal encounter with cyber incidents and cybercrime?
10. Did you face any of the below cyber-security related threats during the COVID-19 crisis?
11. Have you faced any cyber-threats in the last five years before the pandemic?
12. What in your opinion the weakest link in security of remote working?
13. What is more preferable workspace for you?
14. Does the government apply some preventive measures to counterforce cybercrime in your country?
15. Does your company proceeds with further development in cybersecurity and protection of information? (Such as adaptation of SDP and Zero Trust Solution Principles)
16. Which solutions is your company planning to undertake for the purposes of securitization?
17. What tools do you personally use to protect your private time on the Internet?