CYBERSPACE – A CHALLENGE

Adriana GRIGORESCU
National University of Political Studies and Public Administration
30A Expoziției Blvd, București 010324, Romania
Correspondent Member of the Romanian Scientists Academy
54 Splaiul Independentei, Bucuresti, 50085, Romania
adriana.grigorescu@snspa.ro

Razvan-Ion CHITESCU
National University of Political Studies and Public Administration
30A Expoziției Blvd, București 010324, Romania
razvanric@yahoo.com

Abstract. *The future means cutting-edge technology, much more developed human relationships, but lacking effective engagement, advanced knowledge and also new frontiers to achieve. Thus, the society of the future means technology, unlimited possibilities of unknown connections and challenges. All these opportunities are, however, associated with risks, threats and vulnerabilities. The Internet, as a tool, has significantly contributed to the technological and scientific progress of mankind. The multitude of opportunities it offers and easy access to every citizen, with the lack of a unitary legislative framework at an international level, effective and concrete control over the development of some applications. This confrontation does not always have the desired result, and the relatively controlled development and use of it is very difficult to achieve, especially for state actors. The virtual world thus gains ground through addiction, the cyberspace becoming the quirk that aligns the successes and failures of mankind, the pattern of future battles that can reconfigure the map of the world, the easel on which our deep emotions are outlined. It is a mirror of society and the place where predictions on the future can be sold. Cyberspace has no borders. It is globalization in its purest form, it is a new paradigm of modernity. It is the opening of man to man at every level. Risk is a constant component of technological, social and economic development, but knowing the limits in which it can manifest, through its anticipation and action can diminish its negative effects. In front of the cyber-attacks, everything becomes vulnerable - from the critical infrastructure of a country to the security of each individual. The product effect is chained, each vulnerability creating prerequisites for exponential growth of associated risk and affecting security from an individual level to a global level. The virtual world is already the world of tomorrow. How will we identify the opportunities and manage the benefits? And how will we reduce the associated risks, current and future threats? What are the solutions? These are the questions we will be trying to answer through our study. For this purpose, the current situation of the Romanian society connected with the transformations brought by the cyberspace will be analyzed. We will refer to the infinite possibilities of action, information resources and products in operation, and we will try to identify effective actions that can limit the risks.*

Keywords: *Digital transformation; Cyberspace; Treats; Opportunities; Risk management.*

Introduction

Cyber space has been called the fastest technological space of evolution in human history, both in scale and in terms of properties, the "fifth theater of operations" as Marc Goodman called it. Citizens have the right to exteriorize, in the virtual space, their emotions, thoughts, creations without being constrained in any way: such as, expression, content, and form. This freedom generates new issues, especially legal controversies, that way imposing a substantive reorientation in the interpretation of freedom of expression. The extensive community of Internet users, the ones with easy access to virtual environments, generate a rich palette of cultural patterns, way of thinking, preferences, habits, necessities and, implicitly, generates a demand for extremely varied contents (Buzan, 2014).

This information must be available instantly and, most often free of charge, in this way the information market is constantly growing, by demanding and offering more complex virtual services. Throughout this virtual world, the sense of security is given by the anonymity, even if only to a relative degree.

Under the protection of anonymity, you can request data, information, and you can convey opinions and messages, without being subjected to legal treatment or sanction. This stimulates the courage to ask and convey information. In this "legal paradise", users are banned from legal constraints, which generates a detachment behavior towards the rules applicable to ethical conduct in the virtual space and a comfortable, intimate state in this global community.

The relative security offered by anonymity in virtual space, as well as the large number of smart devices or applications designed to simplify our lives, turn us into potential victims of hackers. It is impossible to have total, effective protection against these kind of attacks in the virtual space. Marc Goodman believes that "all personal data disseminated online or offered by accepting the terms of use of applications transform us from customers to products". The target of these attacks is the information, the data that can be obtained, and the costs that generate the development of applications that can generate data are insignificant in relation to the profits made by the experts who develop them.

New economy or the digital economy

The digital economy is defined as being the interaction between the personal computer, the Internet, telecommunications and electronics, having a set of distinctive features towards the traditional economy.

The new business model - e-business, e-commerce, e-banking, etc. - developed via the Internet, brings a radical change in efficiency: costs, including transaction costs, are reduced, based on the business/business relationship (B2B), business/customer (B2C), C2B and C2C business/employee (B2E) business/government (B2G), government/ business (G2B), etc. This ecommerce model has developed exponentially in the last decade, and has expanded into all areas, now being considered the concrete form of accomplishing most businesses (Gordon, 2016).

The microeconomic and macroeconomic effects of the new economy and information systems are based on the generally valid principles of its development, which are: awareness, accessibility, availability, affordability and appropriateness.

Electronic commerce

The figures and statistics put into place by the main players in the Romanian electronic commerce show that in 2017, online shopping grew to 2.8 billion euros, 40% more than in 2016 with a registered 1.8-2 billion euros. This would mean that Romanians spent an average of 7.67 million euros every day of the year on internet shopping (details on e-commerce in Romania in Zbuchea, Vătămănescu & Pînzaru, 2015).

This value refers strictly to e-tail, without considering services, utility payments, airline tickets or holidays, hotels, shows reservations. The 40% increase is one of the highest in the EU countries, but rather small compared to the developed economies, thus showing the enormous potential for growth in this segment.

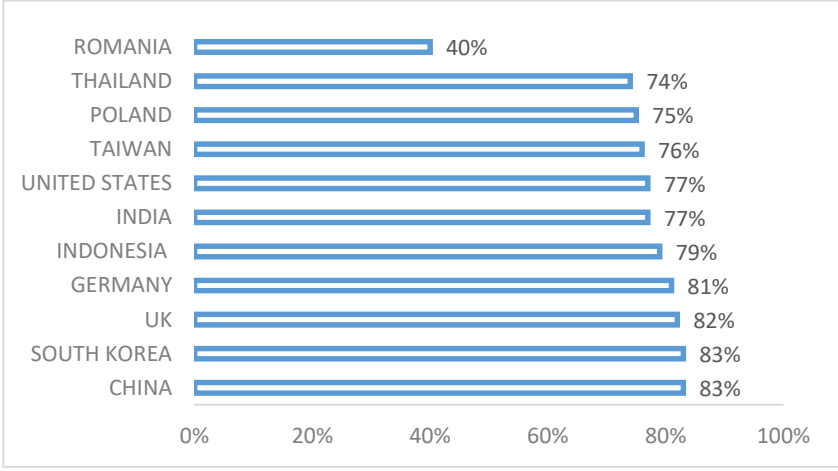

Figure. 1. Global market with the highest online shopping penetration rate as of 2nd quarter of 2017 (Source: Processing after https://www.statista.com/statistics/274251/retail-site-penetration-across-markets/.GlobalWebIndex ©Statista 2018 Additional information: Wordwide, GlobalWebIndex; Q2 2017, 16 to 64 years)

E-commerce is a concept that designates the process of buying and selling or exchanging products, services and information, using a computer network, including the Internet. This concept can be defined from several perspectives: communications, business processes, services, or online. The used technologies are diverse, including messaging, internet, and intranet or extranet services.

The reasons for the implementation and development of e-commerce are based on the ongoing need to broaden the clientele, as well as to reduce the costs for services and distribution towards customers. The initiation costs of an electronic commerce process are quickly amortized, with the main advantages being the volume of information sent through the electronic channels, the upgrading and accuracy of the transmitted data, as well as a better control over the market segment to which the message is transmitted. Back-up can be received in real-time, changes required by the market or development

policy can be applied or modified immediately. Other benefits of using e-commerce are: interoperability, global character and easy to use.

According to **Statista**, global retail e-commerce sales will reach $ 4.5 trillion by 2021 (246% more than 2014).

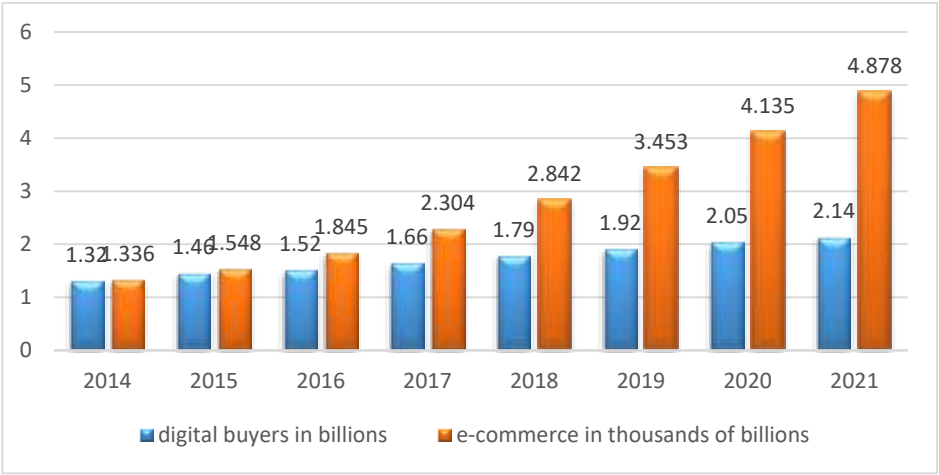

Figure 2. Worldwide digital buyers versus Retail e-commerce, 2014 to 2021 (Source: Processed data eMarketer ©Statista 2018 Additional information: Wordwide, eMarketer; 2014 to 2017 https://www.statista.com/statistics/251666/number-of-digital-buyers-worldwide/ https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/)

Financial-banking activities

The development of the banking market also took into account digital technologies. Banking systems are being used more and more, whether it be credit, cards, ATM or POS. The client is virtually positioned within the banking institution through mobile, internet and home banking. The development of these systems was also possible due to the explosive development of digital telecommunication, the advanced technology installed on mobile phones (Grigorescu, Chitescu & Diaconeasa, 2016).

However, in this situation, the risk of using electronic banking services on smart devices increases due to the dual way of achieving the security of these operations: both banks and mobile phone operators must develop encryption systems for transmitted data as well as secure reception channels or data transmission. It is necessary to establish common security, interoperability and compatibility parameters of the offered services.

Socialization – social media

The presence of e-commerce on social media networks has become a must-have, regardless of the type of business: B2B or B2C. Being the space where more and more people spend their free time, the social media approach from the perspective of electronic commerce is essential. It is a familiar environment where you can learn or realize the value of a product or service. Studies have shown that more and more social media consumers are looking for product reviews on their favorite social network, and in this way they can decide the degree of trust they have for that brand.

It is the social-proof effect - when a social networking user gains confidence in a brand based on reviews received from virtual friends - influencers. Promoting a product on social networking is more applied, these networks identifying a certain type of behavior and consequently, adapting the promotion to that profile. The tools offered by these social networks also allow the measurement of trade efficiency of this type.

According to Statista, 80% of people frequently accessing social networks are shopping online, and 50% often shop. 71% buy products only based on reviews in the virtual space or based on recommendations.

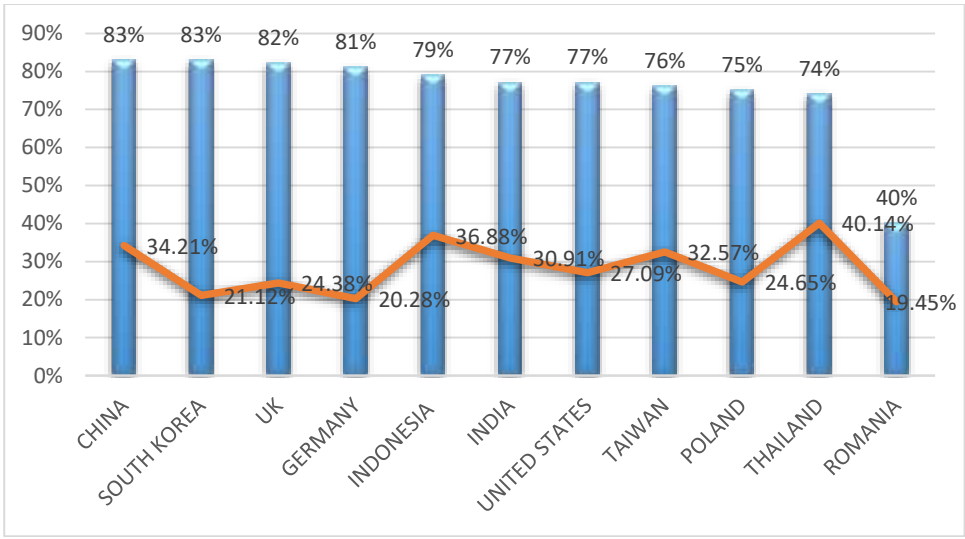

Figure 3. Online shopping penetration rate vs. Time spent on the internet (Source: Processing after https://www.statista.com/statistics/274251/retail-site-penetration-across-markets/.GlobalWebIndex ©Statista 2018 Additional information: Wordwide, GlobalWebIndex; Q2 2017, 16 to 64 years)

In figure 3 we analyzed the penetration rate of online shopping in different countries, relative to the average time spent by users in those countries on the Internet. The percentage of time spent on the internet was calculated as the ratio of time actually spent in 24 hours. Regarding that in those 24 hours a person has different activities - sleep, meals, work/school, etc. - we notice that the time allocated to the virtual space is very high. Thus, in Thailand, the time spent on the internet exceeds 9 hours a day.

The dynamics of the increase in the use of information to and from the virtual space shows that the number of users increases daily by more than one million. In 2018, the total number of users is over 4,021 billion, up 7% from 2017. The number of social media users is almost 3,2 billion, up 13% from 2017, as we have over 5,135 billion mobile phone users. GlobalWebIndex shows that, on average, an internet user spends about 6 hours a day using Internet-based devices and services. If we evaluate this time at the level of over 4 billion Internet users, we see that in 2018 alone, over one million years, cumulated, will be spent on the internet.

The processing of the data in figure 3 shows that developing countries have, in relation to the value of online shopping, a long time spent on the internet. This is explained by

the fact that these countries have been introduced to technological developments in recent years, the internet being a much newer tool than in developed countries. Emphasis is placed on capturing information, on social media with its advantages and disadvantages. In African countries like Mali, the number of social media platform users increased 6 times in 2017. Accelerating access to these economies will influence Internet experience for users everywhere, companies such as Facebook, Google, and Alibaba will have to adapt their resources to deliver products that meet the needs and demands of these emerging economies.

Risks in cyberspace

The dynamics of virtual space expansion and its intersection with social relationships in the real world are genuine challenges (Dunnigan, 2010). Vulnerabilities and risks tend to arise. ***Vulnerability*** is a weakness of a hardware or software system that allows unauthorized users to gain access to it.

The main vulnerabilities in computer systems are physical, hardware, software or human. Information systems are primarily vulnerable to classical attacks when a hacker manages to physically penetrate computing systems and evade confidential information. Every computer system has vulnerabilities, so we can say there is no 100% secure system, an attacker can act in many different ways. Ways of responding to these attacks generate, first and foremost, long time resources: identification of the aggressor, vulnerability and threat analysis, methods used, development of response elements, and counterattacks are necessary.

The dynamics of this field's development requires an equally dynamic evaluation and development of Cyber Security policies, the challenge addressed to specialists in cyber security methods/actions being to reduce the extent of damage that can be produced in the short or long term. A cybernetic attack may have a major impact, may affect the economies of some countries, influence policy decisions, or make decisions in adopting a concrete response. Thus, the solution is a continuous, dynamic technical, analytical and intelligent process that integrates the information provided by various specialized sources (Marga, 2017). It is a process that requires at least the same determination, intelligence and thoroughness that attackers have when they aim to gain access to a targeted cyber infrastructure. The solution has a continuous character, an incomplete and sporadic approach produces a gap between the operational and informational needs, leaving valuable assets under the incidence of the ***risk***.

The fundamental role in preventing and combating risks and threats towards national security in all areas of manifestation is held by the state through its defense policies. The main feature of the virtual space - the lack of borders - imposes a more active role, an involvement of all its institutions in the prevention of virtual space threats. The overall objectives of cyber security are to identify and classify the vulnerabilities and risks present in the cybernetic environment, to analyze the evolution and structure of cyber-attacks, to identify good practices on preventing and limiting the effects of these attacks, to research the state preparedness, to counter the risks and challenges present in cyberspace and to analyze the cooperation between the public and private sectors.

Cyber security means different things for different stakeholders, often without a total and common understanding of meaning, implementation and risks (Goodman, 2016).

There are also important cultural impediments, not only between sectors, but also within the same sector or within certain organizations. Traditional approaches to security may be inadequate in cyberspace, but the consensus on alternatives has been elusive.

In the field of intelligence paradigm shifts have emerged - from "need to know" to "need to share" and then "need to share capabilities" - which implies overcoming the formal barriers in the exchange of classified information, the framework of public-private partnerships, in order to effectively improve the communication between the two parties and a unitary and efficient coordination.

Increasing the vulnerability of personal systems to cyber-attacks of any kind is directly proportional to the ability to evaluate the data received by each user. Thus, the more we believe in the screen, the more automatic data will be taken, we will consider them real, without a concrete analysis of them, and without considering piracy of data or sources. Efficiency of an IT system should take into account a set of factors such as the value that needs to be defended, identifying attacks and cyber attackers, or analyzing the attack and finding ways to stop or reduce its effects. A first step in making an answer more efficient takes into account the fact that no system is invincible, that we must change the paradigm of the "non-breaking wall" assuming, the awareness that cyber-infrastructures are already penetrated, that there is no total protection. Attackers are interested in penetrating the informational infrastructure to either detect it for as long as possible in order to access as much filtered information as possible.

The global expansion of cyberspace has led to the development/modification of conflict zones and of modalities of action. Thus, the costs of a cyber-attack have made it possible to attack state-level targets with advanced technological levels, even by traditional criminal groups, but without advanced capabilities, but by using tools that exist on the relevant markets. Goodman said that *"Traditional criminal groups have set up cybercrime divisions to exploit the possibility of huge gains and low risks".*

This context denounces increased efforts by states to collaborate and coordinate cyber-attacks in partnership with international organizations. It is aware of the need to adopt rules for the use of virtual space, standards for assuming responsibilities in the case of cyber-attacks, and practices in the fight against cyber-bullying committed by non-state actors.

To this end, the United States of America (USA) are an active participant in United Nations (UN) meetings in the field, developing cooperation plans with other states to ensure cyber security (v. Council on Foreign Relations, Cyber Threats and International Cooperation, Workshop Summary Report, Washington DC, 26.02.2015).
EU policy places cyber security responsibilities on the prerogatives of member states.

Attributable to this the *EU Strategy on Cyber Security* has been developed, *"representing the EU's global vision on the best ways to prevent and manage cyber-disruptions and attacks"* ("Cyber security issue in international organizations and involvement of Romania as a member thereof", www.mae.ro). This document, even if it does not require a unitary approach at the level of the union, states the collaboration with international partners, the private sector and civil society. A key objective is *"to establish a coherent international policy of the European Union on cybernetic space and to promote the*

fundamental values of the EU" and an implementation measure of *"international cooperation on cyberspace".*

The states, on behalf of a subsidiarity, can control only 10-15% of the cyber space, the rest being in the private and family sphere, a global partnership approach is needed for the first time with a common mission (Rohrig & Smeaton, 2018), clearly defined objectives and globally accepted, firm action directions and generally valid legal provisions.

According to Marc Goodman, in "Future Crimes", which appeared in 2015 (translated in Romanian in 2016 under the title "X-Cyber: The future begins today"), believes that "we entered the era of computing transformed into a weapon, virtually anyone who has a few dollars to spend can have access to levels of unimaginable cyber power" so far and the action to counter these attacks has to be done voluntarily by every internet user using crowdsourcing strategies ("the action to direct a task to a vast and undefined group of people through a public appeal"), gamming, a "new field of study that allows playful thinking and mechanics in real contexts to motivate and engage players in solving problems concrete" or even improving the public-private partnership.

In 2013, Romania had implemented, the *Cyber Security Strategy of Romania*, whose main directions of action are: *"to conclude international cooperation agreements to improve the response capability of major cyber-attacks; participating in international programs that target cyber security; promoting the national interests of cyber security in the international cooperation formats of which Romania is part of"* (Decision No. 271/2013 for the approval of the Cyber Security Strategy of Romania and the National Action Plan on the Implementation of the National Cyber Security System, Annex no. 1).

Frauds, thefts

According to the Nilsen Report, one of the biggest fears in the online space is fraud. According to this study, in the last 4 years, fraud has developed faster than e-commerce, for every 100 $ profit, 5.65 cents are stolen. Among the most used methods of fraud, Worldpay has identified identity theft - 71%, phishing - 66%, account theft - 66%, friendly fraud, clean fraud, subsidiary fraud, triangular fraud and trader fraud.
According to CERT.ro, in Romania, in 2015, a number of 2,321,931 IP addresses, representing 26% of the total number of IP addresses valid nationally, were involved in at least one cyber-security alert, and a number of 17,088 .ro domains (6.5% of all .ro active domains) were reported as compromised - up 58% over the previous year.

Manipulation

According to the Sociology Dictionary, *"manipulation represents the action of determining a social actor (person, group, etc.) to think and act in a way that is compatible with the interests of the initiator and not his interests, using techniques such as persuasion that deliberately distorts the truth, leaving the impression of freedom of thought and decision".* On social networks, manipulation means imposing the interests of some groups by misleading, distorting information, or influencing opinions and behavior of an individual or a group. Manipulation can take many forms: misinformation, intoxication, lies, rumors, persuasion, temporal distortion, attribution, etc.

Manipulation, as a form of deviation from objective information, and plays an active role in influencing the social network user in determining choices, behaviors, action or inaction. In this way, the digital economy becomes a tactical field for professionals in handling. The risk of using the Internet is the presence of disinformation professionals, especially on new media channels, the stake being the large number of consumers of this type of information and their concern for a particular topic (Iancu, 2010). Political manipulation has the greatest impact, by imposing new media as an alternative/competitive form of written media, by eliminating divergences of interest and extending targets.

Terrorism

The most aggressive form that relies on social media networks is terrorism. Terrorist organizations have thus found a way of developing, several main directions: intimidation - by presenting executions or attributing terrorist attacks, in order to create a sense of insecurity - coordination, positioning - by exemplifying the activity that it does - or recruit it. Beyond the social media communication aspects that terrorists use in their work, another extremely violent side of their work is cybernetic terrorism, meaning the use of cybernetic tools for attacks on private or public targets. (Grigorescu, & Chitescu, 2017).

More and more extensive Internet facilities allow the use – without much knowledge- of a "dark net" part of the encrypted Internet, which is not registered by search engines, and which offers a higher degree of anonymity to its users. In this way, tools that help cybercrime develop very quickly and can create state-of-the-art security breaches. Twitter social network closed over a quarter of a million accounts linked to jihadists from the Islamic State, Europol estimates there are no fewer than 90 different platforms and social networks currently used by the State of Islam.

All these negative, harmful, secondary effects of electronic services are not able to determine approaches that restrict the rights and freedoms that cyberspace are offering. There would be a situation in which people interacting in the virtual environment would benefit from different legal protection than those in the real world. Extremely dynamic technology development leads to extremely complicated legal issues (Radziwill, 2015), a natural situation in this context.

The censorship of content handled in the electronic space must take into account the cultural, social, political and economic differences of a user community in a globalized context. Globally accepted legal rules will be established with great difficulty, by identifying and accepting moral norms that each state promotes. In this context, well-defined democracies will better understand the positive valences of the virtual environment, access to vast information resources in all fields - science, education, culture -, and will not lift legal barriers in the cyberspace. Censorship in this environment will be directed to information users/receivers rather than to information issuers.

Cambridge Analytica Case study

An extremely important opportunity offered by virtual space is that it creates a space for debates, opinions of any kind, as well as components of a stable democratic process.

This facilitates the participation of a large number of users in the debates of political ideas and the adoption of certain political decisions on different levels. This type of debate allowed the possibility for low costs in relation to the number of present users, sent messages, the rational arguments presented and the interaction with the other participants in the debate. The reverse of this type of meeting consists in the possibility of manipulating the data of interested organizations for political purposes. Goodman thinks we are now entering "the computer scientist turned into a weapon era".

One of the most recent examples of virtual data security was that of Cambridge Analytica. It has illegally accessed the data of 2.7 million Facebook users in the countries of the European Union. The European Commission said that *"Facebook has confirmed that the data of up to2.7 million Europeans - or, more specifically, people in the EU - were probably inadequately accessed by Cambridge Analytica".* Statistically there were 1,079,031 people in the UK, 309,815 people in Germany, over 6,000 Maltese people, 214,134 people in Italy, 211,667 people in France, 136,985 people in Spain and 112,421 people in Romania, 89,373 users in the Netherlands, in Portugal 63,080, 60,957 people in Belgium, 59,480 people in Greece. In Poland, 57,138 people are affected, 55,337 in Sweden, 44,702 in Ireland, and 41,820 in Denmark. In Bulgaria, 35,718 people were accessed, 33,568 users in Austria and 32,067 people in Hungary and 29,376 in the Czech Republic, 21,517 in Croatia, 19,693 in Finland, 15,123 in Lithuania, in Slovakia 14,846, in Slovenia 11,255, in the Republic of Cyprus 7,455, Estonia 5,510, Latvia 4,757 and 2,645 people in Luxembourg.

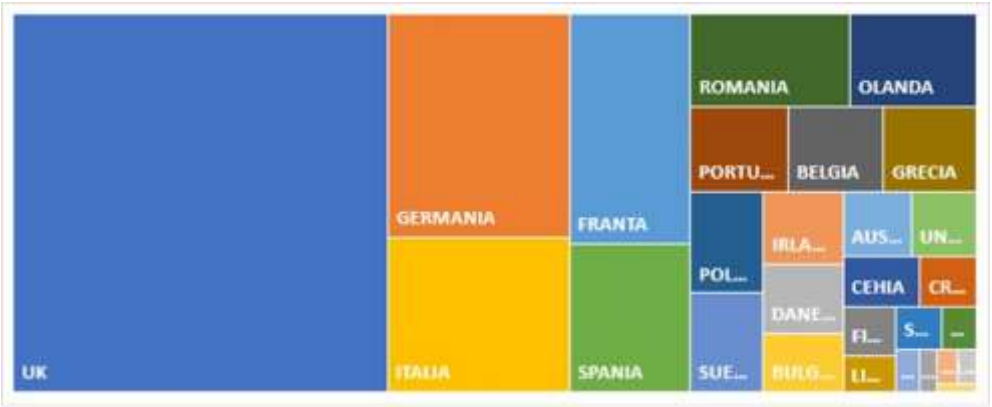

Figure 4. Country distribution on affected people
(Source: Facebook)

The consultancy firm has thus taken advantage of the vulnerability of data protection in the virtual environment, in this case on a high-impact social networking site, to steal Facebook accounts for use for undeclared purposes, in political interest, with serious repercussions in real life.

In 2014, the company, by interpreting data extracted from social accounts, achieved the political profile of American voters to whom election was influenced by sending personalized political ads. An observer mentioned: "*we have exploited Facebook to get millions of voters' profiles. (...) This was the basis on which the company was built*". The information was collected through an application called "thisisyourdigitallife" created by Professor Aleksandr Kogan independently of his Cambridge University work, which, through his company, Global Science Research (GSR), in collaboration with Cambridge

Analytica, has contacted hundreds of thousands of Facebook users to complete personality tests under the pretext of using data for academic studies. However, the application also collects the data from the "friends" lists of those who accepted the tests, so the profiles of tens of millions of people have been obtained.

Cambridge Analytica was involved in US President Donald Trump's campaign and the pro-Brexit campaign, that is, Britain's out of the European Union. Named by Steve Bannon as a *"psychological war tool",* the company exploited Facebook data of tens of millions of American citizens, for electoral purposes, using their Facebook profiles fraudulently to build a powerful software program to anticipate and influence electoral preferences. Facebook Vice President said *"it's a scam. We'll take all the necessary steps to erase the stolen data, we'll initiate legal actions against the authors of the illegal activities",* Facebook initially did not warn users and took only limited measures to secure data over 50 million people. According to The New York Times, copies of Cambridge Analytica data are still online.

Facebook defended their actions, claiming that *"Most users gave the app access to information such as their public profile, but also the pages they liked, the friends list, and the birthday. It was the same for friends whose settings allowed sharing"* and that it is *"important to remember that bank account details, credit card information, or national identity card numbers have been distributed were not distributed"*, and *"the developer of the application involved in this leakage sold Cambridge Analytica data US users, not users in the EU"*. Facebook will not pay compensation to the 2.7 million European users whose data were improperly transferred to Cambridge Analytica.

Following the scandal, Facebook's CEO, Mark Zuckerberg, apologized for his company's mistakes for using personal data, and assured that he is committed to making changes to that. However, mistrust, suspicion and uncertainty among users did not lead to the creation of an individual culture of information security, meaning the lesson was perhaps only the first step in the informational war.

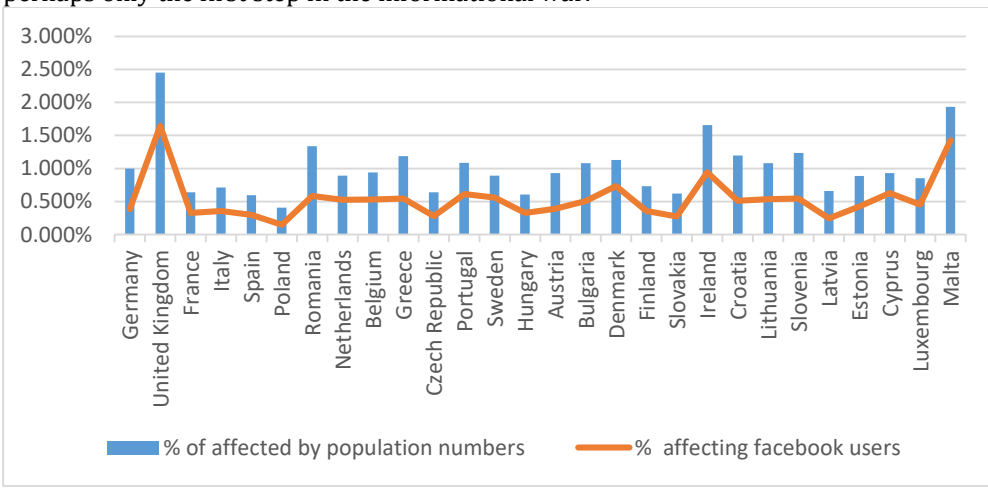

Figure 5. People affected inside the EU regarding the number of Facebook users and population (Source: Facebook)

In figure 5 we highlighted the percentage of users affected directly compared to the total number of persons in the country. We can observe that there is a balance between these

two values in almost all the EU countries. Therefore, there were no countries regarded as direct targets of this data theft, but it was only the clear tendency to obtain data from as many Facebook users as possible. This is more worrisome because we can observe the global dimension of this attack. The possibility of an economic, social, political manipulation or even a security attack would have regarded as a whole and not a particular case. The effects would have been felt at the EU level as well as globally. Not a country or community was the target, but the extended community of Facebook users, which represents more than 2.23 billion people. At a European level, nearly 3 million people have been affected.

Conclusions

The Cambridge Analytica case is one of the events that has affected a huge number of users and which, thanks to the measures taken by the affected states, have become extremely visible. Similar cases, of a greater or lesser magnitude, but which have not been discovered or have not caused a response of such intensity exist and will still exist. Due to political manipulation, this scheme can also be used in the case of economic, social or even terrorist manipulation. We do not have access to data about such schemes, but they certainly exist. These areas are not dispersed, but there is an interconnection and influence between each. Social manipulations are reflected in the economy, the economics of society, the reactions of society and implicitly, the safety of citizens, as terrorist manipulation manipulates the trust of the population and strongly influences the economic and political area: certain unsustainable social needs to potentiate the importance of terrorist attacks to the extent of society's dissatisfaction. These can have a great impact, with local, national or global influences: for example, a terrorist action dressing the globe's environmental action can become an extremely easy and profitable source of finance.

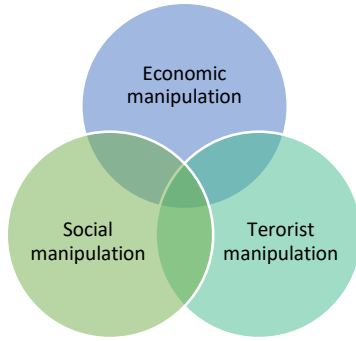

Figure 6. Manipulation forms, shift and interferences (Source: Authors conception)

This case highlights a very real and very worrisome issue: the reaction to this scheme was felt only at the level of the authorities, and Facebook users did not have a prompt reaction to amend these practices. Understanding the power of such manipulation, the mechanisms and the possible consequences, but also the connection between some simple data and the power given by these databases and their use for unfair purposes or the link between the simple postings of a user and very important elements of economic, social, political or safety evolution from the individual to the interstate level cannot be perceived.

Each of us, as Internet users, can help create a safer virtual space by implementing additional measures against cyber-attacks. Max Goodberg believes it is an urgent *"technical literacy of the general public"* by running programs to promote full encryption of internet traffic and to educate society on the safe use of the Internet, but they would not be possible without unified legislation regarding cybernetics crime. He considers that the issues that should be taken into account in the legal provisions should be protection against the sale of personal information on the Internet and the publication of the vulnerabilities of a system.

An expanded ability to respond to computer aggressions and implicitly, to secure virtual environments should take into account a constant education of all users. They should be aware of the dangers they are personally exposed to or the way they are vulnerable to a community, even a state, through cyber-security actions or inactions is at risk. Together with users, developers of software and technological equipment should find the way to have early security alerts, to develop permanently and in a sustained manner the tools to fight against computer aggression attempts in collaboration and cooperation with state institutions and with respect for citizens' rights and freedoms in the virtual and real world environment. We believe it is necessary to create a warning function implemented by online application developers and create a warning registry where users can individually report possible fraud attempts, cyber security incidents, or even non-compliant practices. The law will need to be amended to ensure that there is a global level of non-conforming concepts of how to report these incidents, but also the authorities' response to collaborators with the developers of the risk-creating applications.

The main directions of action should be to modify and adapt the legislation, to the unitary control, supervision and action procedures, supported by a permanent and sustained education of all involved - users, application developer and authorities, the answer to a cyber-attack can only be effective with an active and professional collaboration of the three categories.

The analysis of this phenomenon cannot be contextual in order to be relevant and sufficient, but must have the dynamics of the technological and conceptual evolutions of the users, in a geopolitical and economic context, with a constant and sustained effort of cyber intelligence officers and analysts who have the duty to observe the *"elements of finesse"* of daily changes on the geo-economic-political scene, thus ensuring the *"anchoring to the present"* of the cyber-attack investigation.

References

Beck, U. (1992). *Risk Society: Towards a new modernity*, London: Sage.

Buzan, B. (2014). *Popoarele, statele și teama* [Peoples, states and fear], Bucharest: Cartier.

Dunnigan, J.F. (2010). *Noua amenințare mondială: cyberterorismul [The New World Threat: Cyberthermism],* Bucharest: Curtea Veche.

Goodman, M. (2016). *X-Cyber: viitorul începe azi [X-Cyber: The future begins today],* Bucharest: Rao.

Gordon, L.A. (2016). Cybersecurity risk management: an economics perspective. Retrieved from http:// www.rhsmith.umd.edu/faculty/lgordon.

Grigorescu, A., & Chitescu, R.I. (2017). Information management in digital era – benefits and threats. In *Proceedings of International Conference in Economics and Management, EMAN, 2017, "Global Challenges"* Liublijana, Slovenia.

Grigorescu, A., Chitescu, R.I., & Diaconeasa, A.A. (2016). Risks Management of IT Smart Software and Hardware Controlling Daily Activities. *Imperial Journal of Interdisciplinary Research (IJIR)*, 2(11).

Hardy. C (2016). Cyberspace is officially a war zone – NATO, *Euronews*. Retrieved from http://www.euronews.com/2016/06/15/cyberspace-is-officially-a-war-zone-nato.

Iancu, N. (2010). Securitate și putere în spațiul cibernetic [Security and power in cyberspace]. In Maior, G.C. (ed.), *Un Război al Minții: Intelligence, servicii de informații și cunoaștere strategică în sec. XXI [A War of the Mind: Intelligence, Information Services and Strategic Knowledge in the XXIst Century]* (pp.231-234), Bucharest: RAO.

Marga, A. (2017). *Ordinea viitoare a lumii [The future order of the world]*, Bucharest: Niculescu Publishing House.

Marshall, McL. (1997). *Mass-media sau mediul invizibil [Media or the invisible environment],* Bucharest: Nemira Publishing House.

Radziwill, Y. (2015). *Cyber Attacks and the Exploitable Imperfections of International Law*, Leiden-Boston, MA: Brill Nijhoff, 13-14.

Rohrig, W., & Smeaton, R. (2018). Cyber security and cyber defence in the European Union. Oportunities, synergies and challenges. Retrieved from https://www.eda.europa.eu/docs/default-source/documents/23-27-wolfgang-r%C3%B6hrig-and-j-p-r-smeaton-article.pdf.

Zbuchea, A., Vătămănescu, E.-M., & Pînzaru, F. (2015). M-commerce–Facts and Forecasts. A Comparative Analysis within a Triad Framework: India, Romania, and the United States. *Management Dynamics in the Knowledge Economy*, 4(3), 387-408.

*** FFIEC Handbook Definition of Reputation Risk. Retrieved from http://ithandbook.ffiec.gov/it-booklets/ retail-payment-systems/retail-payment-systemsriskmanagement/reputation-risk.aspx.

*** Governing for Enterprise Security. Retrieved from http://www.cert.org/governance.

*** New York Times, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*

*** Socializing Securely: Using Social Networking Services. Retrieved from http://www.us- cert.gov/reading_room/ safe_social_networking.pdf.

*** Strategia de Securitate Cibernetică a României și Planul de acțiune la nivel național privind implementarea Sistemului Național de Securitate Cibernetică [The Cybernetics Security Strategy of Romania and the National Action Plan on the Implementation of the National Cyber Security System], M.O. nr. 296 / 23.05.2013, H.G. nr. 271/2013).

*** United Nations Office on Drugs and Crime (2012). The use of the Internet for terrorist purposes, United Nations, New York.

*** US-CERT's Protect Your Workplace Posters & Brochure. Retrieved from http://www.us- cert.gov/reading_room/ distributable.html.

*** What Businesses can do to help with cyber security. Retrieved from http://www.staysafeonline.org/sites/default/files/resource_documents/What%20Businesses%20Can%20Do%202011%20Final_0.pdf.

Online sources

BBC - http://news.bbc.co.uk/2/hi/technology/6653119, Accessed February- June 2018.
Cambridge Analytica - https://en.wikipedia.org/wiki/Cambridge_Analytica, accessed April 2018.
Eur-Lex - https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32016L1148&from=RO, accessed March 2018.
MAE - www.mae.ro, accessed February 2018.
Mediafax - http://www.mediafax.ro/externe/scandalul-cambridge-analytica-datele-a-112-000-de-utilizatori-facebook-din-romania-accesate-de-compania-de-consultanta-17125286, accessed at 03.06.2018.
Securitatea informatiilor - http://www.securitatea-informatiilor.ro, Accessedt May 2018.
SRI - http://www.sri.ro, accessed February 2018.