CORONAVIRUS PANDEMIC – LEVERAGE FOR CYBERCRIME

Daniel Dumitru[1] and Tiberiu Ion[2]
[1) 2)] *Carol I National Defence University, Bucharest, Romania*
E-mail: dumitru.daniel@unap.ro; E-mail: ion.tiberiu@unap.ro

Please cite this paper as:

Dumitru, D. and Ion, T., 2020. Coronavirus Pandemic – Leverage for Cybercrime. In: R. Pamfilie, V. Dinu, L. Tăchiciu, D. Pleșea, C. Vasiliu eds. *6th BASIQ International Conference on New Trends in Sustainable Business and Consumption.* Messina, Italy, 4-6 June 2020. Bucharest: ASE, pp. 1211-1217

Abstract
The global Coronavirus pandemic has not only a social impact, by causing infections and deaths, but it has also shaped the economy at a global scale, having the potential to close entire cities or regions by installing quarantine, bankrupt small or unsustainable business, rise to commercial shortage certain industries, while causing a dramatic fall for others.
The current paper illustrates how the coronavirus pandemic influenced different sectors causing the transition of certain activities to the virtual space. Cyberspace is not immune to these fast changes: public and private organization are now being forced to implement remote working solution for their employee. In this sense, the internet usage has increased exponentially. Thus, understanding the impact of the online transition and analysing the potential threats and their causes, is a crucial task for organisations in order to not be vulnerable to cyberattacks. As more and more users, with no basic knowledge in cyberdefence, are using public networks to pass sensitive information, cybersecurity has become more important than ever. Therefore, the current research outlines a set of cyber due diligence and cyber due care strategies that represent good practices for organisations in the context of crises.

Keywords
Global crises, digital policies, cyberattacks, due diligence, due care

JEL Classification:
F02, F60, O21, O33

Introduction

Global crisis, from climate change to the global war on terror, from world poverty to humanitarian disasters, represent the dark side of the globalised planet, and, increasingly, prompt awareness of our civilizational community of fate (Cottle, 2009). The outbreak of COVID-19 has determined a major shift for the modern society, trends like social distancing or self-isolation being recommended and in certain cases imposed. In an attempt to identify and understand the turmoil effect that the pandemic has on the society and all its main sectors and industries, the current paper tries to summarize how the impact –

response relationship evolved during the first months of this crises and how did this crises impact cyberspace and cybersecurity for both public and private organizations.
The aim of this paper is to better understand how a four pillar model based on cyber due diligence and cyber due care strategies can help end users represented by teleworkers to protect the information that they disseminate, using cyberspace channels. By implementing these recommendations, each organization can take an extra step in adjusting the negative economic effects of the pandemic. Nevertheless, these good practices can be also learned and adapted for certain daily activities of each individual, as normal life as we know will slowly migrate to the online environment and will be hosted in a space with no boundaries.

1. Analysing the social impact of Coronavirus crisis and the response of public and private sectors

The year 2020 has begun with a crisis situation, caused by the Coronavirus pandemic, that raised a series of challenges for the entire world. Excepting Antarctica, the pandemic has affected all social and economic sectors on all continents. Governments are racing to stop or to slow down the spread of the virus by any means necessary. Much of the world's states have declared state of emergency, imposing a series of strict measures like closing schools, banning congregations, limiting traveling or social activities or even placing quarantine restrictions/isolation at home for citizens.
The rapid spread of COVID-19, the coronavirus disease, has also a major political impact, raising old tensions between nations and raising the risk of security threats. From an economical point of view, major economic powers like the United States of America (USA) or China are becoming less significant as international trade is slowing down, while the European Union is facing a major economic lockdown for some of its strongest members. In this context, it can be said that the globalisation process has reached a standstill.
In the coming months the world is expecting to see changes in the way society will operate and how will the normal life look like. As governments and businesses around the world tell those with symptoms to self-quarantine and everyone else to practice social distancing, remote work is our new reality (Neeley, 2020).
Governments have also a major role in limiting as much as possible the social impact of this crisis, especially by taking the necessary actions in order to assure critical supplies and prioritise vital resources for the population. This means economic measures that can include export limitation for certain products, price-cap regulations, unemployment policies. Furthermore, the effect of *panic buying* is creating shortages in the logistic chains for goods of strict necessity (food, water, personal hygiene products etc.)
On the other hand, if certain categories of good are impacted by high demands, a powerful contraction in demand is registered for industrial production and construction (Laing, 2020).
Thus, the pandemic has caused dramatic falls in the prices of a wide range of products, for example metals and construction materials, even stock market shares. According to the World Economic Forum, the world stock market has dropped up to 40% by the end of March 2020, this evolution having a negative impact of multiple big companies (Figure no. 1).

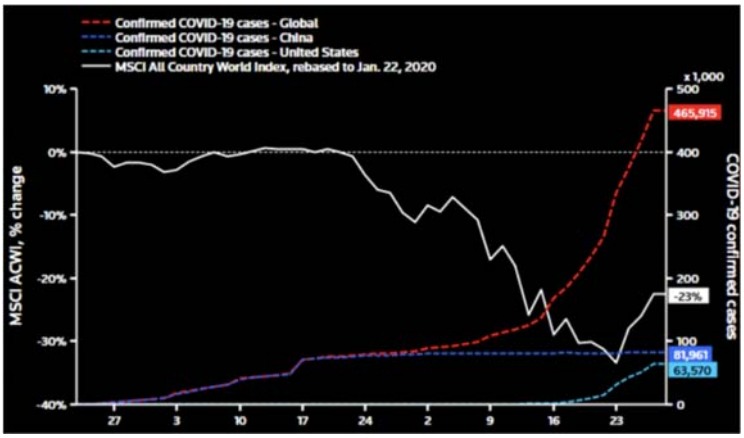

Fig. no. 1 World stock market vs COVID-19 confirmed cases
Source: World Economic Forum, https://www.weforum.org/agenda/2020/03/take-five-quarter-life-crisis/

Moreover, social distancing and isolation have blocked main public sector activities that are directly related with the companies and organizations and their economic activity. Thus, in the context of social distancing, the need to implement and deploy digital technologies is rapidly growing, as the chain reaction public - private – population has determined a significant reduction in demand of goods and services across March and April 2020.
But switching to online is not an easy task and it cannot be achieved in a very short period of time. Also, the lack of specialized human resources in information technology represents a challenge for this transition. Governments must act and create partnerships between private technology companies, international organizations and other social entrepreneurs in order to facilitate the online migration of ministries, public accreditation bodies or other institutions which carry out important activities for the society.
For example, digital technologies, as artificial intelligence software, can be helpful in the healthcare services, by improving emergency communications when their capacity is outpaced, or in overcoming language barriers. Based on multiple economic analyses, The Department of Economic and Social Affairs from the United Nations (UN) has developed a model that illustrates a digital government policy response to Covid-19 (Figure no. 2).

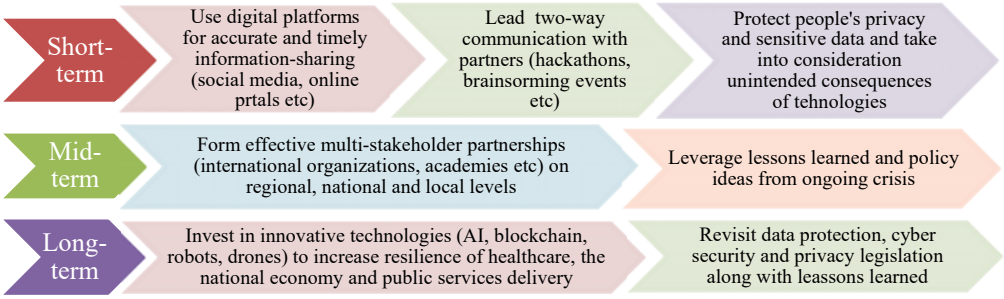

Fig. no. 2 Digital Government Policy Response to Covid-19
Source: adapted after United Nations, 2020

Public-private partnerships will be reshaped during this pandemic crisis. There is now an opportunity to revaluate and redesign the term *normal*, in order to streamline processes,

actions and maximize the added value of the results. During this crisis, Apple and Google (Apple, 2020) announced a collaboration that involves a common investment of their resources (capital, human, know-how) in order to find a technical solution that can help governments and health agencies to reduce the spread of the virus. The two multinational technology companies are working to provide a cross-platform of application programming interfaces (API) that application developers can use in order to implement contact localization and tracing.

Also, other big companies are trying to assist the public sector in fighting the crises (Atlassian, 2020): CenturyLink, provides high-speed internet to temporary hospitals around US; HP provides 3D printing technology for COVID-19 face shields, face masks, wrists covers; Facebook is allocating funds towards fact-checking of information, in order to avoid the spread of misinformation. Other big corporations announced donations in IT infrastructure in order to facilitate remote education (Amazon, 2020). Furthermore, as of March 30, more than 6.000 contributors have provided support to more than 3.000 COVID-19 response projects worldwide. Most of these projects are hosted on GitHub, a Git repository hosting service.

Thus, the positive response of both big companies and small businesses in offering support to the governments has once more demonstrated that the public sector and international organizations will not overcome this crisis alone. In this sense, social responsibility and ethics will bring businesses one step forward in adapting to the society that will follow post COVID-19 pandemic. Nevertheless, digitalization together with related products and services will become a necessity for the public and private sectors around the world.

2. The need of digitalization in the context of Cybercrime: prevention and good practices

As countries and organizations stand together in facing the new challenges determined by the coronavirus crisis, another threat is escalading with the need of transition to online, and that is the cybersecurity threat. The same cyberthreats or hacking strategies can be tracked prior to this crisis, but in the last month an increase in social engineering targeting was registered, by leveraging vulnerabilities caused by the present crisis.

Social engineering is an incredibly effective process of attack with more than 80% of cyber-attacks, and over 70% of those from -nation-states, being initiated and executed by exploiting humans rather than computer or network security flaws (Erbschloe, 2020).

In order to assure social distancing and prevent the spread of the virus, governments and companies have established measures to isolate its workforce and to offer technical solutions to accomplish their tasks remotely. In this context, the use of the internet and social media applications have increased exponentially.

Home internet access does not always ensure a secure connection and can determine network vulnerabilities, that can be easily used by cyber perpetrators in order to get access to sensible data. Moreover, these technical vulnerabilities are increased by the consequences that people are facing because of the coronavirus pandemic and their constant search for information on the subject, that has been widespread on the social media. This causes people to take fast actions on social media applications, in cases they otherwise might have been circumspect.

Society has heightened the dependency for information technology and individuals whom were not technical by formation, are now forced to adapt and embrace this new technique of communication, without any advising in cyber security knowledge. In this context, cyberattacks will target both individuals and organisations, as teleworkers will facilitate a direct connection to their employers' systems.

All of these factors can cause an increase in the number of attempts of cyber criminals. Taking the advantage of the current crisis, cyberattacks can even cause the closure of an hospital. According to Europol (2020), the Czech Republic reported a cyberattack on Brno University Hospital which forced the hospital to shut down its entire IT network, postpone urgent surgical

interventions and re-route new acute patients to a nearby hospital. According to Europol, in the first months of the current crises.

According to the Center for Internet Security (2020), a non-profit organization that leads communities for enabling an environment of trust in cyberspace, starting with the beginning of the current crisis, an increase in following specific types of attacks has been registered:

- phishing and malspam,
- credential stuffing,
- ransomware,
- remote desktop protocol (RDP) targeting,
- distributed denial of service (DDoS) attacks.

Thus, in order to prevent attacks, organizations must adopt a comprehensive strategy based on cyber due diligence and cyber due modules, that must be further implemented by the end user, in this case the teleworker. These modules represent a set of good practices that can help both organizations and employees to better adapt to the transition towards the online or remote environment. In this sense, a model has been outlined (Figure no. 3), based on all 4 main strategies that must be adopted by an organization - due diligence of the organization, due care of the organization, due diligence of the end user, due care of the end user. The model contains a collection of one of the most important and best applied good practices, hat have been correlated in a logical way.

Education represent the starting point for preventing, or in the worst case, correcting all security problems. Companies must organise cybersecurity courses for all employees, in order to teach them the basic knowledge regarding cyberspace and threats. The actual situation represents an alarm trigger for the organizations that did not consider cybersecurity as a resource in defending the company's online environment.

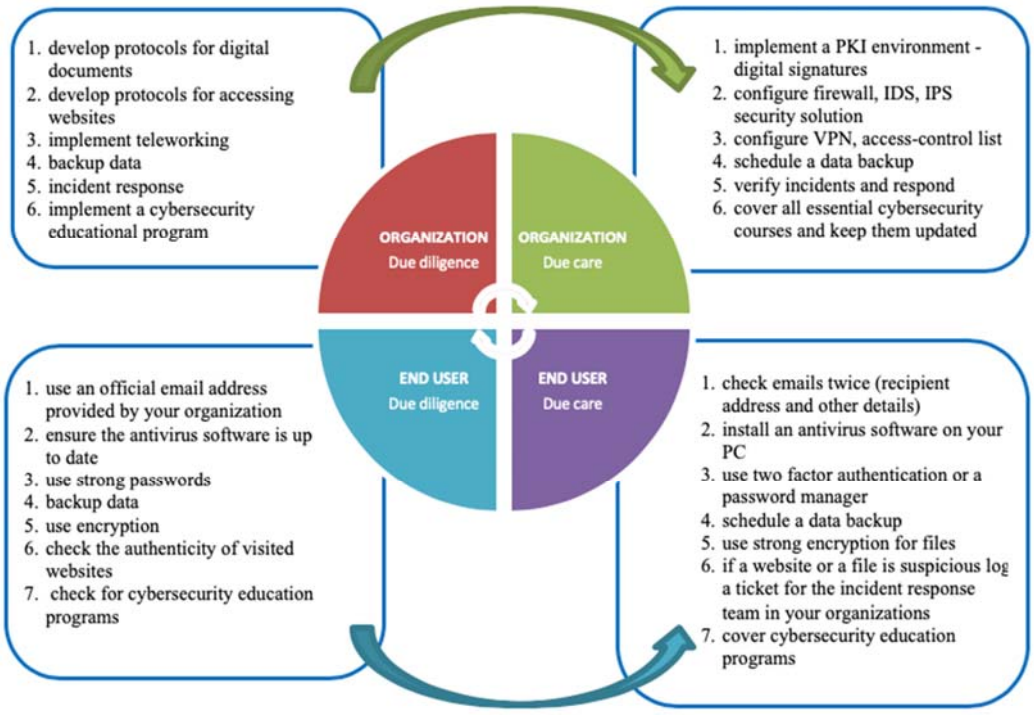

Fig. no. 3 Good practices in the context of crises: modeling cyber due diligence and cyber due care strategies

Source: author research

Thus, according to the above model, in order to provide the most extensive coverage through cybersecurity specialists, organisations must offer cyber due diligence and cyber due care modules to help assess and address information security risks. The main outcome is that a company will implement information technology solutions and that employees will have the necessary resources to use. In this sense, active and proactive technologies (for example: Virtual Private Network – VPN, Intrusion Detection System – IDS Intrusion Prevention System – IPS, PKI – Public Key Infrastructure) will be used by teleworkers in order to maintain network security.
Moreover, public and private organizations should adapt to the dynamic evolution of the information technology and its increasing dependency by creating a special structure of cybersecurity specialists. With the help of these specialists, organizations can develop security policies for preventing the leak of sensitive information or cyberattacks. Employees will also have an important role in maintaining a secure online environment by respecting the due diligence and due care strategies.

Conclusions

The current Covid-19 crises could become the most significant economic, political and social event to characterize the twenty first century. Actions and measures that are trending at a global level have already shaped the global economy, increasing or decreasing the demand in different sector and industries, causing logistic shortages and long-term implications for the post-pandemic society. Fear of a new recession caused by an increasing unemployment level, by falling wages, or fail of measures that might be placed to help the economy can determine a general state of panic and uncertainty, corroborated with the transition to online of multiple business or individual activities, creates a fair environment that can facilitate the occurrence of cyberattacks, as an social and economic consequence of the Covid-19 pandemic.
Analysing the social impact of the Coronavirus crisis and the response of public and private sectors is a crucial step for governments, organisations and academia in order to understand future trends and implications for communities and countries.
In short term, in order to promote social distancing for avoiding the spared o the virus, most governments, organisations, companies and even the individual must transition to the online environment. This transition calls for caution and awareness from all involved parties as remote work being a new reality, brings a number of risks for both the organisation (whether public or private) and the end user.
In this sense, cyber due diligence and cyber due care models are one of the best practices that organisations can implement. The current model shows the basic steps that an organisation and its end users must follow in order to maintain a safe online environment. The four pillar model is resilient and calls for ensuring basic knowledge of cybersecurity and cyberspace regardless the domain that the organisation actives in (healthcare, business, production, constructions, government or social activities).

References

Amazon.com, 2020. Amazon donates 8,200 laptops to Seattle Public Schools families, [blog] *Amazon's COVID-19 blog Prioritizing health and safety Our Positions Available* at: <https://blog.aboutamazon.com/community/amazon-donates-8-200-laptops-to-seattle-public-schools-families> [Accessed 08 April 2020].

Apple Inc., 2020. *Press release - Apple and Google partner on COVID-19 contact tracing technology*, [online] Available at: <https://www.apple.com/ro/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/> [Accessed 14 April 2020].

Atlassian Corporation Plc., 2020. *How private-sector tech companies are stepping up to the COVID-19 fight,* [online] Available at:

<https://www.atlassian.com/blog/technology/private-sector-tech-companies-covid-19-fight> [Accessed 16 April 2020].

Center for Internet Security, 2020. *Resource Guide for Cybersecurity During the COVID-19 Pandemic,* [online] Available at: <https://www.cisecurity.org/blog/resource-guide-for-cybersecurity-during-the-covid-19-pandemic/> [Accessed 16 March 2020].

Cottle, S., 2009. *Global crises reporting.* RefineCatch Limited: Suffolk.

Erbschloe, M., 2020. *Social Engineering Hacking Systems, Nations, and Societies*. CRC Press.

Europol, 2020. *How criminals profit from the Covid-19 pandemic*, [online] Available at: <https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic> [Accessed 30 March 2020].

Laing, T., 2020. The economic impact of the Coronavirus 2019 (Covid-2019): Implications for the mining industry. *The Extractive Industries and Society*, S2214790X2030126X.

Neeley, T., 2020. *Managing your remote team*. Harvard Business School Publishing Corporation.

United Nations, 2020. *UN/DESA Policy Brief #61: COVID-19: Embracing digital government during the pandemic and beyond*, [online] Available at: <https://www.un.org/development/desa/dpad/publication/un-desa-policy-brief-61-covid-19-embracing-digital-government-during-the-pandemic-and-beyond/> [Accessed 02 April 2020].

World Economic Forum, 2020. *Five charts that show the global economic impact of coronavirus*, [online] Available at: <https://www.weforum.org/agenda/2020/03/take-five-quarter-life-crisis/> [Accessed 10 March 2020].