[Volume 9, Issue 2(22), 2020]

ARTIFICIAL INTELLIGENCE AND CYBER SECURITY – FACE TO FACE WITH CYBER ATTACK – A MALTESE CASE OF RISK MANAGEMENT APPROACH

Narcisa Roxana MOŞTEANU
American University of Malta, BML 1013, Malta
narcisamosteanu@yahoo.com
Kevin GALEA
IT Business Intelligence Department, BML 1013, Malta
kevin.galea@gmail.com

Abstract
The work paper aims to underline the benefits of using Artificial Intelligence to improve the business productivity, and in the same time to address awareness in order to overcome fear in exploring new technology, because of cyber-attacks. How vulnerable are businesses to computerization? 100%. Internet is a virtual space available for everyone. Storing data on any device that can be connected to the internet can become vulnerable in any given second. This article comes to show how we can use cybersecurity to protect our business, presenting in the same time cases of risk management form Malta.

Key words: *cybersecurity, cyberattack, artificial intelligence, risk management, banking system.*

JEL Classification: *G41, M15, O3*

I. INTRODUCTION

It is a fact now that Artificial Intelligence helps companies to reduce operating costs, boost productivity and deliver the ultimate customer experience. Artificial Intelligence is one of these game-changing tools for business. However, many companies are still shy in integrating and using Artificial Intelligence and new technologies for various reasons, mainly due lack of knowledge, and/or lack of resources (Marketingcharts, 2017). For those companies which started to use Artificial Intelligence the business process and financial results already improved. These new technologies helped them. However, in the same time, Artificial Intelligence imply to have a centralized database for clients, for individual and business information with same characteristics. This is helpful on one hand, but on the other hand can be a huge exposure for cyberattack. In this respect, along with Artificial Intelligence, businesses have to implement and use cybersecurity tools. Cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. In other words, risk management includes now another category: cyber-attack, which can be protected through cybersecurity. The antidote for this type of risk is cybersecurity, which comes as a practice of protecting systems, networks, and programs from digital attacks.

II. RESEARCH METHODOLOGY

The present work paper is an exploratory research, qualitative, based on investigative techniques. It is a fundamental research, which aims to identify the threat of using artificial intelligence for business, being possible to be vulnerable by cyberattack, and give possible solutions to manage the cyber risk. The investigation starts from Maltese companies, which are using or willing to use Artificial Intelligence in their daily operations and continue with cases about cyber-attack and their financial losses. The research paper comes to present how cyber security can use artificial intelligence to create a safer business environment.

III. LITERATURE REVIEW

History of Cyber security

Cyber security has emerged as a response to technological innovations and their involvement in changing the approach of economic, geographical and political development (Hansen, Nissenbaum, 2009). The term CYBER SECURITY is often used interchangeably with the term INFORMATION SECURITY *(VON SOLMS, VON NIEKERK, 2013)*. The Cyber security history issues begins in 1970s with a project called *The Advanced Research project Agency Network* (ARPANET). The program appeared inside the project and was named *Creeper* fallowing the printed massages left behind: *I'm the Creeper: Catch m if you can* (Murphey, 2019). That was the world's first hacker. Once the internet starts to be open to the public (1990s), more and more people started to use computers, and add their personal information on them and sharing it on the internet too. This was the time when organized crime entities took this opportunity get more financial resources, stealing data and money form individual, businesses and governments. By mid of 1990s, in order to protect the people and the government against all this whipped, NSA create the first *firewall*.

Over the year, due to the continue improving the technologies, hacking become more complicated. New and new cases of cyber-attack risen, such as: *Snowden & The NSA, 2013* (a former CIA copied and leaked classified information from NSA); *Yahoo 2013-2014* (hackers broke into Yahoo, jeopardizing the accounts and personal information of all their 3 million users); *WannaCry, 2017* (known as *ransomworm* – targeted computers running the Microsoft Windows operating systems and demanded ransom payments in the Bitcoin cryptocurrency), (Murphey, 2019). All this was possible because, while there are significant advances in information technology and infrastructure which offer new opportunities, cyberspace is still far from completely secured (Shiva et. al., 2010).

In the present time, cyber-attack can appear as: *Phishing* (it is the practice of sending fraudulent emails that resemble emails from reputable sources, with the scope to steal sensitive personal data); *Ransomware* (it is a practice to extort money by blocking access to files or the computer system until the ransom is paid); *Malware* aims to gain unauthorized access or to cause damage to a computer; *Social engineering* (which comes a tactic that adversaries use to trick you into revealing sensitive information). In the current life, there are also other two types of cyber-attack, used for obtaining access to the system, like: *Man-in-the-Middle* (which is a cyber-attack where the data to be exchanged between communicating parties is compromised by an attacker), and *Brute Force* (where the attacker tries guessing system access credentials like passwords). With the advances in information technology, criminals are using cyberspace to commit numerous cyber-crimes. Anything which is using IT infrastructure is highly vulnerable to intrusions and other threats. Physical devices and human intervention are not sufficient for monitoring and protection of these infrastructures; hence, there is a need for more sophisticated cyber defense systems that need to be flexible, adaptable and robust, and able to detect a wide variety of threats and make intelligent real-time decisions (Dilek et. Al., 2015). During the journey of this present research, we consider that Artificial Intelligence can and will play an important role in cybercrime detection and prevention.

History of Artificial Intelligence

The history of *Artificial Intelligence* started around 100 years ago, in 1920, when Czech writer Karel Čapek published a science-fiction piece called Rossumovi Universal Robots, which introduced the word *robot*, a humanoid *machine* which work for people (Turing, 1950). In 1950, Alan Turing (mathematician, computer scientist, logician and cryptanalyst) asked himself (publicly) *Can machines think?* (Koistinen, 2016), and from this question the *Artificial Intelligence* started its journey. Turing continued to develop three distinct strategies that might be considered capable of reaching a thinking machine: through programming; *ab initio* of machine learning (Koistinen, 2016); and, knowledge management (using logic, probabilities, learning skills). As a result of discoveries in neurology, information theory and cybernetics in the same time, researches, and with them Alan Turing, created the idea that it is possible to build an *electronic brain*. Turing introduced his widely known Turing Test, which was an attempt to define machines' intelligence. Now, the *Artificial Intelligent* market (hardware and software) has reached billions of dollars. This all is possible by exploring *Big Data*, using quicker computers and advancements in machine learning techniques.

The digital revolution is changing the way of living, working and communicating. New technologies have a major impact on the surrounding world with the continued improvement of digital technologies. Artificial Intelligence is one of them. It is a recent technological breakthrough, which, combined with industrial technology, it helps overcoming many human errors, exceeding human performance in different areas. IT programs are becoming more accurate, detecting and scaling objects better than human performance. Speech recognition systems can now identify the language of telephone calls and voice recordings with levels of accuracy that match human abilities (Moșteanu, 2019a). Translating from one language into another is now done in real time, using a simple application on the phone. Glasses can be connected directly to google map or another search program. All of these are already part of our lives (Moșteanu, 2019b). *Artificial Intelligence* solutions have the potential to transform such diverse and critical areas as education, research, healthcare, finance, accounting, auditing, transport and energy. It is not a single technology but a family of technologies (Moșteanu, 2019c). In addition, *Artificial Intelligence* solutions can help sustainable, rapid and viable regional development. The regional economic disparities that exist in different areas of the world can be diminished considerably. Therefore, *Artificial Intelligence* can help to successfully implement regional development policy objectives (Moșteanu, 2019d), regardless the geographical area, the spoken language or the sectors of predominant activity. *Artificial Intelligence* is taking the financial services industry by storm. Almost every company in the financial technology sector has already started using Artificial Intelligence to save time, reduce costs, and add value. Robo-advisors track account activity using Artificial Intelligence capabilities to analyze and understand how account holders spend, invest and make financial decisions, so they can customize the advice they give their customers. Many banks have prioritized strategic technological advancement by investing in Artificial Intelligence applications to better serve their customers, improve performance, and increase revenue (Sigmoidal, 2019; (Moșteanu, AlGhaddaf, 2019). Over the years, global technology has evolved, we have switched from television, radio and newspapers to the Internet, and now we are slowly and gradually adapting to *artificial*

intelligence. Artificial Intelligence processes are more effective in identifying data models than in people, which is beneficial for companies to understand the target audience and gain an understanding of how to perceive the financial services they offer. For thousands of companies around the world, Artificial Intelligence has become the next tool to improve the performance of the financial industry (figure no.1). The service and financial industry are the ones that benefit most from Artificial Intelligence. Cognitive computing, Chatbots, Personal Assistant, Machine Learning are all peripherals of AI used in the finance industry today. Many financial organizations are now willing to invest in the Artificial Intelligence, with their own funds or non-refundable foreign funding. Europe has increased its commitment to developing Artificial Intelligence technologies. The *Artificial Intelligence for European Union* (AI4EU) project officially started in January 2019, with a kick-off meeting among the partners in Barcelona on 10 January 2019. AI4EU brings together 79 top research institutes, SMEs and large enterprises in 21 countries to build a focal point for Artificial Intelligence resources, including data repositories, computing power, tools and algorithms. It will offer services and provide support to potential users of the technology, help them test and integrate AI solutions in their processes, products and services (European Commission, 2019). Although they are confronted by a lack of confidence, prejudice, and major regulatory concerns, Artificial Intelligence has begun to gain popularity as a result of the use of large data, cloud services, and hyper-processing systems. Therefore, today's companies are open to a reliable solution designed to help people. Technological development is evolving at a very dynamic rhythm, and in the near future, important business decisions will also be based on the solutions provided by Artificial Intelligence, as it has the ability to identify how customers react to different situations and problems. Artificial Intelligence will help make good decisions at a very fast pace. However, finding the right balance between people and machines will always be necessary and timely.

There can be five ways how Artificial Intelligence has transformed the finance industry: risk assessment; fraud detection and management; financial advisory services; trading; and managing finance.

Artificial Intelligence can be successfully implemented where there is a previous database. Institutions providing financial services offer such a database either because accounting and records are second nature of the business, or because they have a record of clients and their services. An example for financial service can be: credit cards. Banking uses credit scores as a means of deciding who is eligible for a credit card and who is not. Thus, based on customer data, information is obtained about the individual loan repayment habits, the number of loans currently active, the number of existing credit cards, etc. These data can be used to customize the interest rate on a card so that it makes more sense for the financial institution that offers the card. Now, take a minute to think about the system that has the ability to go through thousands of personal financial records to come up with a solution - a machine taught. Here comes Artificial Intelligence (Moşteanu, 2019c). Given that it is based on data and dependent data, scanning through these records gives Artificial Intelligence the opportunity to make a recommendation of historical lending and credit offerings (Maruti TechLabs, 2019). Artificial Intelligence helps reduce data processing time, customer risk assessment, and decision-making on current and future client management. One of the biggest challenges faced by large banks, insurance companies, and financial institutions when trying to adopt Artificial Intelligence is that large volumes of their historical data are stored in paper documents rather than in digital spaces. Machine learning models are necessarily trained on digital data, so financial institutions have to ensure that they digitize old documents before hiring scientists to build Artificial Intelligence solutions or to purchase Artificial Intelligence software from vendors (Azuly, 2019).

Risk reduction is taken into account by each institution, especially those that offer financial services, and trades money or movable assets with economic value. For example, a bank's loan. The loan that a bank offers is, in principle, someone else's money, so you also pay interest on deposits and dividends on investments. That is why banks and financial institutions have many frauds. Artificial Intelligence ranks first in identifying security and fraud. Can use past spending behaviors for different trading tools to highlight strange behavior, such as the use of a card in another country just hours after being used elsewhere or an attempt to withdraw an amount unusual money for the account in question. Another excellent feature of fraud detection using Artificial Intelligence is that the system has no doubts about learning. If it raises a red flag for a regular transaction, and a human being corrects this, the system can learn from experience and make even more sophisticated decisions about what can be considered fraud and what cannot (Autonomus Next, 2019). Currently, the site of the majority of financial institutions has chat consultants. In the future, we can expect more robot consultants. These would reduce the costs of counselling and consultation, and therefore, at the institution level, the level of commissions for individual investments would be reduced. Another evolving area is bionic consulting, which combines machine calculations and human understanding to offer options that are more effective than what their individual components provide. Collaboration is crucial. Even now SMEs still use to perform financial and accounting recordings in a rudimentary and essential way using very simplified software (Faccia et. al., 2019), artificial Intelligence together with people becomes a common component of the financial decision-making process (Moşteanu, 2019c).

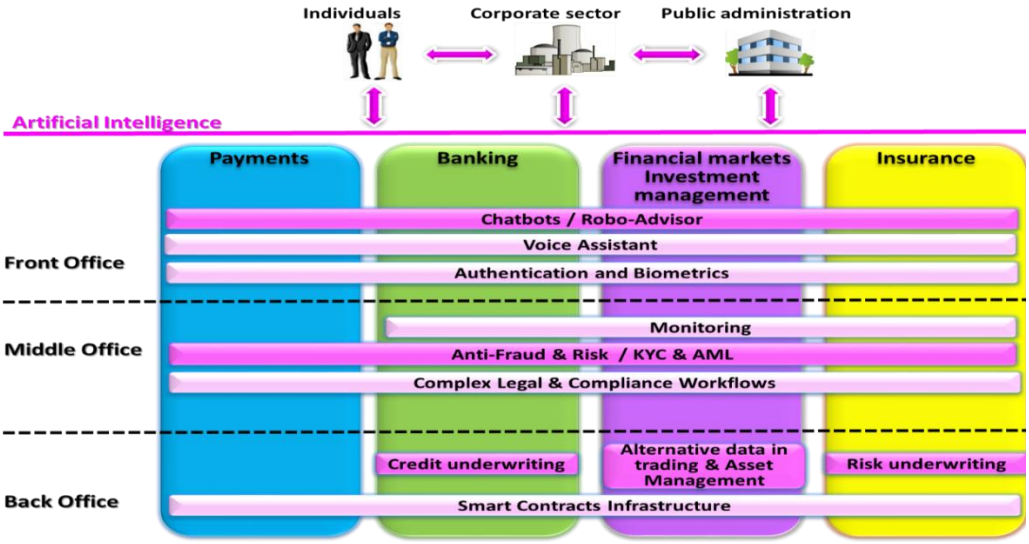

Figure no.1: Artificial Intelligence used in different types of businesses. (Moşteanu, 2019c)

With regard to capital markets, financial institutions are based on and rely on computers and experts to determine future models of the market. Transactions and investments depend on the ability to accurately predict the future. The machines are excellent because they can shorten a huge amount of data in a short time. Cars can also be taught to follow patterns in previous data and predict how these patterns could be repeated in the future. Although abnormalities such as the financial crisis of 2008 are in the data, a machine can be taught to study the data to find *triggers* for these anomalies and to plan them in terms of future forecasts (Autonomus Next, 2019). Moreover, depending on the individual risk appetite, Artificial Intelligence can suggest portfolio solutions to meet the demand of each individual. Therefore, Artificial Intelligence can definitely help in making decisions about when to buy, hold and sell the stock.

IV. RESEARCH ANALYZE AND FINDINGS

Analysis of Artificial Intelligence

Few years ago, Artificial Intelligence was considered as a threat as some studies were predicting that a big slice of the workforce was going to lose their jobs and replaced by artificial intelligence applications and machinery. In 2013, Carl Benedikt Frey and Michael Osborne, both Oxford academics, estimated that by middle of year 2030, 47% of Americans jobs are at high risk of losing their jobs since they will be replaced by automation (Frey, Osborne, 2017). Even near-term outlook has been quite negative. A study by OECD revealed that 9% of the jobs in 21 countries forming part of the OECD membership could be automated (Arntz et. al., 2016).

Yet recent studies revealed that companies are more likely to be using Artificial Intelligence to enhance computer to computer activities and much less often to human activities. This is a case of Associate Press where, in 2013, the company saw the necessity to adopt Artificial Intelligence and train Artificial Intelligence software to write short earning stories. Staff reporters at Associate Press could not barely cope with the increased demand for quarterly earning stories. In 2015, Artificial Intelligence helped Associate Press by writing over 3,700 quarterly new short stories, 12 times the number written by the staff reporters. In this case, Artificial Intelligence did not contribute to mailbag reports, instead it contributed to free business reporters in writing more in-depth stories on business trends (Associated Press, 2019).

As mentioned previously, Artificial Intelligence is being used for several purposes such as suggest what customer can buy, conducting online securities trading, however as shown in the above image Information technology is the largest adopters of Artificial Intelligence. Geographically increase in cyber-attack attempts are overloading IT professionals, who have to deal almost daily with these increase in hacking attempts. In fact, 44% of the global companies surveyed are using or willing to use Artificial Intelligence in their IT department to monitor, detect and deterring security intrusions. This is achieved by monitoring huge amount of machine to machine activities. Artificial Intelligence is not automating the jobs of IT security personnel but with it help to detect cyber-attacks, and, with an intensive monitoring of machine to machine data, these types of attacks were significantly reduced. In reality, Artificial Intelligence is helping IT security professionals to be more valuable to their company by focusing on other more valuable security tasks.

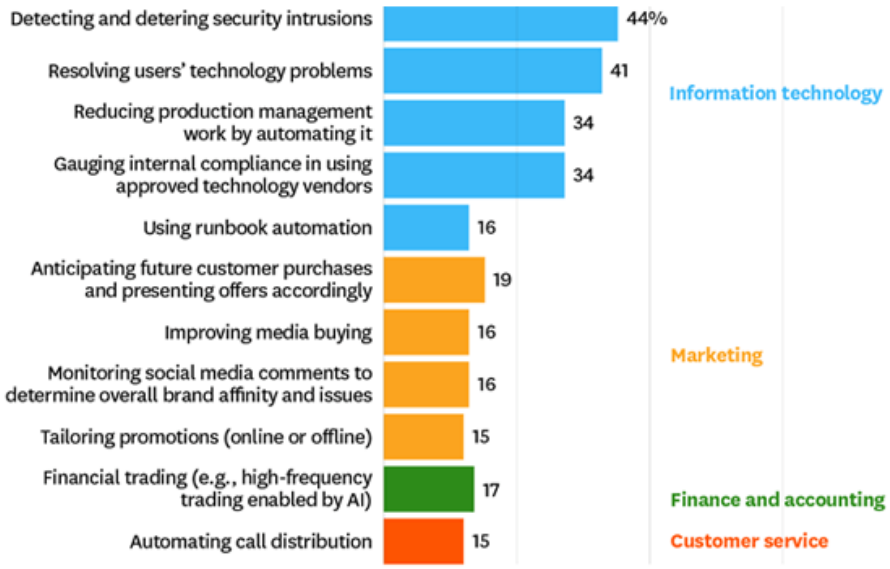

Figure no.2: The use of AI within businesses activities. (r-stylelab.com, 2017)

Analysis of Artificial Intelligence implementation in Malta

The Maltese government is embarking heavily in Artificial Intelligence and keen to work and collaborate with companies, nations and R&D organizations to accelerate the Artificial Intelligence agenda. Malta is being seen as the ultimate Artificial Intelligence project site.

The present analyze revealed that there are numerous factors for Malta to be considered as the Artificial Intelligence project site. Malta's population is only half a million of inhabitants and a tech-savvy population, EU member state and English as an official language. Apart from that, its strong and rapidly growing economy with established law and regulatory framework make it more ease to promote the adoption and use of innovation technologies. Our research understood, that during the last two years, Malta give a special attention to Artificial Intelligence and Cybersecurity, organizing forums and summits (2018-2019), making a link between public and private sectors, businesses and academia (Malta.AI.com, 2019). More than this, there is a Public Strategy for implementing Artificial Intelligence. The first strategic pillar seems to be to increase awareness of what Artificial Intelligence and all about its of practical use for businesses, particularly, and society in general. From this respect, a special attention is given to research and Development activities and Start-ups focused on new technologies innovations. The second pillar aims to adapt Artificial Intelligence in public sector and transform the way citizens and business interact with government by providing public services of excellence by being more efficient and improving internal operations and governance, leading to better use of taxpayers' money. In this respect, there are many pilot-projects. One of them include Artificial Intelligence for traffic management. Artificial Intelligence can identify traffic patterns behavior and optimize traffic light control with an ultimate aim is to reduce congestion and emissions. A mobility analytic dashboard will be developed to generate location intelligence across different modes of transport in real time. Similar approaches will be used in public sectors, such as education, healthcare, tourism and utilities. The third pillar foreseen to adopt Artificial Intelligence in the local businesses. From this perspective, the government will aid in developing and integrate Artificial Intelligence applications in the way they work and the way they do business (Hub.packpub.com, 2019). From our analyze we may say that topic as Artificial Intelligence is bleary new in Malta, and starting with 2018, along with awareness of it importance promoted at European Union level, it began to occupy one of the prime places in the country's development strategy. Currently no businesses implemented Artificial Intelligence within their operational process. Nevertheless, Malta expect very soon to have businesses and public entities which are using Artificial Intelligence to increase profitability and as a tool for risk management (specially to reduce human errors).

Analysis of Cybersecurity

Over the years followed, computers started to become more and more connected, programs more and more advanced, interconnecting many data. Today we are using smart phones, glasses or watches, which are connected to our social and professional network. This is great! It makes our life easier. Still to have access to all these *benefits* we are using many applications, which may come at the package with viruses, which are becoming more advanced, and may expose ourselves to any cyber-attack.

The Accenture's graphical representation collected from 254 companies all over the world, describes the costs of the most common attacks based on their frequency in 2016 and 2017 (figure no.3). The study reports

that this year (2019) the global average cost of a data breach is up 6.4% over the previous year to $3,860,000 million. The average cost for each lost or stolen record containing sensitive and confidential information also increased by 4.8% year over year to $148. The top costliest cyber-attacks like malware attacks do not involve directly the theft of money from the targeted organization. However, this costs to an organization an average of $2,400,000 per attack (Hub.packpub.com, 2019).

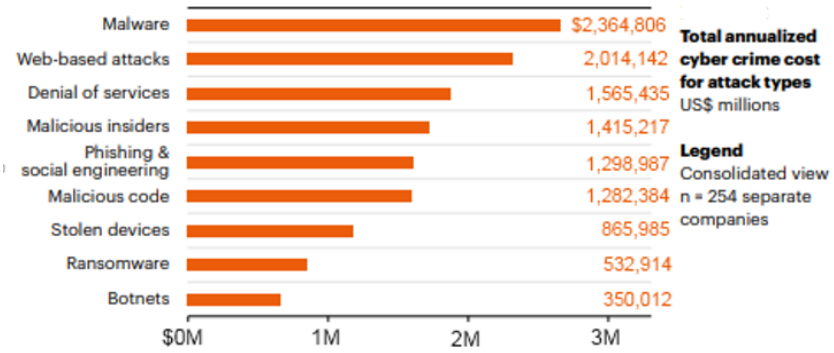

Figure no.3: Cyber-crime' cost from different attack types (r-stylelab.com, 2017)

Malware threat has become sophisticated and more accessible as skilled hackers are selling their malware on the dark web at affordable prices. Similarly, as in real life, a house can have high security measures and hardware such as cameras and alarms, still a thief may obtain unauthorized access by using a backdoor, which may have less security protection. The thief can still have access to the house without activating alarms and cameras, thus letting the owner unaware of the intrusion. Similarly, in cybersecurity a backdoor refers to an unauthorized user infiltrate in a computer system, gaining high-level user access without the owner's knowledge. In practice, we have notices find out various forms of malware. It includes all malicious software like tracking cookies, which are used to monitor the trends and habits of user, key logger, Trojan horses, worms and viruses. The intention of this attack is mainly to steal personal and financial data, install additional malware and hijack devices. Unlike other cybersecurity attacks that make the user aware of the attack like ransomware, backdoors are discreet. Due to the discreet nature, backdoor attacks are one of the most common threat for both consumers and business. In fact, in 2018 this cyber-attack threat increased from 34 to 173% over previous year (Malwarebytes.com, 2019). A common example cybercriminal obtain access by hiding a backdoor malware inside a tool used to hack a pirated software. Another example is to attach the malware software to seemingly legitimate application such as Coin Ticker. This application has two purposes; the first purpose is to allow users to monitor prices of various crypto currencies, and the second purpose, a malicious one, is to secretly install in the background not one but two backdoors with the aim to gain remotely access and control to the system (Csoonline.com, 2017).

Cyber-attack can affect drastically the production process causing financial losses such as an ecommerce shop will be unable to continue its business after a DDoS attack or web-based attack. Similar attacks can also affect physical machinery, for instance the Stuxnet cyberattack against one country's nuclear facility. The Stuxnet purpose was not only to be able to access the computers but also to target specific machinery like the centrifuges used to the production of enriched uranium that powers nuclear weapons and reactors. The attack managed to control the speed of spun of these centrifuges, damaging the delicate equipment, and, also managed to falsify the diagnostic status of these equipment thus making it difficult to detect the wrongdoing (Csoonline.com, 2017).

Analysis of Cybersecurity and Cyber-attacks in Malta

Cyber-attack also affected Malta, in fact 40% of local businesses suffered from a form of cyber-attack. Most of the firms where affected with various forms of cyber-attacks, mainly by fraudulent emails, scam calls and unknowing installation of malware or malicious software. There are various motives in doing a cyber-attack, for instance a bank can be attacked asking for money or denial of service (DDos). In cases where that attacks are on government entity, the aim of the attack could be disrupting any government operations (Schembri, 2019).

A very recent cyber-attack affected operations of a local bank. Bank of Valletta (BOV) had to halt all its operations this year after a cyber-attack hacked the system and moved funds overseas (Reuters, 2019). The attack consisted of creating false international payments totaling 13 million and transfer these millions to banks in UK, US and Czech Republic and Hong Kong. The state security service informed the Central Bank that the BOV conducting the wrong activities. From that certain moment, BOV initiated a task force to suspend all the ATMS, branches and website after the reconciliation of payment failed to match. This move caused a disruption in the economy as BOV hold half of the Maltese accounts. Additionally, apart from the Maltese economy, it

disrupted the operations abroad as like some credit card holders couldn't send payments to hotels abroad (Reuters, 2019).

Cyber-attack can also be intended to disrupt government reputation. The local press announced that Malta's government servers has faced a rise in attacks during the Malta's presidency of Europe's Council of Ministers in 2017. The attacks increase by 40% on the normal level of attacks, mainly DDoS and some malware on computer systems from phishing emails, over five million phishing emails a month. This attack caused governmental service web sites to perform drastically slower, causing the government online services to a halt. However, it is believed that the attacks did not penetrate the government systems (The Guardian, 2017).

V. CONCLUSIONS AND RECOMMENDATIONS

The research paper it emerged that Cyber-attack is a real threat and will definitely increase in its intensity and sophistication in the coming years. Thus, we have to be prepared and use new technological tools such as Artificial Intelligence and Cybersecurity to protect sensitive data, at any level, from individual, business to government and entire nation from warfare created by cyber-attacks. In this regards nation around the world should adopt strategies in creating awareness about new technologies and give financial support for research and develop in new technologies.

The present research tried to present the importance of Artificial intelligence and Cybersecurity to protect ourselves against Cyber-attack. Simultaneously, the present paper comes to underline the importance of using the artificial intelligence and cybersecurity to create a safer business environment. From this perspective, we can say that, companies from today and those from the coming future is better to start be aware, learn about, and look for opportunities where new technologies such as Artificial Intelligence could help in increasing business profitability and help in the same time to develop and implement an efficient cybersecurity system.

The research had shown that Artificial Intelligence can assist in creating a safer business environment. Artificial Intelligence can be implemented in any part of the business process, front-office, middle and in back-office functions. Artificial Intelligence can be implemented in any business, no matter the area of activities, anywhere where there are many computer-to-computer interactions. Good initiatives, as one proposed in recent months by the Government of Malta – *BSecure* scheme, it is better to be in any country. This program wants to instill an Artificial Intelligence and Cybersecurity mentality and assist the private sector in cybersecurity enhancement and awareness.

Nevertheless, humans can still be the weakest point in terms of cyber security. Although Artificial Intelligence can use machine to machine data learning to greatly aid in cyber-attacks, still a single careless user can cause severe damage the whole system and there is no way to predict that. Awareness about thinking on how to use internet should be the first priority for IT security manager's way before adapting any new technology. All of us has to be aware that *everyone can be a target* for a cyber-attack, and, from this respect is better to limit sharing data on social media (Moşteanu, 2019e). The present paper present below some possible solutions that can help in having a secure work environment: use a strong password for any electronic device; lock any equipment that have sensitive information or that is a gateway to other computers with sensitive information; attachments or links is better to not be opened if they are coming from unknown sources; sensitive browsing such as internet banking should be done on secure devices that you can trust; the computer or any device which is connected to the interned is better to have and anti-malware and anti-virus program, updated regularly; or, use carefully any external hard disks or flash drives (they can contain virus or malware which can spread into the system); and, ask for help if any unfamiliar activity appears on computer's system.

VI. REFERENCES

1. Arntz M., Gregory T., Zierahn U. (2016) *The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis*, OECD Social, Employment and Migration Working Papers, No. 189, OECD Publishing, Paris, [Retrieved on 17th November 2019] from https://doi.org/10.1787/5jlz9h56dvq7-en
2. Azuly D. (2019) *Artificial Intelligence in Finance – a Comprehensive Overview*, [Online], [Retrieved November 15, 2019], https://emerj.com/ai-sector-overviews/artificial-intelligence-in-finance-a-comprehensive-overview/
3. Autonomus Next (2019) *Augmented Finance and Machine Intelligence*, [Online], [Retrieved November 15, 2019], https://next.autonomous.com/augmented-finance-machine-intelligence/
4. Dilek S., Çakır H., Aydın M. (2015) *Applications of artificial intelligence techniques to combating cyber crimes*: A review. arXiv preprint arXiv:1502.03552
5. Faccia A., Moşteanu N.R., Fahed M., Capitanio F. (2019) *Accounting Information Systems and ERP in the UAE*. An assessment of the current and future challenges to handle big data. ACM International Conference Proceeding Series. SCOPUS Proceedings of 3rd International Conference on Cloud and Big Data Computing (ICCBDC 2019), St Anne's College in University of Oxford, Oxford, UK August 28-30
6. Frey C.B., Osborne M.A. (2017) *The future of employment: How susceptible are jobs to computerization?*, [Online], [Retrieved on 16th November 2019], from https://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf
7. Hansen L., Nissenbaum H. (2009) *Digital disaster, cyber security, and the Copenhagen School*, International studies quarterly, 53(4), 1155-1175

8. Koistinen A.K. (2016), *The (care) robot in science fiction: A monster or a tool for the future?*, Confero, 4 (2), 97-109. doi:10.3384/confero.2001-4562.161212
9. Marketingcharts (2017) *AI is the Marketing Trend That Has the Most Marketers Feeling Unprepared*, [Online], [Retrieved on 17th November 2019], from https://www.marketingcharts.com/customer-centric/analytics-automated-and-martech-81716
10. Moşteanu N.R. (2019)a *Principles of International Finance, Banking and Taxation*. Publisher: Universitara, Bucuresti, Romania
11. Moşteanu N.R. (2019)b *International Financial Markets face to face with Artificial Intelligence and Digital Era*, Theoretical and Applied Economics. No.3/2019 (620), Autumn. P.123-133. ISSN 1844-0029
12. Moşteanu N.R. (2019)c *International Financial Markets under Artificial intelligence influence*, 34th IBIMA Spain, 13-14 November 2019, Conference Proceedings
13. Moşteanu N.R (2019)d *Regional development and Economic Growth approach in Europe and GCC*. Ecoforum Journal, Vol.8, No.2., 583-595
14. Moşteanu N.R., (2019)e *Artificial Intelligence and Cybersecurity – A shield against Cyberattack as a Risk Management tool – A case of European Countries*, Quality Access to Success Journal, Vol.21, No.175, April 2020
15. Moşteanu N.R., AlGhaddaf C. (2019) *Smart economic development using foreign direct investments – UAE case study*, Journal of Information Systems & Operations Management, Vol.13 No.1., p.9-20
16. Murphey D. (June, 2019) A history of information security, [Online], [Retrieved November 15, 2019], from IFSEC Global website https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/Schembri S. (October, 2019) *€250,000 cyber security scheme launched; 'cyber security must be incorporated into ecosystem'*, Cyber Security Summit, The Independent Malta, [Online], [Retrieved on 15th November 2019], from https://www.independent.com.mt/articles/2019-10-23/local-news/Live-Malta-s-first-ever-Cyber-Security-Summit-gets-underway-6736215132
17. Shiva S., Roy S., Dasgupta D., (2010) *Game theory for cyber security*, In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (p. 34). ACM
18. Sigmoidal (2019) *Artificial Intelligence in Finance*, [Online], [Retrieved November 15, 2019], https://sigmoidal.io/real-applications-of-ai-in-finance/
19. Turing A. (1950) *Computing machinery and intelligence*, Mind, 59(236), 435–460
20. Von Solms R., Van Niekerk J. (2013) *From information security to cyber security*. Computers & Security, 38, 97-102
21. Associated Press (2019) *Leveraging AI to advance the power of facts*, [Online], [Retrieved on 17th November 2019], from https://www.ap.org/discover/artificial-intelligence
22. BleepingComputer (2018) *Mac CryptoCurrency Price Tracker Caught Installing Backdoors*, [Online], [Retrieved November 16, 2019], from https://www.bleepingcomputer.com/news/security/mac-cryptocurrency-price-tracker-caught-installing-backdoors/
23. Csoonline (August, 2017) *What is Stuxnet, who created it and how does it work?*, [Online], [Retrieved November 16, 2019], from https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html
24. European Commission (2019) *Digital Single Market, Press Release*, [Online], [Retrieved November 15, 2019], https://ec.europa.eu/digital-single-market/en/news/artificial-intelligence-79-partners-21-countries-develop-ai-demand-platform-eu20-million-eu
25. Hub.packtpub (2019) *Understanding the cost of a cybersecurity attack: The losses organizations face*, [Online], [Retrieved November 16, 2019], from https://hub.packtpub.com/understanding-the-cost-of-a-cybersecurity-attack-the-losses-organizations-face/
26. Malta.AI (2019) *Malta_The_Ultimate_AI_Launchpad*. [Online], [Retrieved on 17th November 2019], from https://malta.ai/wp-content/uploads/2019/10/Malta_The_Ultimate_AI_Launchpad_vFinal.pdf*** Maruti TechLabs (2019) *5 ways AI is transforming the finance industry*, [Online], [Retrieved November 15, 2019], https://www.marutitech.com/ways-ai-transforming-finance/
27. Malwarebytes (2019) *Backdoor*, [Online], [Retrieved November 16, 2019], from https://www.malwarebytes.com/backdoor/
28. Reuters (2019) *Cyber attack on Malta bank tried to transfer cash abroad*, [Online], [Retrieved on 15th November 2019], from https://www.reuters.com/article/us-bank-valetta-cyber/cyber-attack-on-malta-bank-tried-to-transfer-cash-abroad-idUSKCN1Q21KZ
29. The Guardian (May, 2017) *Malta accuses Russia of cyber-attacks in run-up to election*, [Online], [Retrieved on 16th November 2019], from https://www.theguardian.com/world/2017/may/27/russia-behind-cyber-attacks-says-malta-jseph-muscat