DOI: 10.5281/zenodo.6396274

MANAGEMENT OF OPEN SOURCE INFORMATION IN THE MANAGEMENT OF CURRENT CYBER THREATS AND WAYS TO FIGHT FRAUD AT FINANCIAL COMPANIES

Cosmin Sandu BĂDELE
Expert within the Ministry of Internal Affairs,
PhD Student, Valahia University of Targoviste, Romania
cosmin.badele.cb@gmail.com

Lucian IVAN, PhD
Expert within the Ministry of Internal Affairs, Romania
ivan.lucian2@gmail.com

Abstract: *The multiple ways of accessing the virtual environment are changing, those who access the Internet are changing and the role that the Internet plays in our lives. In 1995, only 1% of the world's population had access to the Internet. There are now over 4 billion Internet users worldwide and this number is growing. Over time, cyberspace has generated a series of controversies, starting from the difficulty of being given a unanimously accepted definition. At both state and institutional levels, an attempt was made to define this new concept, the results being different and adapted to the specifics of each organization. Thus, in the Cyber Security Strategy of Canada, cyberspace is presented as "the electronic world generated by the interconnection of computer networks", and in the Cyber Security Strategy of the United Kingdom of Great Britain and Northern Ireland, it is defined as "An interactive domain of digital networks that store, modify and transport data".*

Keywords: *cyberspace, artificial intelligence (AI), Big Data, COVID-19 pandemic, corporate governance, Open Source Intelligence OSINT, economic perspectives, OSINT type analysis*

JEL Classification: *F3, O3*

1. Introduction

Cyber threats have recently become a phenomenon that can be seen in societies previously known as "developing countries", which are entering the cyber bubble due to the extremely rapid development of wireless telephony networks. *But the movement is even more evident in developed societies, where cyber coverage is much more significant and much faster*.

Digital systems have become very complex so that a cyber attack cannot be detected and prevented in time, which is why all states are currently preparing and studying such illicit activities through the permanent development of methods to prevent possible attacks.

Within the Romanian Cyber Security Strategy (2013), the cyberspace is characterized by "lack of borders, dynamism and anonymity, generating opportunities for the development of the information society based on knowledge, but also risks to its functioning", with implications both individually, as well as the state.

At the level of the **International Organization for Standardization** (ISO), cyberspace is dealt with extensively in the ISO 27032 standard, relating to cybersecurity. In the document, cyberspace is defined as "a complex environment, resulting from the interaction between people, software products and services through the Internet and computer networks."

Artificial intelligence (AI) is the ability of a machine to mimic human functions, such as reasoning, learning, planning, and creativity. Thus, artificial intelligence allows technical systems to perceive the environment in which they operate, to process this perception and to solve problems / equations, acting only in order to achieve a specific goal. The computer / machine receives the relatively prepared data (collected, processed, analyzed, integrated, evaluated) through its own sensors (eg video camera), which it reprocesses, reacting in accordance with the predefined purposes.

AI systems (software or hardware) are able to adapt, to a certain extent, their behavior, analyzing the effects of previous actions and operating autonomously. They also act in physical or digital environments, thus perceiving them according to the data received, the interpretation of the structured or unstructured data received, in full resonance with the knowledge or as a result of processing the information obtained from this data to decide which is best. course to be followed according to predefined goals (Stegaroiu et al., 2014).

AI systems can use symbolic algorithms or learn certain numerical models on their own, and can adapt their behavior by analyzing the effects that their previous actions have on the environment in which they operate. Thus, Machine Learning (ML) is a subdomain of AI, in which specific algorithms

learn how to continuously develop certain patterns from a data set to determine the actions to be taken to fulfill a certain purpose.

In this context, recently, criminal entities and organized crime groups have integrated new AI technologies into their modes of operation, which has led to constant changes in the global crime landscape, thus creating significant threats to law enforcement authorities in and cyber security in the alternative.

We must also reiterate that this new space cannot be reduced to computers alone. Cyberspace can be described according to a triple layered model: a hardware layer (because, despite the emergence of "virtuality", cyberspace is based on an extremely dense and often unnoticed physical infrastructure); a logical layer (the computer itself); and a semantic layer, often overlooked, but extremely important (Kempf, 2012).

On the one hand, big data is the key to innovation and the creation of solutions to complex social and economic problems. On the other hand, the exploitation of personal data on an increasingly large scale raises previously unsuspected risks, from diminishing the personal autonomy of citizens and consumers to undermining the organization of democracies and competitive markets. In this context, the importance of cultivating the thematic sensitivity of the public and developing the skills of future experts who will create and implement strategies for the use and security of data increases (ACS Advanced Cyber Security, n.d.).

2. Concrete threats of Artificial Intelligence in the context of their use by criminal entities

Cybersecurity specialists have identified 3 main areas in which various attacks can be initiated that can make the processes related to artificial intelligence vulnerable, namely:

1. **Contradictory examples** - attempts by the attacker to confuse the AI system by incorrectly classifying the data received, thus being able to cause the victim to make decisions based on erroneous data.

2. **Trojan malware** - modifies the system during the learning stage, also producing an erroneous classification of data. Model reversal is a process by which the attacker breaks down (by reverse engineering) the AI system in an attempt to identify the information used to create the model / algorithm.

3. **IoT (Internet of Things) industry** - is booming, offering unlimited opportunities for criminal entities to:

- Network attacks - involve compromising IoT devices through the network to which they are connected;
- Distributed Denial of Service (DDoS) attacks - the attacker uses bot networks to send a lot of messages to a network that has IoT devices.

Thus, it is overloaded, making all connected systems unavailable. DDoS attacks on IoT devices work similarly to those carried out against any other type of device;

- Radio frequency blocking attacks - these affect wirelessly connected IoT devices, causing them to lose connection or reduce their ability to communicate on the network. Such attacks are most common on IoT alarm systems.

On the other hand, IT&C infrastructures in smart cities are attractive to hostile cyber actors, who can exploit cybersecurity vulnerabilities to affect or make unavailable public services provided. Thus, the theft of personal data and the one aimed at the identity of a person are constant operations of criminal entities, which take over financial data related to the payment system implemented in electric vehicle charging stations, in order to subsequently carry out fraudulent transactions. In the same context, data theft is also associated with the activities of taking control of electronic / electrical devices, the attacker compromising smart meters, including for the purpose of energy theft.

Also, other types of attacks by using AI can follow the interception, redirection or interruption of communications between two systems (man-in-the-middle), when the criminal entity aims to make unavailable the water filtration system by intercepting the communication channel used by this in order to manipulate the transmitted data and subsequently to generate erroneous orders.

Other current and future scenarios related to the use of artificial intelligence for illicit purposes may result from the widespread presence of fraud schemes in the field of social engineering, those related to the generation of false content in the online environment (eg high quality phishing and spam emails written in lesser known languages), activities to filter out a certain type of content / data from documents belonging to individuals / legal entities, those related to the use of robocalling operations v2.0 , corruption of facial recognition systems present in the high technologies of autonomous cars, drones, as well as other land and air electric vehicles, manipulation of stock prices on stock exchanges, as well as transactions carried out at the level of financial-banking institutions and IFN as well as intentions to avoid detection and recognition systems (installed at level i public institutions, in various security areas, banks, etc.).

3. Perspectives of the use of Artificial Intelligence in Romania

The National Defense Strategy stipulates that 5G networks will support multiple communications applications and information technology implemented, including at the level of critical infrastructures, so that the integrity, confidentiality and availability of telecommunications will be important issues of national security.

Some technological vulnerabilities of 5G networks could be exploited through artificial intelligence to compromise, by state or non-state entities, interdependent infrastructures, with the risk of causing severe damage to the national security architecture.

Ensuring the protection of communications infrastructures and information technology with critical values for national security, as well as the knowledge, prevention and countering of cyber threats carried out on them by strategically motivated actors, extremist-terrorist ideology or financial interests, are important objectives to be taken into account by national law enforcement authorities.

Under the impetus of technological developments, in the medium term, the Romanian space will become an area of intense manifestation of interconnected risks and threats, which will increase the complexity and volatility of the national security environment. These trends are now accentuated by the increasing relevance of non-state actors and the proliferation / resizing of cross-border threats, such as terrorism, hacktivism and organized crime in the European space.

The increasing use of artificial intelligence in current technologies, online payments, cryptocurrency transactions, while the growing interest in BigData, IoT, quantum technology and the hidden Internet (DarkWeb), outlines the prospects for their use in organized crime, cybercrime, hacktivist, terrorist or extremist activities, which are not excluded even in offensive operations coordinated by state entities related to the interests of non-state actors.

In practice, the low level of cyber security of national IT&C infrastructures, including as a result of the procedural technological vulnerabilities of the infrastructures owned by internet / communications operators, will continue to maintain the aforementioned risks.

4. The economic perspective

The increase in economic power and the influence of the big technology giants is easy to notice in synthetic indicators, such as turnover, number of users or the share they occupy in a given market. All the more remarkable is the consolidation of their economic power during the global crisis triggered by the COVID-19 pandemic.

Technology platforms create markets that significant proportions of the world's population play as bidders or consumers - from information markets created by search engines like Google, Bing or Yahoo, to digital application markets like Google Play or App Store, to markets retail markets such as Amazon Marketplace, real estate markets such as Airbnb or Booking.

com, transportation markets such as Uber or Lyft, as well as crowdsourcing or microjobs labor markets such as Amazon Mechanical Turk or Yandex.Toloka.

5. OSINT Data Management (Open Source Intelligence) in current risk management

The resources at the level of each organization are limited, it is necessary to achieve an efficient and effective management of the activities carried out, based on the results and conclusions provided by the types of information analysis (OSINT), in order to meet the organization's objectives. (This activity it is very important taking into account budgetary restrictions, being necessary planning and correct allocation of available resources.) Thus, by adapting and integrating existing analytical techniques, it will be possible to correctly anticipate political, economic, social, technological and security developments, which will allow managers to have correct and efficient, scientifically based measures that allow them to maximize results. , simultaneously with the efficiency of the resources used (Ivan, 2018).

OSINT (Open Source Intelligence) is a component of the "intelligence" process and represents, in essence, the information carefully filtered, selected, analyzed and presented to the beneficiaries in a timely manner, obtained exclusively from open sources. With the information age and the development of global communication, open sources have also received increased attention from experts in the field of national security.

OSINT-type analysis is an important strategic capability by providing an overview of the context and threats to various critical / important issues, so that decision-makers can establish and implement long-term policies.

Equally important, open source analysis has the advantage of presenting, together with possible immediate effects, a perspective view of the phenomena that are the subject of the decision-makers' activity, which will allow them to amplify their capacity to prevent and respond to possible crises. appeared.

On the other hand, OSINT products contribute to the analysis of multi-source intelligence (internal sources, open sources), by identifying elements necessary to understand the general context, by providing information that can not always be obtained from classified sources and by facilitating access to certain types of expertise from different areas of interest.

At the same time, from an analytical point of view, it is considered that at the level of each organization, managers are obliged to make decisions regarding the organization of the activity, with or without analytical support. However, in order to make scientifically sound decisions, the manager needs the information analyst and an analytical product that contains correct

information, presented in a coherent, clear and explicit manner and, perhaps most importantly, in a timely manner (Ivan, 2018).

6. Recommendations for the prevention and limitation of the effects of cyber attacks at the level of public institutions in Romania

The online environment, through its resources and hardware / software components, is used for the transfer of information between all entities, from companies, organizations and agencies to end users. Cyber attacks are not just physical environment - mobile equipment, computer systems, smartphones, etc. - but also the logical one - operating systems, applications, e-mail, information transfers between companies or cloud operations.

Most incidents (hardware and software) in public institutions in Romania refer to fixed equipment (38%), followed by e-mail (25%) and Web applications (17%) (Mihai and Ciuchi, 2017).

Cyber attacks have an increasing trend in terms of both volume and complexity, leading to increased risk, additional costs and potential losses for public / private companies. Institutions operating in the financial and capital markets are the most targeted targets being attractive due to the volume of financial transactions and the sensitivity of the data circulated, such as information about customers / suppliers, databases, business plans and confidential strategies / investments, intellectual property (trading algorithms), customer portfolio or list of users and passwords.

Good cyber security practices for public institutions in Romania that aim to establish and maintain a robust and well-implemented awareness of cyber security and ensure that end-users are aware of the importance of protecting sensitive information and the risks of mismanagement of information.

1. Monitoring applications that have access to data

Available applications provide an organization with the tools it needs to function and be productive, with the risk of jeopardizing sensitive data. Protecting information involves installing firewalls and building the infrastructure around the data to be protected. The configuration of firewalls must be done carefully, access rights being granted only to applications entitled to read or write confidential data.

2. Creating specific access controls

By creating specific access controls for users, they can limit access only to the systems they need for service tasks, thus limiting the exposure of sensitive data.

3. Collection of detailed logs

Full logging of what is happening in the company's network systems - both for security and troubleshooting purposes - detailed logs and complete reports must be collected. This is especially true for applications that do not have registrations so that any security breaches created by these applications can be identified and remedied.

4. Education and training of users

Users are usually the weakest link in terms of security information, and this risk can be limited by educating them on cyber security best practices. The training should include how to recognize a phishing email, create strong passwords and avoid dangerous applications, keep information inside the company and any other risks related to cyber security.

5. Clearly define usage policies for new employees

In order to strengthen and clarify the education provided to users, employment should be highlighted clearly the requirements and expectations that the company has in terms of IT security (employment contracts must provide for sections which clearly define these requirements security).

6. Monitoring user activity

While well-trained users are the first line of security, it is needed technology as the last line of defense. By monitoring the activity of users it is checked whether their actions comply with good security practices.

7. Conclusions

Against the background of the exponential evolution of artificial intelligence with direct applicability in the field of IT&C technologies, it is essential to increase the level of concern that national authorities should give to cyber security, and thorough training is needed to ensure a high level of awareness regarding the cyber security risks and threats to which the various entities are exposed, both at individual level and at organizational / institutional level.

The resources at the level of each organization are limited, it is necessary to achieve an efficient and effective management of the activities carried out, based on the results and conclusions provided by the types of information analysis (OSINT), in order to meet the organization's objectives.

Thus, by adapting and integrating existing analytical techniques, it will be possible to correctly anticipate political, economic, social, technological and security developments, which will allow managers to have correct and efficient, scientifically based measures that allow them to maximize results, simultaneously with the efficiency of the resources used (Ivan, 2018).

Cyber security is considered as the constant need to see the continuous evolution of the relevant regulations encountered in the virtual environment.

8. Proposals

In this context, at the level of national authorities it is appropriate that:

- AI should be exploited by law enforcement institutions to their full potential in terms of the beneficial effects that this technology can have in preventing and combating crime, while ensuring robust, legal, ethical and technical operating principles;
- AI innovation is constantly promoted including by supporting good practices in the field (ENISA, EUROPOL, INTERPOL, UNICRI);
- enhancing cyber resilience in a timely manner to prevent possible use of AI for illicit purposes, including by mapping threats in this area;
- the use of risk management to be a constant activity at the level of public institutions to classify the various threats resulting from current and future uses and the misuse of AI;
- the development of the legal and technological framework aimed at the protection of AI systems to be carried out only in carefully controlled security environments (on the principle of the sandbag);
- encourage the adoption, at national level, of an individual-centered IA approach (including through prevention campaigns), as well as sets of cybersecurity standards for this type of technology;
- to encourage and develop the interest of law enforcement authorities in their ongoing preparation to limit the developments that cybercrime constantly generates;
- to initiate public-private partnerships, including by co-opting international experts, in order to know the current and future developments of the field of AI.

Selective Bibliography

Advanced Cyber Security. (n.d.). Faculty of Automatic Control and Computers, University Politehnica of Bucharest. Available online at https://acs.pub.ro/admitere/masterat/ and http://acs.pub.ro/doc/master/ro/short_description/SAS-short-ro.pdf.

Apel, K. O. (1994). *The Ethics of Discussion*, CERF.

Baltzan, P., and Phillips, A. 2008. *Business driven information systems*. New York: McGraw-Hill Irwin.

Bentham, J. (1789). *Introduction to the Principles of Morality and Legislation*. London.

Brey, P. A. E. (2012). Anticipating ethical issues in emerging IT. *Ethics and Information Technology*, 14(4), pp. 305–317.

Clausewitz, Carl von. (2018). *On War*. Publisher: Digireads.com.

Courdarcher, M. (2008). *Kant: pas à pas*. Ellipses Marketing edition, October 22, 2008.

Debar, H. (2018). Intelligence artificielle, risque ou opportunité pour les cyber-défenseurs? *Telecom*, Number 190, Oct. 2018.

Desai, M., Von Der Embse, T.J. and Ofori-Brobbey, K. (2008). Information technology and electronic information: an ethical dilemma. *SAM Advanced Management Journal*, 2008, p. 18.

Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. https://www.europeansources.info/record/proposal-for-a-directive-of-the-european-parliament-and-of-the-council-concerning-measures-to-ensure-a-high-common-level-of-network-and-information-security-across-the-union/.

Coordinated Vulnerability Disclosure - an essential component of cyber security, CERT-RO, https://cert.ro/citeste/divulgarea-coordonat-a-vulnerabilitilor-component-esen-ial-a-securit-ii-cibernetice.

European Commission. (2019). Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising.

European Parliament News. (2021). What is artificial intelligence and how is it used? https://www.europarl.europa.eu/news/ro/headlines/society/20200827STO85804/ce-este-inteligenta-artificiala-si-cum-este-utilizata.

Herzog, L. (2017). *Markets.* The Stanford Encyclopedia of Philosophy.

Intelligence.SRI. (2020). Virtual projections in the real world. https://intelligence.sri.ro/proiectii-virtuale-lumea-reala.

Ivan, L. (2018). *Managementul analizei informaţiilor.* Târgovişte: Bibliotheca.

Jugastru, C. (2017). Proceduri și autorități în noul drept european al protecției datelor cu caracter personal. *Revista Universul Juridic* nr. 6, iunie 2017, pp. 112-129.

Kempf, O. (2012). *Strategia cibernetică*. Paris: Economica.

Malicious uses and abuses of artificial intelligence (2020) – United Nations Interregional Crime and Justice Research Institute.

Mihai, I.C., Ciuchi, C., and Petrica, G. (2017). „*Current Challenges in the Field of Cybersecurity – The Impact And Romania's Contribution to the Field*, Strategy And Policy Studies SPOS 2017 – No. 4.

Ministerul Afacerilor Interne, Centrul de Coordonare a Protecției Infrastructurilor Critice, http://ccpic.mai.gov.ro/legislatie.html.

Miroiu, A. (2001). *Introducere în analiza politicilor publice*. Bucharest: Punct Publishing House.

Mocanu, M. (2020). *Artificial intelligence in intelligence and more*. Defence & Security Monitor Romania. https://monitorulapararii.ro/inteligenta-artificiala-in-intelligence-si-nu-numai-1-28414.

Nadler, J. and D. N. Cicilline. (2020). Investigation of Competition in Digital Markets. Majority Staff Report and Recommendations.

National Institute of Standards and Technology (NIST). (2002). Special Publication 800-30: Risk Management Guide for Information Technology Systems, July 2002.

Romanian Cyber Security Strategy. (2013). Romanian Government Decision 271/2013, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/roncss.pdf.

Stegaroiu, I., Radu, F., & Radu, V. (2014). Convergence and divergence between accounting and taxation in Romania. In International Multidisciplinary Scientific Conferences on Social Sciences and Arts SGEM 2014 (pp. 137-144).

Vasilache A. (2020). HotNews.ro. https://economie.hotnews.ro/stiri-telecom-24036600-strategia-nationala-de-aparare-a-tarii-atac-cibernetic-criminalitate-informatica-securitate-retele-5g.htm.