DIGITAL THREAT ANALYSIS

Professor Serghei Ohrimenco DSc[1]
Associate Professor Lucia Gujuman, PhD[2]
Valeriu Cernei[3]

Resume: *Our ubiquitous world is changing rapidly under the influence of digital transformation and serious preparation for new challenges and threats is required. The composition of the latter is constantly changing due to the development and improvement of computing equipment, software and technologies for collecting, processing and storing information. Under these conditions, the relevance of research work on topics related to the assessment of possible threats in the digital economy is increasing. An additional factor of influence is changes in the digital information structure, the transition to remote (home) work of users and others. Modern society increasingly relies on robotic and digital operations instead of human labor. All this puts the information and communication resources of the state and individual firms at risk of hacker attacks and software abuse. This paper examines the historical aspects of the development of program abuse as the basis of modern digital threats to the individual, society, and the state.*

Keywords: *Cyber Threats, Digital Threats, Cybersecurity, Risk Management, Risk Strategy*
JEL: D74 D81 F52
DOI: https://doi.org/10.58861/tae.pcesetfc.2024.39

1. Introduction

The development and improvement of computing, software and communications have ensured the penetration of information and communication technologies and their components into all spheres of human activity. At the same time, the digital threat landscape is growing, both quantitatively and qualitatively. The authors set themselves the goal of reviewing the evolution of software threats as applied to information systems and developing methodological foundations for identifying promising digital threats to the individual, society and the state.

2. A Short History of Digital Threats

The authors focused their study only on threats to information systems and resources of government and commercial organizations. The study left out

[1] osa@ase.md Academy of Economic Studies of Moldova, Laboratory of Information Security, Chishinau, Moldova
[2] Gujuman.lucia@ase.md Academy of Economic Studies of Moldova, Department Information Technology and Information Management, Chishinau, Moldova
[3] Valeriu.cernei@bsd.md Partner, IT Audit&Advisory, BSD Management SRL, Chishinsu, Moldova

electronic warfare, air defense systems, and others related to systems of electronic confrontation between states in special periods.

In the era of digital economy development, new theoretical research in the fields of economics and management has emerged against the backdrop of rapid startup growth. Our task is to consider the digital economy as the foundation of research through the lens of theories and models. As stated in (Zhu, 2019), if the digital economy is viewed as the basis for macroeconomic research, its substructure can cover the following ten areas: Data economy, Service economy, Platform economy, Internet of things economy, Sharing economy, Prosumer economy, Long-tail economy, Inclusive economy, Collaborative economy, Smart economy.

Historically, digital threats are divided into several phases, which will be discussed below. The material presented is based on research conducted by the authors, as well as additional monographic sources (Ferbrache, 1992), (Parikka, 2007), (Ning, 2022), (Middleton, 2017), (Fitsanakis, 2020) .

2.1 First phase

The first stage is characterized by the use of software abuses focused on personal computers (PCs) before the emergence of the Internet. It covers the period from the first PCs to the mid-1980s of the 20th century. The most representative are the following: Program Creeper (1971), Program created as a test program, a prototype of future computer viruses; Virus Rabbit (1974). The first computer virus created with a malicious purpose, a self-replicating mechanism by creating a large number of copies; Virus Brain-I (1986). A boot sector virus that infected 5-inch floppy disks for personal computers; Virus Brain-II (1987). Virus destroyed files when they were started, one of the first MS-DOS viruses to cause a virus epidemic.

2.2 Second phase

The second phase is characterized by the use of software abuses of the Internet era. These should include the following: Virus Morris Worm (1988). One of the first network worms to spread over the Internet. This malware was able to infect computers due to some vulnerabilities in the software, and the worm could infect the same computer several times, thus causing a significant slowdown in speed, up to complete loss of performance; Virus Malware (1990-1999). An example is Melissa Virus. Malware is malicious software intended to cause some form of damage to a user or computer and its contents. Malware is a general name for all types of cyber threats such as: viruses, trojans, spyware, keyloggers, adware, etc. Malware is the name for all types of cyber threats. A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk; **ILOVEYOU** (2000). This virus spread via e-mail, erased existing files

and wrote its own copies on top of them; DDOS (2000-2001). It is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites; Network Worm (2002-2003). A type of malicious program that self-propagates through local and global computer networks, for example, Slammer, a network worm that caused a denial of service to some Internet hosts and a severe decrease in overall Internet traffic; Spam Phishing (2004-2005). A type of Internet fraud in which a fraudster tries to fraudulently gain access to important information: logins and passwords, bank card and passport data, verification codes, intimate photos, important correspondence - anything that can help him get money, for example **Sasser**, a computer worm discovered on the Web, whose epidemic began on April 30, 2004. Within days, the worm „infected“ some 250,000 computers around the world. When **Sasser** infiltrated a machine, it scanned the Internet for other computers with an unpatched hole and sent itself to them; **Botnet** (2006-2007). A network of computers infected with malicious software, for example - **ZeuS**, a new type of Trojan program and botnet that appeared in 2007 and is designed to intercept passwords from payment systems and then steal money; **Web Threats** (2008-2009). A web threat is any threat that uses the internet to facilitate cybercrime. Web threats use multiple types of malware and fraud, for example **Conficker**, a computer worm that blocks a computer's access to antivirus vendors' websites.

2.3 Third phase

The third stage combines modern cyber-attack tools. These include the following: **Virus Stuxnet, DuQu, Flame** (2010-2012). All three share a common origin. They are often cited as the foundation of cyberweapons; **Advanced Persistent Threat** (APT) (2010-2011). APT - Advanced Persistent Threat is a cybersecurity term referring to an adversary that has an advanced level of specialized knowledge and significant resources that allow it to pose a threat of dangerous cyberattacks, for example - Stuxnet - a network worm that can be used as a means of unauthorized data collection (espionage) and sabotage in automated control systems of industrial enterprises, power plants, airports, etc.; **Ransomware** (2012-2014). **Ransomware, blackmailer** - a type of malicious software designed for extortion, blocks access to a computer system or prevents the reading of data recorded in it, and then demands a ransom from the victim to restore the original state, for example, **CryptoLocker** - restricts access to infected computers by encrypting its contents); **Insider** (2015-2017). These are threats that are malicious to an organization and originate from people within the organization, such as employees, former employees, contractors or business partners, who have information about the organization's security practices, data and computer systems. The threat may include fraud, theft of confidential and commercially valuable information, theft of intellectual property, or sabotage of computer systems, for example, **WannaCry** is a malware, network worm and money extortion program, computers running Microsoft Windows operating

system, after successfully hacking a computer **WannaCry** tries to spread through the local network to other computers like a worm. It scans other computers for the very vulnerability that can be exploited by **EternalBlue**, and if it finds one, it attacks and encrypts them too; **M2M** (2018-2019) **Machine-to-Machine.** Machine-to-machine communication is a general name for technologies that allow machines to exchange information with each other, or to transmit it unilaterally. It can be wired or wireless systems for monitoring sensors or any parameters of devices. It describes the process of exchanging data between devices, for example, between some sensor and a database. M2M is one of the manifestations of the Internet of Things (IoT). It can be used in automotive telemetry, smart meters, smart asset accounting, for supply chain management, wearable technology, for example, VPNFilter is a malware designed to infect routers and some network storage devices; **Attack Surface** (2021). A term used in computer system information security tasks that refers to the total number of possible vulnerabilities. The more components installed on a server, the greater the number of potential vulnerabilities and, consequently, the attack surface. The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment. For example, **Log4j, Kaseya, Godaddy, SolarWinds and Panasonic**; **Destructive** (2022). This is a new form of destructive malware designed to infiltrate and disable Windows devices by destroying files, corrupting the Master Boot Record (MBR) and physical disks. For example **- HermeticWiper**; **AI-Enabled** (2023+present). This stage remains poorly understood but very promising for cybercrime. In recent years, cybercriminals have begun employing AI-enhanced malware to target vulnerable users and systems more effectively. Cybercriminals are adopting Artificial Intelligence (AI) techniques to evade the cyberspace and cause greater damages without being noticed. This sophisticated approach has led to the emergence of smart botnets, cluster-based attacks, and Swarmbots intelligence enabled by IoT devices. Additionally, hackers have used AIs to conduct compelling social engineering and phishing attacks. A major theme for the future remains the expanding landscape of cyber threats from AI applications, from data theft to exploitation of critical infrastructure vulnerabilities and the associated cybersecurity risks (Akartuna, 2024), (Guembe, 2022), (Slattery, 2024).

3. **Modern Digital Threats**

Let us make an attempt to identify a group of current digital threats. Modern trends in the development of digitalization processes are focused on the use of a large number of components, including Big Data, the Internet of Things, Artificial Intelligence, Machine Learning, Digital Twin, and others. Representatives of criminal business are in constant search for opportunities to reorient the achievements of scientific and technological progress for their own interests.

The emergence of technologies like cloud computing, Internet of Things (IoT), social media, wireless communication, and cryptocurrencies has generated security concerns in cyberspace. The trend of cyber criminals offering cyber-attacks as a service reflects shift toward attacks automation for a broader impact. Let us consider the modern threat landscape based on the use of advancements, including artificial intelligence. The development of artificial intelligence (AI) has demonstrated the potential for implementing important innovations, including in the field of crypto-assets (Akartuna, 2024). But, as with any new technology, there is a risk of its use for illegal purposes. Five new typologies of crimes using AI in the crypto-asset ecosystem have been identified. These include:

- Generative AI for deception in crypto scams, including the use and distribution of deepfakes and AI-generated material to advertise crypto scams.
- AI-related crypto scams and market manipulation schemes – including the creation of AI - related scam crypto tokens, investment platforms and ponzi schemes (fraudulent investment scheme).
- Using large language models (LLMs) to facilitate cybercrime – including the use of AI tools by hackers and hostile state actors for code vulnerability detection and for devising exploits.
- Deploying crypto scams and disinformation at scale – including the upscaling of capabilities for deploying scams using AI tools.
- Enhancing illicit markets – including the AI-enhanced expansion and creation of illicit economies for goods and services, such as dark web listings, explicit deepfake generation or falsified identity documents that can bypass know-your-customer (KYC) checks at crypto services.

Most experts attribute the rise in threats to the use of AI, which has significantly increased the productivity of cybercriminals through the use of a powerful new set of tools. Among them is WormGPT, an AI language model based on an open-source model and machine learning algorithms. Let us consider these options in detail.

- Phishing. Currently, the biggest use of generative AI among cybercriminals is phishing, which involves tricking a user into revealing confidential information. Researchers have found that the spread of ChatGPT was accompanied by a huge increase in the number and quality of phishing emails. Primarily, ChatGPT and language models were used to generate messages and improve the text of phishing emails. Thanks to better translation by AI, criminal groups around the world can also communicate better with each other. The risk is that they can coordinate large-scale operations beyond their countries and target victims in other countries.
- Deepfake audio scams. Generative AI used by specialists has made a leap forward and ensured the creation of synthetic images and realistic sounds. Simultaneously, video and audio files look and sound realistic. These achievements have not gone unnoticed by criminals. Cybercriminals use

created deepfakes to convince users to perform needed actions. In addition, deepfakes have become a commodity on the Darknet, where scammers sell their services for as little as $10 per image or $500 per minute of video. The relative cheapness of audio fakes is due to the relative ease of creation.

- Bypassing identity checks. Another way criminals use deepfakes is to bypass „know your customer“ verification systems. Banks and cryptocurrency exchanges use these systems to ensure their customers are real people. They require new users to take a photo with an ID document in front of the camera. But criminals have started selling applications on platforms like Telegram that allow people to bypass this requirement. They work by offering fake or stolen IDs and overlaying a fake image over the real person's face to fool the verification system on Android phone cameras.
- Jailbreak-as-a-service. Most machine models have usage policies. Jailbreak hacking allows users to manipulate the AI system to generate results that violate these policies, such as writing code for ransomware or generating text for phishing emails. Hacking services use various tricks to bypass security mechanisms, such as posing hypothetical questions or asking questions in foreign languages. There is a constant cat-and-mouse game between AI companies trying to prevent the misuse of their models and attackers coming up with increasingly creative jailbreak prompts.
- Doxxing and surveillance. AI language models are the perfect tool not only for phishing but also for doxxing (revealing private and identifying information about someone online). This is because AI language models are trained on huge amounts of internet data, including personal data, and can determine, for example, where someone might be located. The more information about users on the internet, the more vulnerable they will be to identification. Large language models like GPT-4 and others can generate and output such confidential information as ethnicity, location, occupation, etc.

4. Conclusion

The conducted analysis of digital threats will allow moving to the next section of information security management - cyber risk management (Ohrimenco, 2023), (Ohrimenco S. &., 2024)

Another important aspect is the direct impact of IT and AI on cyber forensics. The rapid growth of Internet of Things (IoT) technologies has had a huge impact on digital forensics due to their active use. Multimedia content created by various IoT devices, such as phones, body cameras, drones, vehicles, etc., for sharing and storing information, has forced forensic experts to develop methods that allow thorough data verification and analysis.

At the same time, advances in machine learning algorithms and AI have provided cybercriminals with new, more complex tools for altering and faking media content. One way to deceive the camera source identification method is to

deploy a deep learning structure called a Generative Adversarial Network (GAN) to generate data that mimics the noise of a working video camera.

The listed tools are not final and exhaustive. Over time, new IT advances are expected to emerge and be transformed into tools for cybercriminals. Thus, criminals can create fake videos to falsify the origin of the video source camera.

References

Akartuna, A. (2024, 11 8). *The state of AI-enabled crypto crime: Emerging typologies and trends to look out for.* . Retrieved from Eliptic: https://eliptic.co

Ferbrache, D. (1992). *A Pathology of Computer Viruses.* London: Springer-Verlag London Limited.

Fitsanakis, J. (2020). *Redesigning Wiretapping. The Digitization of Communications Interception.* Springer.

Guembe, B. A.-S. (2022). The emerging threat of ai-driven cyber attacks: A review. . *Applied Artificial Intelligence*.

Middleton, B. (2017). *A History of Cyber Security Attacks 1980 to Present.* CRC Press.

Ning, H. (2022). *A Brief History of Cyberspace.* CRC Press.

Ohrimenco, S. &. (2024). ECONOMIC SECURITY IN THE CONTEXT OF SYSTEMIC TRANSFORMATIONS. *CYBERSECURITY RISK* (pp. 145-154). Chisinau: ASE.

Ohrimenco, S. O. (2023). Cyber Threats Modeling: An Empirical Study. *Business Management/Biznes Upravlenie,*.

Parikka, J. (2007). *Digital Contagions A Media Archaeology of Computer Viruses.* New York: Piter Lang.

Slattery, P. S. (2024, 11 08). *The ai risk repository: A comprehensive meta-review, database, and taxonomy of risks from artificial intelligence.* . Retrieved from arXiv.

Zhu, X. Z. (2019). *Emerging champions in the digital economy.* Springer Singapore.