CYBERCRIME IN DIGITAL ERA

Dumitrescu Mihaela-Sorina[1], Marica Mihaela-Emilia[2]
[1) 2) 3)] *Bucharest University of Economic Studies*
E-mail: sorina.dumitrescu16@yahoo.com;
E-mail: avocatmihaelamarica@yahoo.com

Abstract
In Digital Era, businesses and economy become global easily, helped by innovative technologies. Nowadays, mankind depends on Internet, computer and technology. Trade, services, data flows, have crossed the national borders, transforming into a global market that can be easily accessed.
These new technologies like mobile internet, cloud technology or advanced robotics lead to economic growth, transform our lives, our jobs and the traditional business models, but also have a significant disadvantage: cause the evolution of the new type of crime – cybercrime.
On the global scale, crimes are committed by electronic means, being facilitated by technological progress, considering the speed of data transfer or the number of persons connected globally to the network, anytime.
The aim of this article is to present the challenges of Digital Era, the vulnerability to cybercrime, analysing the influence of digital technologies for cybercrime, including illicit financial flows. Also, it will be presented the newest cybercrime tactics and their costs, for explaining the significance of this phenomenon and for identifying ways of minimize its impact.
Technological advance and globalization impose a fast adjustment to changes of the global business environment for succeed, but also for efficiently control cybercrime. The fight for cybercrime should be global, being absolutely necessary the international cooperation of organizations and countries in order to create and to permanently update the legal framework. Consequently, cybersecurity must represent an important objective offered by corporations and government, which must prevent cybercrimes, using technological advance as a benefit.

Keywords
Cybercrime, Digital Era, Globalization, Cybersecurity

JEL Classification
F60, F63, K24

Introduction

The 21th century could be described by the fast evolution of international trade and finance due to digital flows, which allow the transmission of ideas, information and innovation around the world, in the global economy.
Internet represents a global network which instantly connects people and companies all over the world.

Innovation by digital platforms, impose a new way of doing business globally, reducing the cost of international transactions. It has been created markets and communities at the global scale.

According to McKensey 2016 report, small businesses become "micro-multinationals" through digital platforms like eBay, Facebook, Amazon, for connecting worldwide customers and suppliers.

Individuals are actors in globalization process, using digital platforms for learning, finding jobs or building personal networks. 900 million people connect internationally using social media and 360 million use e-commerce outside the national borders (McKensey, 2016).

The whole human life has changed thanks to technology. There are 4388 billion internet users, representing 57% from total population and 3484 billion active social media users, representing 45% from total population (fig. no.1).

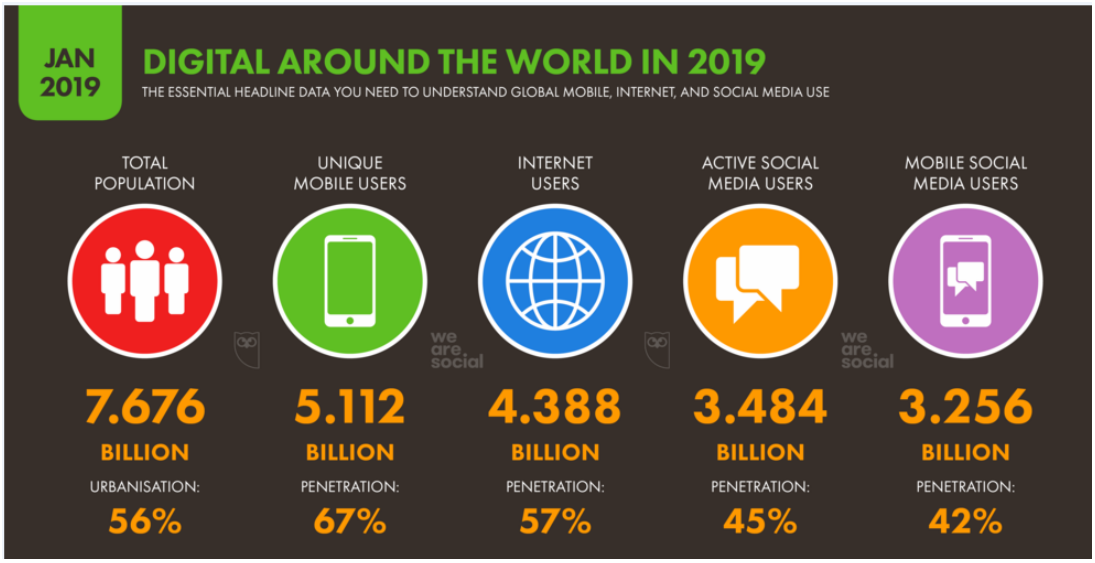

Fig. no. 1 Digital around the world, January 2019
Source: OECDigital 2019. Global Digital Overview.

Over a decade, global GDP raised by 10%, due to global flows which increase productivity. Moreover, countries benefit also from inflows or outflows.

Globalization entered the new Digital Era, defined by data flows which transmit information and innovation. One significant disadvantage of innovation represents the rise of cybercrime, cyber-attacks or cyber espionage.

Digitalization or digital transformation may be described like „the use of technology to radically improve performance of enterprises" (Institute Mines Telecom, 2016). The incomes coming from the digitalization of companies will determine an increase of 3.6% of the GDP by 2020, according to McKinsey predictions.

It has been identified three key ways that technologies could be abused by offenders (Holt, Bossler & Seigfried-Speller, 2015):

1. medium used for communication and for developing subcultures online;
2. mechanism for attracting sensitive resources in order to engage them in crimes;
3. incidental device for facilitating the offense and for providing evidence of criminal activity.

Cybercrime may be define as "a crime committed via Internet, when the target is digital material on a connected device or the aim is to disrupt system or services" (Johnson M., 2016).

The types of cybercrime most discussed in the literature over the last decade are financial theft, hacking, identity fraud, cyberbullying, illicit online networks or markets, child sexual exploitation and the newest ones: digital surveillance and information privacy.
A first objective of this article is to present the concept of Digital Era and its challenges like the increased vulnerability for cybercrime, expanding theoretical frameworks. Secondly, it will be presented the newest cybercrime tactics and its costs for private and public sector in order to highlight the importance of this phenomenon. Another objective of the research is to identify ways of minimizing the impact of cybercrime and preventing it.
Considering the objectives of the article, the research methods used are theoretical research of specialized articles, using quantitative analyse. One step was to understand what implies digitalization in order to identify the challenges of Digital Era.
Also, the concepts cybercrime and cybersecurity and the existing statically data set about these topics were analysed for presenting their importance. Then, the tactics and costs of cybercrime have been explained, using synthesis. Last, using the logical research method, were presented ways of minimizing the impact of cybercrime.

Challenges of Digital Era

According to the 2016 report of Institute Mines-Telecom, due to digitalization, companies must always rethink their business flows, including the interaction with stakeholders in order to face the global competition with new entrants which may use the business model born-global, helping by technology.
Using information technologies, living in "e-everything" world has also disadvantages because crimes committed through electronic means evolve considerable, crossing national or transnational borders, reaching the global scale.
One innovative technology is represented by *big data*. These data are coming from multiple expanding sources, including tracking social media content, website activity or video data. For example, approximately 24000 terabytes is processed every day by Google (Institute Mines Telecom, 2016).
Actually, the key principle of these new technologies is that data are permanently changing. This is the reason why the key success principle for companies is to accept the constant changes and to respond agile as quickly and as efficiently as possible.
Big data creates a network architecture which permanently shares information, allowing companies to identify opportunities, but also offering perspectives for committing cybercrimes using these data.
Likewise, in the Digital Era we are speaking about the *Internet of things*. It refers “to the use of sensors, actuators, and data communications technology built into physical objects—from roadways to pacemakers—that enable those objects to be tracked, coordinated, or controlled across a data network or the Internet” (McKinsey Global Institute, 2013).
Nowadays, devices, machinery or infrastructure have included networked sensors that allow monitoring their environment or reporting their status. Moreover, these devices receive instructions and action responding to the instruction received.
The number of devices which are now connected worldwide to internet exceeds nine billion, including smartphones and computers. In the next decade, it is expected that the number of these devices will reach one trillion.
The estimated impact of the potential of Internet of Things is between $2.7 trillion and $6.2 trillion by 2025 (McKinsey Global Institute, 2013).
The challenges of this innovative technology are about privacy and security. Involving data connection for allowing remote machines to respond, these may be hacked by terrorists or criminals. All data sets collected by monitoring could be abused. Moreover, the home controller applications can be debated concerning autonomy and privacy.

Network reliability and data represent important concerns because it may be the targets of terrorists, criminals or hackers. For example, if the electric system's network and sensors will be controlled by terrorists, the attack will be threatening.
Internet of Things devices represent nowadays "the biggest technology crime driver" (Herjavec Group 2019 Official Annual Cybercrime Report).

Costs and new tactics of cybercrime
The evolution of cybercrime is similar to the evolution of street crime, due to population growth. Nowadays we have an increase of internet users. Cybercrime creates huge damages for private and public sector, costing 6 trillion USD, according to Herjavec Group 2019 Official Annual Cybercrime Report. The global expenses for cybersecurity will cumulatively exceed 1 trillion USD for 2017-2021, citing the same report.
For example, according to Alvarez Technology Group, in US, a hacker tries to attack a computer connected to internet every 39 seconds. Researchers from University of Maryland discovered that one of three Americans has already been target of a cyber-attack.
Concerning the typology of cybercrime, David Wall synthesises four types of cybercrime (Stratton, 2017):

- cyber-trespass which supposes system hacking, malware – malicious software or online attacks through unauthorised access to a network, computer system or data source;
- cyber- theft which includes financial or data thefts, electronic piracy or intellectual property rights thefts, being facilitated through malware, identity fraud or fraudulent scams;
- cyber-porn and obscenity which includes child sexual exploitation and grooming materials;
- cyber-violence, which involves harms like cyberbullying, cyberstalking or acts of terror caused to others (e.g. sharing instructions for manufacture explosives or other weaponry).

A new trend for criminals is to abuse cryptocurrencies for criminal activities. According to Europol, cryptocurrency users or intermediaries represent victims of cybercrimes. The target of traditional cyber-attacks - traditional financial instruments is now replaced by users of cryptocurrencies.
Hacking attack or personal data theft affects currency exchangers, miners and cryptocurrency wallet holders (Europol - Internet Organised Crime Threat Assessment Report, 2018).
Having new Mac and Windows malware, using mining APIs or server-side attacks, criminals continue to try this type of attack (Malware Bytes - Cybercrime tactics and techniques: Q2, 2018).
Cryptojacking represents a cybercrime trend, involving the exploitation of miners who use processing power for mining cryptocurrencies.
Cybercriminals hack websites for exploiting visitor's systems. Like hacking, cryptomining malware has the same effect, crippling the victims system through monopolising the processing power.
This happens by a script running in an website, through the browser of visitor, allowing the website to use the processing power of visitor for mining cryptocurrencies, during his visit.

Also, terrorists use cryptocurrencies for fundraising. According to Europol, in November 2017, the website Akhbar al-Muslimin requested for Bitcoin donations. First, the link redirected to an external payment site in Bitcoin.
Then, the link redirected to a page that created Bitcoin addresses, existing the option to donate outside the page, including malware into the website for mining, fact that confirms technical sophistication.

Cryptocurrencies are used for money laundering, being decentralized and not regulated. For example, small amounts could be traded through more cryptocurrency accounts, owned by the same person or by a network for fraudulent purposes or it could be used multiple transactions of cryptocurrency for cash through individuals, avoiding exchanges which may apply Know Your Customer policy.
Another target for cybercriminals is represented by the global phenomenon of social media networks (e.g. Facebook, Instagram, Twitter). Being free, billions of users communicate through these networks, a part of them being addicted to post a lot of personal information, almost living virtually. Even though social media represents an advantage of Digital Era, these networks has a huge potential for cyber criminals.
First of all, cybercriminals may attack for having access at personal information like name, date of birth, date about family and friends, address, telephone number. LinkedIn was hacked and it has been exposed 6.5 million users and passwords (Johnson, 2016**).**
Another vulnerability of social media is the identity verification. It could be easily created fake accounts, using attractive photos in order to harass or to target potential victims. Criminals could locate, identify and investigate them.
For example, scammers use Twitter for coordinating spam campaigns which promote fake tech support (fig no. 2).

Fig. no. 2 Fake malwarebytes number on Twitter
Source: Malware Bytes - Cybercrime tactics and techniques: Q2 2018

Also, there is a reputational risk that can be quickly affected by a negative message which is massive shared. For example, 'Twitter Storms' which involved the target of a brand and thousands of critical messages written by users and read by a lot of consumers worldwide in few minutes (Johnson, 2016**)**.
Moreover, social media networks are abused by terrorist groups, sharing propaganda photos and videos in order to organise attacks, to fundraise and to recruit, apparently using legitimate the services.
Another important aspect is the fact that children have easily access to social media networks, on their smartphones, being unmonitored and represent potential victims of child sex offenders.
Although tactics for cybercrime evolve with new technologies, according to Europol, social engineering is the most used method. 40% of EU Member States performs investigations for phishing cases. In March 2018, 20 suspects were arrested in Italy and Romania for banking fraud of 1 million euro coming from customers of two important banking institutions, after a

two year cybercrime investigation (Europol - Internet Organised Crime Threat Assessment 2018).
Phishing via email is the most used form, followed by vishing (used via telephone) and by smishing (used via SMS). Social engineering is used by criminals in order to get personal data, to steal identities, to hijack accounts or to initiate payments on the stolen identity account. Also, they may convince victims to transfer money or to share personal data.

Ways of minimizing the cybercrime's impact

The fight against cybercrime should be both at public and private level. For adequate policies regarding cybersecurity and for allocating the right budget, reliable data are necessary for governments in order to have measures cost-effective. More detailed, money allocated for preventing and detecting cybercrime should be compensated by a decrease in losses coming from offences (Armin et al., 2016).
International cooperation for setting directives, conventions and guidelines is absolutely necessary in order to prevent, combat, investigate and fight against cybercrime.
Cybercriminals may be everywhere, and it will be necessary that any jurisdiction may be compliant for locating, preserving evidence, investigating and for judging fair this type of crime, respecting the human rights standards (Casey, 2011).
Companies should invest in the education of the personnel in order to understand the spread of cybercrime and how to protect the cybersecurity of the company. The amount spent globally for the trainings of employees is estimated at $10 billion, until 2027 (Herjavec Group 2019 Official Annual Cybercrime Report). It's essentially that employees of a company should know how to recognize and defend cyber attacks.
Private and public sector should invest for research and for solutions which prevent cyber attacks, because just detecting existing threats is not enough. They should anticipate and respond to the newest threats before the fulfilment.
Top cybersecurity companies innovate by creating products and services which fight against cybercrime. They are known as managed security providers and takes risks for organizations worldwide.
For fighting against social engineering, the most used method by cybercriminals, it should also be invested in the education of technology users through awareness and prevention campaigns. The campaigns may be targeted to the features of potential victims (teenagers or adults).
These kind of campaigns should also be apply to users of cryptocurrencies for avoiding being victims of cryptojacking.
Last, but not least, cybercrime investigators should be specialized in investigating cryptocurrencies.

Conclusions

One important disadvantage of the new Digital Era represents the rise of cybercrime, cyber-attacks or cyber espionage on the global scale, but also through innovation and last technologies, cybersecurity companies should create products and services which successfully fight against cybercrime.
Cybercrime creates huge damages for private and public sector, evolving with new technologies. The target of traditional cyber-attacks - traditional financial instruments is now replaced by users of cryptocurrencies.
Nowadays, companies should accept the constant changes and should respond agile to them as quickly and as efficiently as possible. They should invest in cybersecurity for preventing cybercrimes, including training for employees who should know to recognize and defend cyber-attacks.

States should invest in cybersecurity, including trainings for investigative tools of the newest technology in order to anticipate the cybercriminals' moves or awareness and prevention campaigns for the users of the new technologies products like social media, cryptocurrency or Internet of things.
Moreover, international cooperation for setting directives, conventions and guidelines is absolutely necessary in order to prevent, combat, investigate and fight against cybercrime.
Until countries' criminal laws will be harmonized, new cooperation procedures will be developed, based on advanced technology and advance study of these technologies, cybercrime will mostly win.
Considering the new technologies detailed, the tactics of cybercriminals applied to these technologies explained, some solution for fighting against cybercrime, this research could represent a starting point for the future regulatory framework.

References

<https://resources.malwarebytes.com/files/2018/07/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q2-2018.pdf> [Accesed 10 April 2019].

<https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf> [Accesed 10 April 2019].

Armin, J., Thompson, B., and Kijewski, P., 2016. *Cybercrime economic costs: No measure no solution*. Cham: Springer.

Casey, E., 2011. *Digital evidence and computer crime: Forensic science, computers, and the internet*. Walthham: Academic press.

Europol - *Internet Organised Crime Threat Assessment 2018.* [online] Available at: <https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018> [Accesed 10 April 2019]

Herjavec Group, 2019. *Official Annual Cybercrime Report.* [online] Available at:

Holt, T.J., Bossler, A.M., & Seigfried-Spellar, K.C., 2015. *Cybercrime and digital forensics: An introduction.* London: Routledge.

Institute Mines-Telecom, 2016. *Companies of the future. The issues of digital transformation.* [online] Available at: <https://portail.telecom-bretagne.eu/publi/public/fic_download.jsp?id=67447> [Accesed 2 April 2019].

Johnson, M., 2016. *Cyber crime, security and digital intelligence*. New York: Routledge.

Malware Bytes, 2018. *Cybercrime tactics and techniques: Q2 2018.* [online] Available at:

Manyika, J., Lund, S., Bughin, J., Woetzel, J., Stamenov, K., Dhingra, D., 2016. *Digital Globalization: The New Era of Global Flows*. New York: McKinsey Global Institute. [online] Available at: <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows> [Accessed 1 April 2019].

McKinsey Global Institute, 2013. Disruptive technologies: Advances that will transform life, business, and the global economy. *McKensie Quarterly*, *45*(May), pp.1-176. [online] Available at: <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies> [Accessed 1 April 2019]

OECDigital, 2019. *Global Digital Overview.* [online] Available at: <https://datareportal.com/reports/digital-2019-global-digital-overview> [Accessed 1 April 2019].

Stratton, G., Powell, A., and Cameron, R., 2017. Crime and justice in digital society: towards a 'Digital Criminology'?. *International Journal for Crime, Justice and Social Democracy*, 6(2), pp 17-33. [online]