# Cyber Security Reactivity in Crisis Times and Critical Infrastructures

**Conference Paper** · November 2020

DOI: 10.1109/ICSTCC50638.2020.9259695



**4 authors:**

Mircea Constantin Scheau
University of Craiova
**27** PUBLICATIONS **6** CITATIONS
SEE PROFILE

Viorel Gaftea
Romanian Academy
**24** PUBLICATIONS **26** CITATIONS
SEE PROFILE

Achim Monica-Violeta
Babeş-Bolyai University
**78** PUBLICATIONS **312** CITATIONS
SEE PROFILE

Corina Narcisa Bodescu
**2** PUBLICATIONS **0** CITATIONS
SEE PROFILE

# Cyber Security Reactivity in Crisis Times and Critical Infrastructures

Mircea Constantin Șcheau
Faculty of Automation, Computers and Electronics
University of Craiova
Craiova, Romania
mircea.scheau@edu.ucv.ro

Viorel Nicolae Gaftea
Dept. of Science and Information Technology
Romanian Academy
Bucharest, Romania
viorel.gaftea@acad.ro

Monica Violeta Achim
Faculty of Economics and Business Administration
Babeș-Bolyai University
Cluj-Napoca, Romania
monica.achim@econ.ubbcluj.ro

Corina-Narcisa (Bodescu) Cotoc
Faculty of Economics and Business Administration
Babeș-Bolyai University
Cluj-Napoca, Romania
narcisa_bodescu@yahoo.com

***Abstract*—Technological and social developments lead to repositioning of criminal actions and adapted responses of Information Systems. On the invisible front, confrontations between national or international organizations and entities that are strictly economically motivated or supported by terrorist groups take place. The direct and indirect effects are difficult to predict due to the high degree of uncertainty of the phenomenon as a whole. The mobility of the relevant factors is quite high and that is why the algorithms use probabilistic models. The losses are quantified as a post factum effect of the events. The present study aims to present Data Mining and Analysis of possible impact that can be felt, starting from a review of actions against official institutions, transformations that occur in crises and finally, a set of proposals in support of alignment with common international standards**.

***Keywords*— cybernetics, analysis of variance, dark market, data mining, infrastructures, vulnerabilities, crisis, impact**

## I. INTRODUCTION

If we refer strictly to the economic aspect, cyber-attacks focused on strategic objectives can generate considerable profit, higher than those launched on random objectives, the redemption requests being directly proportional to the potential damages that can be caused. In separate quadrants the actions supported by state actors or very strong multinational companies are placed. The target in this second case is not necessarily focused on capital transfers or immediate material gains, but rather on disrupting the business, taking control or compromising access to current and backup information. Requests to pay fees for the recovery of encrypted data sometimes hide the real intentions, especially since there is no guarantee in any way of returning to the original state or the fact that data recorded before encryption will not be capitalized on the black market. Criminal actions are encouraged and last but not least supported by payment decisions that lead directly or indirectly to the financing of those groups, provided that the refusal may lead to a partial or total loss of resources. The policy adopted and applied by each victim is dictated by the particularities of the situation and the coercive factors. In the case of cities or states whose leaders have declared a state of emergency, refusing any cooperation with criminals, efforts to reactivate computer devices have been huge but the message of non-cooperation with criminals has been particularly strong and resonant. The same happened in the case of important companies that also fell victims, the name Norsk Hydro from Norway being intensely circulated in the media. Transparency in communication and the decision not to pay for data redemption supported by the active involvement of companies specialized in the field of IT security allowed the remedy, the management of the event being an example to follow for all industries.

Each state is functionally organized so that the structures meet the expectations of society, to ensure its independence, security and integrity in relation to other states. In the legislation of one of the states of the European Union, the national critical infrastructure (ICN) is defined as "an element, a system or a component thereof, located on national territory, which is essential for maintaining the vital functions of society, health, safety, security, the social or economic well-being of people and whose disruption or destruction would have a significant impact at national level due to the inability to maintain those functions", and the European Critical Infrastructure (ECI) is defined in accordance with the European legislation [5] as "a national critical infrastructure, the disruption or destruction of which would have a significant impact on at least two Member States of the European Union... The importance of the impact is assessed from the perspective of intersectoral criteria. It includes the effects resulting from the intersectoral relations of dependence on other types of infrastructures" [7] and the protection of critical infrastructures (PIC) represents "the unitary set of processes and activities organized and carried out in order to ensure functionality, continuity. ICN / ICE services and integrity to discourage, mitigate and neutralize a threat, risk or vulnerability by identifying, implementing and maintaining security, organizational, technical, procedural and other measures resulting from risk management processes" [19].

Compared to the previous years, 2019 was marked by an increase in the number of (reported) attacks, especially ransomware, directed against critical infrastructures, institutions, healthcare systems, population service units and last but not least, against certain states, communities, commercial or financial groups, an increase in the intensity of the attacks, the amounts demanded as redemption and, why not, the amounts paid in the attackers' accounts. Such complex attacks in which unauthorized access is obtained, which has not been detected for a long time and with serious consequences for one or more of the structures of a state requires special resources, are considered to be supported by another state, terrorist organizations, multinational companies and are classified as Advanced Persistent Threats (APT). The radiography presented for the United States of America by

Dan Lohrmann, Chief Security Officer & Chief Strategist at Security Mentor Inc. [21] is quite clear in this regard. Medical systems in the European Union have been equally affected, with the UK occupying an undesirable leading position in the top of attackers' preferences. Adam Thompson, leader in e-business and cyber security, has published a study in which he tried to explain how severely they can be affected. care and treatment complexes and what may be the consequences [25]: the functional blockage of an intensive care unit required the transfer of patients to another unit several tens of kilometers away, delays in the application of treatments caused more many deaths (strokes, heart attacks etc.), disrupted the functioning of about thirty percent of the National Health Service organizational units, leading to the rescheduling of medical interventions, including critical surgeries and increased fatality rates for a period of at least three years after the attack.

Sports competitions have not been by passed by cyber attacks, the 2018 Olympic Games being seriously affected. Until the end of 2019, the activity of the "Olympic Destroyer" worm could not be attributed with certainty to a certain group, even if there were initial hypotheses that led to the Lazarus group and deeper verifications that revealed elements common to the Sofacy group (also known as APT28 and Fancy Bear) [16]. Telemetric and stylometric analysis allowed to avoid an association that would later favor the ignorance of the real actors behind the actions, especially since there were secondary attacks on targets in Ukraine, the Netherlands, Switzerland, Russia, France, Germany etc. Olympic Destroyer joins some families of computer viruses considered to be created and managed, operated with state support in Advanced Persistent Threats and which include Flame, Icefog, Industroyer, Plugx, Regin, Shamoon, Stuxnet, Triton, Uroburos, Winnti etc.

In response to the non-payment decisions of some of the victims, multiple pieces of identification captured during the attacks were published online, raising the level of subsequent exposure, which may lead to the idea of an informal platform for collaboration between criminal groups and adoption of common strategies.

The remainder of the paper is organized as follows. In the second section of this paper we intend to present some of the actions of the teams providing cybercrime and technological / institutional reactivity, and in the third and fourth sections, the orientation of the flow of aggression according to national and international events and the response of civil society as a whole in crisis management along with the adopted measures. The results presented in the fifth section regarding the impact that can be felt at different levels of society, are based on information provided by specialized companies, which we have processed and adapted to the context in question. The comparative analysis on alternative scenarios in this field is also based on probability theory, given the high degree of uncertainty and delays in data collection and processing due to cyber events. The final section offers our conclusions and proposals and summarizes the findings, with a brief discussion of economic, social and policy implications, limitations, and avenues for future research.

## II. ADVANCED PERSISTENT THREATS AND STATE SPONSORS

Not a few times a malware code is used as a "mask" for concerted attacks by teams not registered on the list of aggressors. Both the original code sequence, borrowed or purchased together with a set of instructions, and one of the modified variants "to order" to exploit new technologies or to produce different effects are exploited. For credibility, it is intended that the size of the program be identical or very close to the primary one. Careful reading of the instruction set and the exact application of the "manufacturer's" recommendations can mislead the authorities and mislead the investigation teams. However, it is difficult to maintain a perfect pattern for different criminal operators, which allows the exploitation of cracks, comparison, analysis and finally identification.

On the other hand, the allocation of resources by the aggressor state for the creation of a distributed structure, acting on the principle of separate "cells", allows concentrated cell / target attack. High-level interconnection mechanisms allow for the transfer of capabilities in situations of overload (offensive) or crisis (defensive). To cover the traces, official state institutions are used as a screen, without any apparent connection with the respective field, or companies with different lucrative activities are built behind which well-trained cyber espionage teams are hiding. Theft of intelligence and advanced technologies complement the espionage activity. Data leakage, custom or system credentials are preceded and followed by infiltration, infection, soft, hard compromise, and possibly staff recruitment. It is considered to be allowed and any type of instrument of collection or aggression is used in the process of collecting, transferring information or attacking.

### *A. Technological reactivity*

An investigation report posted in the online environment by one of the security companies with expertise in the field of cybercrime presents relevant elements of a link between one of the groups being responsible for very broad-spectrum actions and the state actor behind it [25]. As a unit in a network that has been established to include APT3, APT10, APT17 and which "have a common blueprint: contract hackers and specialists, front companies, and an intelligence officer", according to a team of cybersecurity analysts [15]. APT40 group has carried out actions against targets in the medical field, services, transport, government administration, aerospace and defense, scientific research, communications, construction, industrial equipment, education, high-tech, chemical industry etc.

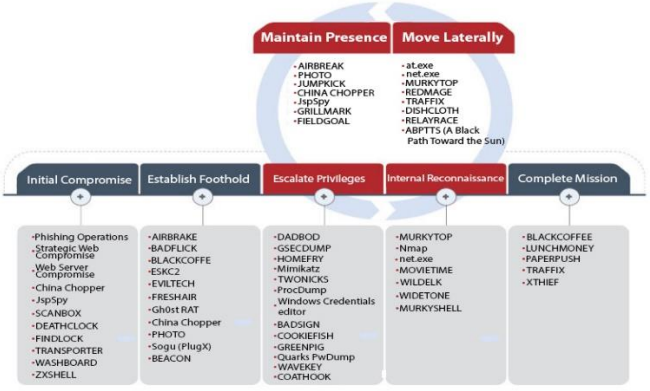


Fig. 1. APT "XX" attack life cycle [23]

A fairly wide range that can be considered, for example, from the unavailability of medical equipment to the implementation of plans to sabotage the navigation system of an aircraft, a high-speed train, overheating, blocking or destruction of energy systems. The way of operation is described in figure 1 being common to other "XX" APTs, especially those sponsored by the same state actor that supports APT 40. Maintaining the presence in a system as long as possible involves, among other things, lateral movement / movement to many components of the system. Fulfilling the mission involves going through the stages of compromise, establishing one or more points of support, escalating privileges and verifying the internal procedures for the system to recognize the intruder as a legal presence.

Technology policies are the ones that influence the personal life and activity of each of us. Hence the confrontations dictated by advantages versus protectionism. Internet of Everything (included Internet of Things and Internet of People like subdomains) is closely linked to Artificial Intelligence (included Machine Learning like subdomain) and in direct dependence on 5G networks landscape. As the changes are likely to cause uncontrollable events or even climatic emergencies, the specialized agencies in the European Union take the subject very seriously, subject it to organized debates and propose appropriate sets of measures [9]. We do not consider that there can be a discussion in 2020 about an over-regulation or a bureaucratization of decision-making processes, even if there are areas of influence impacted differently. Efforts are being made to eliminate the imbalance generated by the advantages of "illicit" growth, sustained by innovation. The capabilities that become available through high-speed information networks can quickly become the subject of "cyberwar". The stability of critical infrastructures, including of the military field, will be dictated by contracts of sale - purchase and supply of 5G technologies, the independence and sovereignty of a country being seriously questioned. The hybrid threats we referred to at the beginning of this study will take on forms that are difficult to anticipate. As an example, the impact of DDoS attacks will be felt more seriously, in proportion to the ability to inter connect, process and communicate devices that can be trained in a coordinated manner against the target. The connection between the producer, the attacker and the state actor is direct. "XX" APTs will benefit from resources made available even by victims. While some government institutions will try to exploit the benefits of 5G, AI and IoT in a positive way, other (state) organizations will also use them as launch levers of attacks. The action of aggressors is sometimes facilitated by poor supervision by competent institutions, coupled with divergent international rules for online services, with the misfiring of information with ignorance of classification or knowingly violating data protection rules, all this being able to produce long-term effects.

In this context, some specialized companies make available to those interested Data Mining platforms with free access, through which are presented real-time statistical situations, dynamic developments, advice, support and appropriate tools needed to prevent and combat cyber aggression. The daily exchange of information between specialized companies contributes to the increase of the analysis capacity, to the reduction of the reaction time and to the consolidation of the capacity to respond to IT incidents. One of the platforms that show trends related to the evolution of cyber threats is shown in figure 2. Graphical information representing the frequency of occurrence between certain calendar data of some malware families is easy to interpret. Placing the pointer over the range of interest provides consistent information that can be exported to several types of formats for processing.

### *B. Institutional reactivity*

Memorandums between countries on compliance with the criteria for the evaluation of 5G technology providers are concluded. The documents are adopted and included, as in the case of one of the EU states, Romania, in the national defense strategy of the country. Strategic partnerships and membership of political, military and economic unions are key pillars in maintaining stability. By signing non-aggression treaties and drawing boundaries that are not wanted to be overcomed / violated, it tries to be kept the balance by the great powers, suppliers and beneficiaries alike.

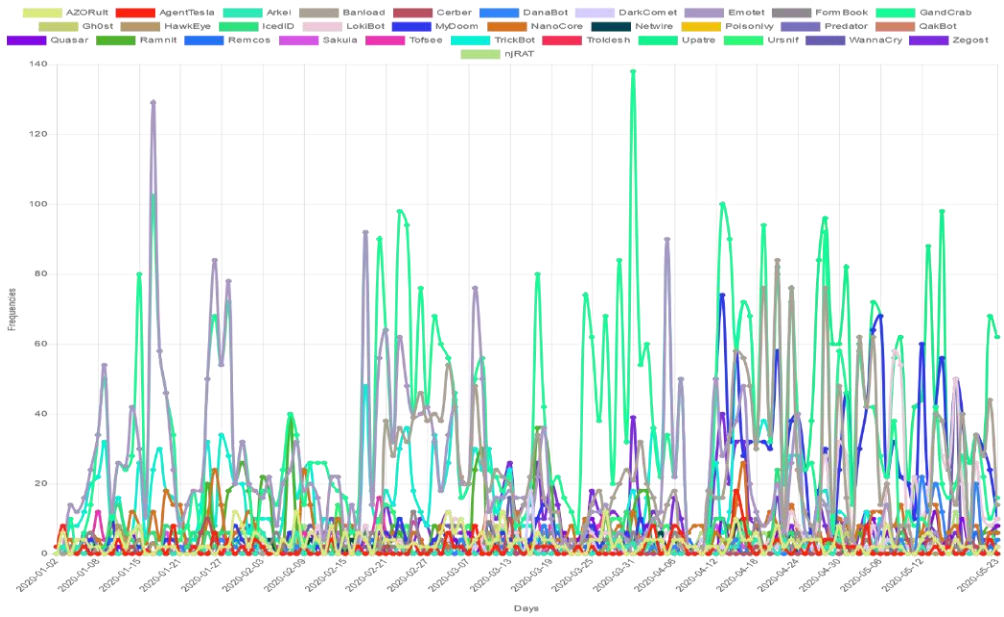

Fig. 2. Frequency in January - May 2020 of Malware Families [24]

With the proposed aim of creating a safer world, the official bodies of the European Union are involved in organizing training sessions and competitions, with the active involvement of the private sector. We consider that the meetings focused mainly on the subject are particularly useful in the sense of proposing, analyzing and accepting future directions for the implementation of security solutions. The European Union Agency for Cybersecurity (ENISA) is an example of involvement in 5G cybersecurity activities and each international entity can participate in supporting the joint effort. To this end, cross-border crisis management exercises caused by one or more cyber incidents are also organized. Following the announcement in a G7 press release to be held in June 2019, the decision was adopted to quickly review all financial regulations. The report presented by the European Commission of the European Systemic Risk Board (ESRB), as part of the European System of Financial Supervision (ESFS), also highlighted one aspect, namely that a cyber incident could evolve rapidly from an operational crisis to a crisis of liquidity and trigger financial instability, especially since the reported losses from cybercrime amounted to between 65 and 654 billion USD in 2018 [18]. In the absence of a firm position on investment and the mandatory adoption of preventive conduct, major crises become increasingly predictable.

## III. CRISIS MANAGEMENT

Crisis events tend to divert attention from common threats, allowing security breaches to be developed and exploited by aggressors. In a crisis situation, one or more critical infrastructures may be affected. Controversial messages and contradictory actions weaken defense mechanisms and create an environment conducive to the infiltration of destabilizing elements. Regardless of the nature of the crisis, the methods of manipulating and exploiting "opportunities" are about the same. The Hegelian principle with its three components, the thesis - the problem is created, the antithesis - the reaction and synthesis are directed - the solution is offered, it works both in case of an economic crisis, security, and in case of a medical crisis. The concept of the Overton Window, of reframing a reality accepted until then as implicit, complements the other methods of manipulation, intoxication, misinformation, fraud etc. What for the majority of the population of institutions and economic agents is at least an issue with debatable, unclear or difficult to solve issues, is an opportunity for a minority, difficult to assess as a share. The cyberspace provides those interested with tools for obtaining illicit income by exploiting the lack of education, obtaining information, key positions in hybrid conflicts etc. Apparently advantageous offers, "miracle" solutions, reports with "knowledgeable" people or opinion polls are often nothing more than vectors of infection for well-scheduled attacks.

If we turn our concrete attention to the criminal cyber actions carried out during the pandemic known as COVID-19 (Coronavirus disease) or SARS-CoV-2 (Severe Acute Respiratory Syndrome Coronavirus 2), we will observe different patterns and volumes of attacks, applied depending on transformations occurred as a result of social distancing and remote working [2] and [4]. Online time slots have changed in terms of schedule and scope, and dependence on digital solutions has intensified. Even if it seems hard to believe, the top three Western countries most affected by the pandemic are also those that have recorded a large number of cyber attacks - Italy, The United States of America, United Kingdom (figure 3). We will try to explain this phenomenon further in this section Campaigns of intimidation, induction of fear and insecurity were followed by so-called information campaigns, but which did nothing but deliver malware and collect credentials. The "rescue" messages were constructed in such a way as to appear to be provided by competent bodies and the topic addressed, COVID-19, increased the interest in voluntary redistribution. Globally, the ranking of the most affected countries in March and April 2020 (pandemic peak) has changed depending on the strategies applied and the speed of propagation / dissemination of malicious components.

We have tried to make Data Mining in-depth analysis and we may conclude that the field of cyber threats is characterized by flexibility, adaptability and has a special specificity - faithfully follows the geographical spread of COVID-19, starting in Asia, passing through Western Europe, the United States America and later Eastern Europe. We mainly distinguish with addressability bulk to lists of contacts purchased on dark / black (web) marketplaces or previously collected and actions with exact / specific / weaponized addressability directed against monitored targets.

The first category includes, among others, messages sent through applications online social networking service and social media, emails with malicious attachments etc. The text, photo, video, audio or other components are nothing but interfaces that allow the virus to be installed when accessed or run, as in the case of links with "sensational" information. Against the background of a high appetite for information, phishing campaigns are built / oriented "thematically" and address topics related to new cases of COVID-19 confirmed right in the place of residence of the recipient of the message, calls that encourage victims to support a seemingly charitable action or to combat the pandemic, urges to take positions under the pretext of restricting fundamental rights and freedoms etc. Even the US in March 2020, the Department of Health and Human Services fell victim to a phishing campaign that delivered malware in the DDoS version under the pretext of an information and counselling campaign (emails and text messages) in the field of health. Social engineering combines feelings of panic, misinformation, and desire to help and stimulates the user to redirect to as many contacts as possible [22]. The tentacles of organized crime are much more branched than they seem at first glance. Revenues from cybercrime can be reinvested in fake products and pharmaceuticals can cover illegal activities. Revenues from fraud can be "laundered" and reinvested in cybercrime or terrorist acts. All of these endanger human lives, organizations or societies. But it is precisely the feeling of panic that "sells" the best and urges even people in good faith to turn to "underground" suppliers. Demand for counterfeit products is rising sharply in times of crisis, despite the negative potential for health. The range is quite wide, from sanitizers and (medical) protective or testing equipment, to food or even "security" systems for which incredible discounts are offered.

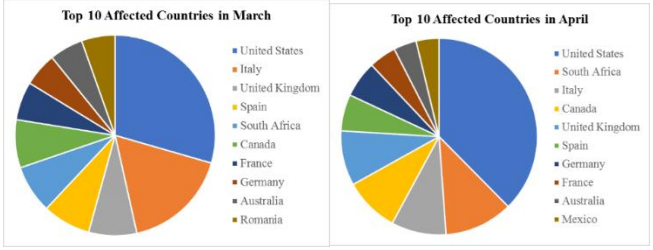


Fig. 3. Countries Targeted by Coronavirus-themed Malware [2]

Not surprisingly, teams offering malware or Crime ware-as-a-Service code for sale diversified their offerings and launched sites with fake products and various types of embedded malware. The collection of information goes hand in hand with the sale of counterfeit products and channels such as Big Blue, Cypher Market, Empire Market, Europe Market, Openbazaar, Telegram, Torrez, Yellow Brick Road etc. Through the online social networks, the interest on fake products or fake news of criminal groups could be measured and countermeasures could be taken. A suggestive Data Mining Graph presented by Europol on this subject is available in figure 4.

The second category includes complex actions, very clearly targeted against some people or of some organizations and from which the aim is to obtain some information of interest for the attacking group, destabilization, intoxication or "hosting" in latent state for a lateral movement and a subsequent reactivation etc. A conclusive example is the employees of the World Health Organization (WHO), who were subject to monitoring / espionage long before this was discovered in April 2020, according to the chief information officer WHO, Bernardo Mariano.

## IV. ADOPTED MEASURES

It is difficult to estimate which of the two categories causes more damage, but we can say with certainty that they overlap in certain areas. On the one hand, bulk messages can generate occasional losses of a mainly economic nature for individuals or small and medium-sized enterprises, but they can also provide gateways to important targets targeted by attackers. On the other hand, compromising key people / points increases the vulnerability of the organization they belong to, allows the contamination of other people / key points of lower, equal or higher level with which it corresponds institutionally and thus can trigger chain reactions with consequences difficult to anticipate. As mentioned in the previous chapter, Advanced Persistent Threats are particularly difficult to detect, the damage can only be quantified after many years and it is unfortunate that in times of crisis APT groups intensify their attacks. Once a certain product is launched on the black market, it becomes difficult to attribute it to a certain group because it can be put into practice by those who developed it or by anyone else who bought it and "tested" it with or without support of developer. The mode of operation, however, entitles specialists to report an event even if it cannot be certified as the work of an "XX" APTs, especially if the attack was short-lived or interrupted when an undercover investigator was detected by attackers. In the absence of firewalls, VPNs and professional security packages, protection (antivirus), mobile devices are as vulnerable as any computer, operating systems being quite exposed in both cases. The overall picture does not look good at all, nor are there any signs of a decrease in the intensity of the attacks. Unfortunately, one of the targets of the attackers is the critical health infrastructure. After the cyber attack on March 12 and 13, 2020, two very important medical units in the Czech Republic were severely affected. The event took place in the middle of the outbreak, forcing the shutdown of computer systems on March 15, 2020 in one of the hospitals and the relocation of patients. Another attack (ransomware) on March 21, 2020 was directed against Parkview Medical Center in Pueblo, Colorado and led to a slowdown in health care services right in the middle of the fight against huge flows of infected patients. On May 4, 2020, Europe's largest private healthcare provider, Fresenius, was hit by a ransomware attack. On May 5, 2020 the Department of Homeland Security's Cyber security and Infrastructure Security Agency (CISA) issued an alert along with the U.K.'s National Cyber Security Centre warning that so-called "advanced persistent threat" groups - state-sponsored hacking teams - are actively targeting national and international organizations involved in the management of COVID-19 disease. To these are added other attacks registered in Spain, France, and Thailand etc. [17].

It is becoming increasingly clear that in the face of global threats, the response must be global. Criminal cartels can only be dismantled if the risks are understood [11] regulatory procedures are aligned and collaboration between global decision-makers is improved so that the response to complement prevention is integrated and at least as fast as the attack [20].

In response to the recrudescence of COVID-19-based attacks, defense mechanisms were naturally activated. At the national and international level, groups of volunteers were mobilized who offered, with the opinion of the IT incident response centers, to support the efforts made in combating the pandemic on all levels. Identifying vulnerabilities is a first step that must be taken in the construction of defense walls in the virtual space to protect medical units engaged in treating diseases. As in other situations, one of them we presented in the second chapter of this document, more many information platforms have made available to the public free-of-charge statistical data with real-time developments, with information on the pandemic being required to be inserted to allow for timely or more comprehensive analysis. One source, https://www.worldometers.info/, is run by volunteers with no corporate, governmental, or political affiliation, and benefits from positive referrals from the American Library Association. Another group of volunteers provided information for more than 25,000 COVID-19 cyber threats. Unlike the group of volunteers mentioned above, COVID-19 Cyber Threat Coalition has other composition [1]. If the detected problems require special access rights, they are escalated to specialized bodies, among them Europol, Interpol, FBI, Department of Homeland Security's Cyber security and Infrastructure Security Agency etc. Voluntary public-private partnerships are proving their usefulness once again. Thanks to good coordination, the new partnership


Fig. 4. Public tweets on fake products and COVID-19 [10]

titled COVID-19 Cyber Threat Intelligence League (CTI League) is built for a possible long-term collaboration as a cyber version of the "Justice League" with more than 1,400 members from various sectors of activity [3].

Even powerful companies like Microsoft have populated button applications that allow access to up-to-date information from official sources online. After waves of "fake news" campaigns invaded a large part of social media channels in January 2020, filtering measures were adopted. Therefore, Artificial Intelligence and Machine Learning systems were activated with the permission of those who supervise the exchange of information in the online environment, managing to identify types of fake news and to block them in a timely manner. In turn, Google has implemented anti-malware packages and blocked tens of millions of phishing emails every day. The published reports referred to dozens of criminal groups supported / sponsored by governments. As in the case of the APTs we discussed in section 2, they also launch their attacks from the eastern part of the European continent, Asia, the Middle East and more recently, South America, the latter preferentially targeting the World Health Organization.

Several states have joined forces and cross-border cooperation has in some cases prevented losses. In one of the cases, the United States sent a very clear warning and support signal in April 2020 when it received complaints from the Information Security Agency about serious cyber attacks on the health system (critical infrastructure) from the Czech Republic, which we discussed earlier. In addition to government initiatives, there are those of the global law enforcement communities. In this view, the Purple Notice alert launched by Interpol in April 2020 in all 194 Member States and the #WashYourCyberHands awareness campaign against crime and computer science from May 2020 are just two of the examples.

## V. FINANCIAL IMPACT

The total cost of an attack (ransomware) depends on the duration and severity of the attack. As we mentioned above, the financial costs also include remediation expenses for restoring the soft and hard state of the systems. If the outcome of an attack also has the effect of leaking a company's multi-level access credentials, the entire security system needs to be rethought and restructured thus leading to additional costs. If there is no business continuity policy implemented, to the losses mentioned above are added those caused by interruptions in activity, potential image deficit etc. Data Mining on operational, financial or other risks data depend on the type of activity.

From figure 5 one may see that the percentages regarding the motivation of the attackers are approximately constant, the first place being occupied by cybercrime. The number of events is growing with the COVID-19 thematic campaigns fully contributing. Unfortunately, globally, in the first quarter (Q1) of 2020, the social and health field is outpaced as a target in the top of preferences of criminal groups only by the individual users and the field of public administration and defense. From the figure 3 we note that among the top 10 most affected countries in Q1 2020 are the United States, the United Kingdom, Spain, France and Germany and we will try to highlight this aspect in the graph presented in figure 6.

In a global crisis, it cannot be said that only one area or one critical infrastructure is affected. Depending on the severity of the crisis, tens or even hundreds of millions of jobs could be lost globally. The COVID-19 pandemic led to a deterioration of working conditions, disruptions of financial markets, accentuating the need for liquidity of companies. Under these conditions, the theft of banking data, followed by the compromise of savings accounts, fraud of some institutions / companies or blocking access to information systems, can lead to a general increase in pressure on society. Due to the nature of the cause-effect relationship, the financial impact is felt at all levels, the human factor being particularly affected. Cybercrime is closely linked to components of financial crime such as money laundering, fraudulent lending and corruption. Illegally obtained money is placed in crypto currencies, in deposits, in retail or real estate projects, investment funds or other legal / illegal businesses, which can go as far as the (hostile) acquisition of important enterprises or companies. We see how cybercrime can fuel a medical crisis and how a medical crisis can fuel cybercrime, economic crime and even cause another food, financial or other crisis in the short, medium and long term.

Under normal circumstances, economic forecasts can be made and even if no mutual agreement can be discussed, it is still possible to estimate possible damage to be recorded because of criminal activities, by reference to previous statistics and the current state from the moment of elaboration. The ratio of gain and loss in relation to cybercrime is much more difficult to build because the effect of an action can show its "fruit" in several years. A regional or global crisis further complicates matters. Therefore, we will not risk in this field to advance figures that may later prove erroneous, especially since there are uncertainties related to evolution.

According to the studies of [13] and [15] for the 4th quarter of 2019 and the first quarter of 2020 the average value of data recovery fees captured by attackers remained relatively stable marking only a slight increase, from $ 4,179 at $ 44,021. Ransomware campaigns have targeted strong businesses,

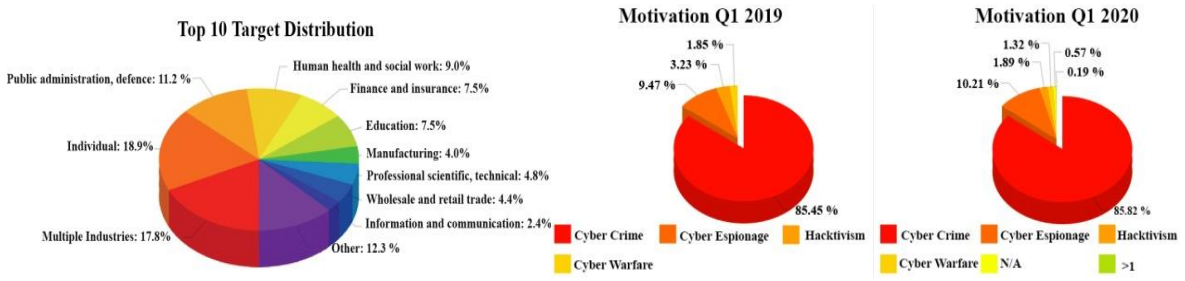


Fig. 5. Distribution of Targeted Domains and Motivation [13]

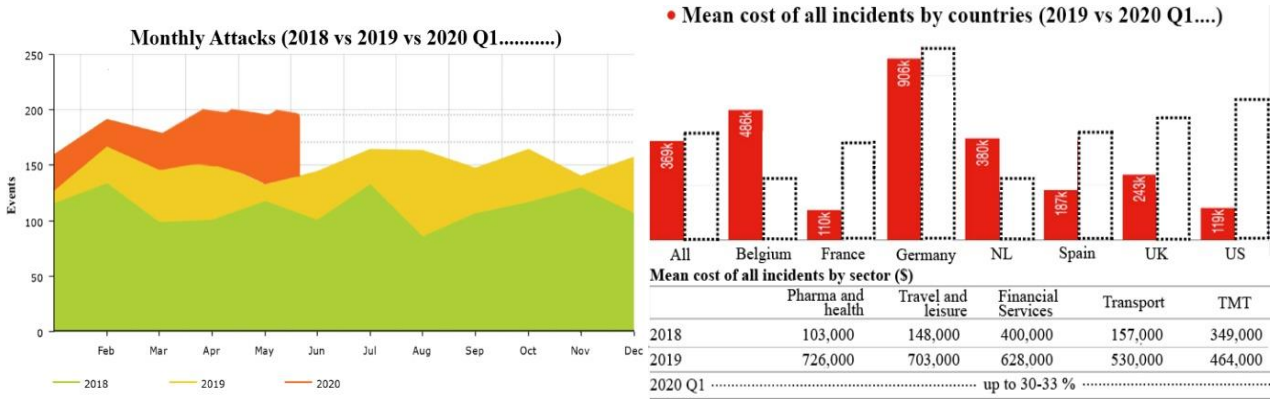


Fig. 6. Monthly Attacks and Mean cost of cyber incidents (own processing based on [13] and [14]

forcing them to force ransom payments. For the industrial sector, the average payment reached $ 111,605, up about 30% in the first quarter of 2020 compared to the fourth quarter of 2019. Referring to the distribution chart from the figure 5 and taking into account the share of the field and the fact that the overall average value has remained roughly constant, they result in a decrease of the average redemption value of the data for individual users for Q1 2020 [6].

## VI. CONCLUSIONS AND PROPOSALS

Technical teams can provide much easier support if units enrolled in a given network make efforts to implement a minimum set of recommendations or requests, which would allow for much better coordination in crisis situations. Public-private partnerships are particularly important. Penetration tests or complex external audits can bring to light vulnerabilities that may prove critical in extreme situations. As an example, altering the data of hospitalized patients with serious illnesses, encrypting or losing them can lead to aggravation of the situation or even death, if the decision to apply treatment is not made in accordance with the consultation form and the person's history. The same destructive effect can be obtained in the event that certain devices connected to information processing servers become inoperable. Good governance requires a proactive attitude, resilience being directly dependent on it. The steps need to be taken in a balanced way. Thus, firstly it's needed to develop regulatory models, based on which, secondly, to adopt regulations able to meet the expectations of economic operators and consumers All these steps require using Artificial Intelligence, General Data Protection Regulation and Digital Services Act and managing the functionalities and the security of 5G complexes, as the necessary preamble in the European Union towards the Digital Single Market [12].

The mission of international bodies, including The Global Commission on the Stability of Cyberspace (GCSC), to regulate cyberspace will not be easy. Even if it seems a purely declarative phrase, it is necessary to increase the degree of flexibility in the operative procedures for responding to cyber aggressions, both at state and international level. It is not just about digital sovereignty, regulation of Internet systems policies, but also about effective collaboration mechanisms. The formalization of the exchange of information at European Union level with classification levels and reporting and approval times of a common structure to which all component states can adhere may give a common vision on the potential dangers and the entities behind them. Some of the proposals that we bring to the attention of decision makers are presented in the followings.

First, the construction of a single platform (in public-private partnership) for warning at European level on the potential dangers to which citizens in certain areas, with a vertical and horizontal architecture, may be exposed under the coordination of the European Commission. Centralized data may be collected both from the competent institutions of the Member States and from other international bodies. The platform can have several sections, depending on the nature of the events. As an example, information on cyber aggression or medical data of immediate interest may be uploaded for dissemination on the same structure. Subject to the rules of confidentiality, warnings may be sent directly to the telephone numbers identified in the affected area, via messaging or secure applications. Good monitoring, proper traceability and fast communication automatically imply "good cross-border interoperability" [8]. The computer filters that will allow the structural classification must be based on items unanimously accepted at European level.

Second, the construction of C3 modules (Community Cloud Computing) in areas of interest for each member of the European Union. From an administrative point of view, we propose that the modules to be placed under the coordination of the European Commission, in collaboration with the responsible national / international bodies. The physical structures should be budgeted and managed by the European Union, but the control should be carried out in partnership. As an example, the exchange of information in case of a pandemic should benefit from technical support so that all parameters of scalability, security and resource allocation are respected, with the active involvement of line ministries in each Member State, World Health Organization (WHO) etc. The research results should be uploaded in a special dedicated area, so that the documented case studies can be commented and analyzed by specialists. Conclusions can lead to a fast adaptation of the measures, reduction of losses, saving lives etc.

Third, in order for the aforementioned structures to function without major interruptions it is necessary compliance with the same security rules. Consequently, a layered security solution must be perceived as a necessity, Thus, implicitly the security products must integrate among others, "layered next-type end point protection, corroborated with end point detection and response" etc. In this context, we

recommend that in the functional branch all units (including medical ones), regardless of membership in the Member State, comply with the rules in the safety manuals developed with the opinion of the European Commission and the implementation procedures.

Fourth, the adjustment of European legislation in the sense of framing the acts that include cyber attacks resulting in premeditated murder or manslaughter, as being culpable homicide or murder attempted with particularly serious consequences, and the adaptation of extradition procedures in this regard. In the same vein, we propose amending international law to impose sanctions against organizations or states that support actions against health care and life support systems.

Of course, the proposals presented above are not comprehensive, but they can be a preamble to reports on which to take decisions with medium and long-term effect. Certain sections of the best practice guides may be re-examined and made mandatory. The security of critical infrastructures depends more and more on IT security and that is why we consider it a priority to align standards as quickly as possible at European level. As in the case of the Titanium project co-funded by the European Union's Horizon 2020, the decision-making executive, academia and the private sector must be fully involved in developing the algorithms and implementing the decisions adopted for each of the areas declared as critical infrastructures.

## ACKNOWLEDGMENT

This work was supported by the grant POCU 380/6/13/123990, co-financed by the European Social Fund within the Sectorial Operational Program Human Capital 2014-2020.

## REFERENCES

[1] Abrams, L., Cyber volunteers release block lists for 26,000 COVID-19 threats, *Bleeping Computer® LLC*, 2020, available at https://www.bleepingcomputer.com/news/security/cyber-volunteers-release-blocklists-for-26-000-covid-19-threats/, accessed on May 12 2020.

[2] Arsene, L., Coronavirus-themed Threat Reports Haven't Flattened The Curve, *Bitdefender/Labs*, 2020, available at https://labs.bitdefender.com/2020/04/coronavirus-themed-threat-reports-havent-flattened-the-curve/, accessed on May 5 2020.

[3] Brumfield, C., Legions of cyber security volunteers rally to protect hospitals during COVID-19 crisis, *IDG Communications, Inc*., 2020 available at https://www-csoonline-com.cdn.ampproject.org/c/s/www.csoonline.com/article/3539319/legions-of-cybersecurity-volunteers-rally-to-protect-hospitals-during-covid-19-crisis.amp.html, accessed on May 2 2020.

[4] Chang, C-L, Michael, MC. and Wing-Keung, W., Risk and Financial Management of COVID-19 in Business, Economics and Finance in *Journal of Risk and Financial Management* 13(5), 102, 2020.

[5] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L 345/77, 1-8.

[6] Coveware, INC., Ransomware Payments Up 33% As Maze and Sodinokibi Proliferate in Q1 2020, 2020. Report, available at https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report, accessed on May 3 2020.

[7] Emergency Ordinance No. 98/2010 *on the identification, designation and protection of critical infrastructures,* in the Official Gazette, Part I no. 757 of November 12, 2010.

[8] European Commission,. eHealth Network, Mobile applications to support contact tracing in the EU's fight against COVID-19*, Common EU Toolbox for Member States, Version 1.0*, 2020, available at https://ec.europa.eu/health/ehealth/key_documents_en#anchor0, accessed on April 23 2020.

[9] European Union Agency For Cyber Security (ENISA), Enisa Threat Landscape for 5G Networks, ISBN: 978-92-9204-306-3, DOI: 10.2824/49299, November 2019.

[10] Europol, European Union Agency For Law Enforcement Cooperation. *Viral marketing Counterfeits, substandard goods and intellectual property crime in the COVID-19 pandemic*, 2020, available at https://www.europol.europa.eu/publications-documents/viral-marketing-counterfeits-substandard-goods-and-intellectual-property-crime-in-covid-19-pandemic, accessed on April 23 2020.

[11] Gaftea, V.N., Socio-economic Major Risks Related to the Information Technology in *Procedia Economics and Finance* 8. 336–345, 2014.

[12] Gaftea, V.N., Ioniță, A., NIȚU,I. and POPA, I.F., România şi Piața Unică Digitală a Uniunii Europene. Oportunități şi provocări, *Romanian European Institute*, ISBN online: 978-606-8202-59-4, 2018, Bucharest.

[13] Hackmageddon, available at https://www.hackmageddon.com/2020/04/14/q1-2020-cyber-attacks-statistics/, accessed on May 9 2020.

[14] Hiscoxltd, Cyber Readiness Report 2019, available at https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf, accessed on March 9 2020.

[15] Intrusion Truth, APT40 is run by the Hainan department of the Chinese Ministry of State Security, *Blog*, available at https://intrusiontruth.wordpress.com/2020/01/16/apt40-is-run-by-the-hainan-department-of-the-chinese-ministry-of-state-security/#more-587, accessed on April 30 2020.

[16] Kaspersky Team, Olympic Destroyer: who hacked the Olympics?, #TheSAS2018, *Blog, Kaspersky Daily* 2018, available at https://www.kaspersky.com/blog/olympic-destroyer/21494/, accessed on January 10, 2020.

[17] Krebs, B., Europe's Largest Private Hospital Operator Fresenius Hit by Ransomware, *Krebs on Security*, 2020, available at https://krebsonsecurity.com/2020/05/europes-largest-private-hospital-operator-fresenius-hit-by-ransomware/, accessed on May 10, 2020.

[18] Lagarde, C., Remarks on the occasion of receiving the Grand Prix de l'Économie 2019 from *Les Echos, European Central Bank,* 2020, available at, https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200205_1~cc8a8787f6.en.html, accessed on February 23 2020.

[19] Law No. 225/2018 for the amendment and completion of the Government Emergency Ordinance no. 98/2010 on the identification, designation and protection of critical infrastructures, text published in the Official Gazette, Part I no. 677 of 03 August 2018.

[20] Lipton, D., Cyber security Threats Call for a Global Response, *IMF Blog*, 2020, *International Monetary Fund*, available at https://blogs.imf.org/2020/01/13/cybersecurity-threats-call-for-a-global-response/?utm_medium=email&utm_source=govdelivery, accessed on March 12 2020.

[21] Lohrmann, D., The Year Ransomware Targeted State & Local Governments, Lohrmann on Cyber security & Infrastructure, Government Technology, 2019, available at https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2019-the-year-ransomware-targeted-state--local-governments.html, accessed on April 15 2020.

[22] National Cyber Security Centre (NCSC), Cyber security and Infrastructure Security Agency (CISA), Advisory: COVID-19 exploited by malicious cyber actors, Version 1.0, April 8 2020.

[23] Plan, F., FRASER, N., O'Leary, J., Cannon, V. and Read, B., APT40: Examining a China-Nexus Espionage Actor, Threat Research, Fire Eye, 2019, available at https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html, accessed on April 12 2020.

[24] Ramilli, M., Cyber Threat Trends, Cyber Threat Trends Dashboard, 2020a, available at https://marcoramilli.com/cyber-threat-trends/, accessed on March 14 2020.

[25] Thompson, A., Cyber Attacks Are Killing Hospital Patients: Could Cyber criminals Be Prosecuted for Murder? in *The SSL Store*, 2019, available at https://www.thesslstore.com/blog/cyber-attacks-are-killing-hospital-patients-could-cybercriminals-be-prosecuted-for-murder/, accessed on December 19 2019.